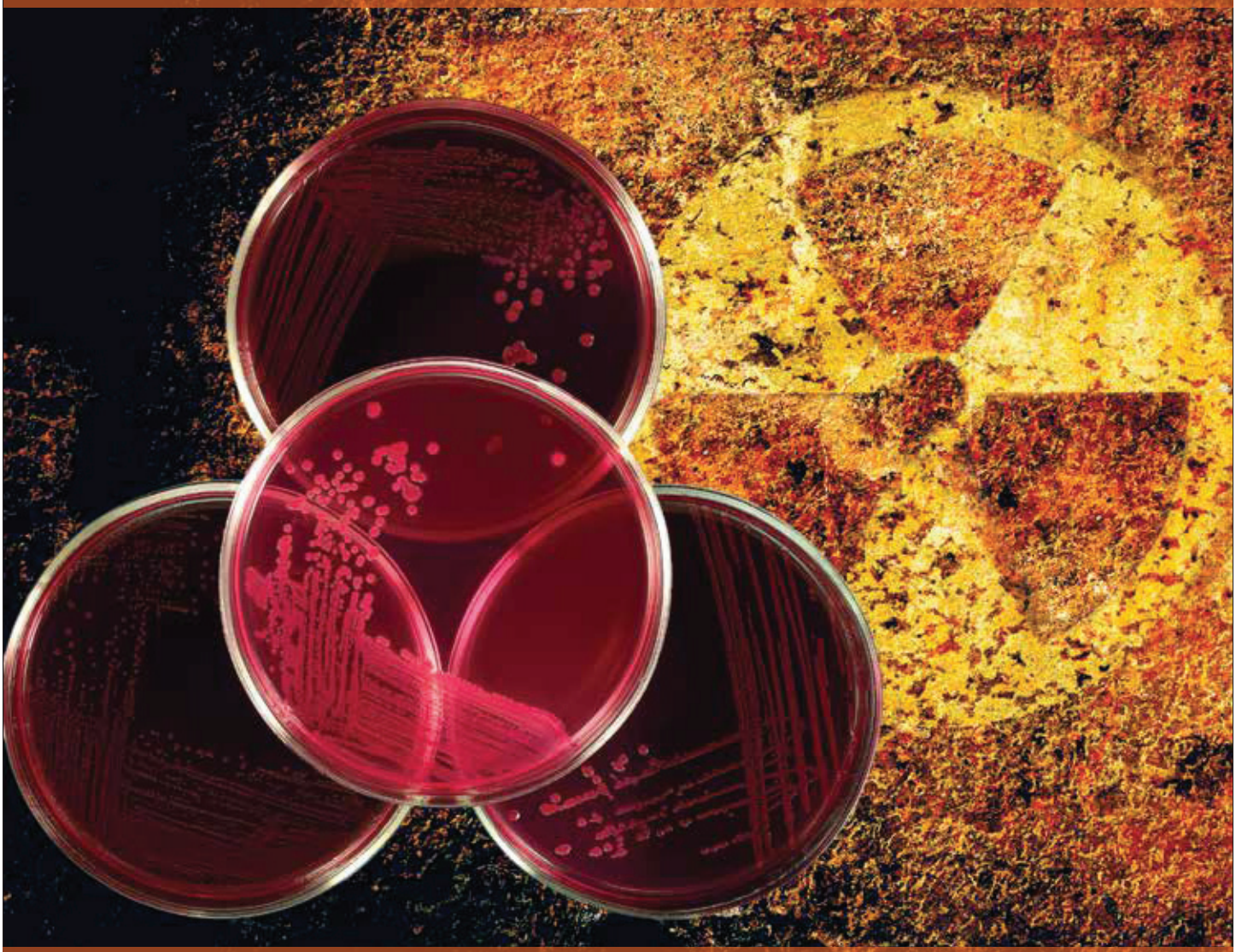
PRISM

VOL. 7, NO. 3 | 2018

COUNTERING WEAPONS OF MASS DESTRUCTION



THE JOURNAL OF COMPLEX OPERATIONS

PRISM
VOL. 7, NO.3 2018

ABOUT

PRISM, the quarterly journal of complex operations published at National Defense University (NDU), aims to illuminate and provoke debate on whole-of-government efforts to conduct reconstruction, stabilization, counterinsurgency, and irregular warfare operations. Since the inaugural issue of *PRISM* in 2010, our readership has expanded to include more than 10,000 officials, servicemen and women, and practitioners from across the diplomatic, defense, and development communities in more than 80 countries.

PRISM is published with support from NDU's Institute for National Strategic Studies (INSS). In 1984, Secretary of Defense Casper Weinberger established INSS within NDU as a focal point for analysis of critical national security policy and defense strategy issues. Today INSS conducts research in support of academic and leadership programs at NDU; provides strategic support to the Secretary of Defense, Chairman of the Joint Chiefs of Staff, combatant commands, and armed services; and engages with the broader national and international security communities.

COMMUNICATIONS

PRISM welcomes unsolicited manuscripts from policymakers, practitioners, and scholars, particularly those that present emerging thought, best practices, or training and education innovations. Publication threshold for articles and critiques varies but is largely determined by topical relevance, continuing education for national and international security professionals, scholarly standards of argumentation, quality of writing, and readability. To help achieve threshold, authors are strongly encouraged to recommend clear solutions or to arm the reader with actionable knowledge.

Our review process can last several months. The *PRISM* editorial staff will contact authors during that timeframe accepting or regretfully rejecting the submission. If the staff is unable to publish a submission within four months of acceptance, *PRISM* will revert publication rights to the author so that they may explore other publication options.

Constructive comments and contributions are important to *PRISM*. We also welcome Letters to the Editor that are exclusive to *PRISM*—we do not publish open letters. The *PRISM* editorial staff will contact authors within two months of submission if they accept the letter for publication.

Please direct all electronic comments and contributions to <prism@ndu. edu>. Hard copies should be sent to the address listed below and include a note that highlights a preferred phone number and email for feedback; *PRISM* does not return hard original hard copy submissions.

Editor, *PRISM*
260 Fifth Avenue, S.W.
Suite 2500
Fort Lesley J. McNair
Washington DC 20319

DISCLAIMER

COUNTERING WEAPONS OF MASS DESTRUCTION

FEATURES

INTERVIEW

BOOK REVIEWS

The chances of a successful nuclear terrorist attack in the decade that began in 2015 are better than even. –Graham Allison

Nuclear Terrorism
Did We Beat the Odds or Change Them?

By Graham Allison

It has been more than 13 years since the publication of *Nuclear Terrorism: the Ultimate Preventable Catastrophe*, which sounded the alarm about the clear and present danger of nuclear terrorism. The book made the case for two seemingly contradictory propositions: first, on the current path, nuclear terrorism is inevitable; second, nuclear terrorism is preventable by an agenda of actions that are feasible and affordable. Juxtaposition of these propositions presented a paradox that the book attempted to resolve.

By highlighting the gap between what the United States, Russia, and other nations had been doing in the decade prior to 2004, and what could be done if they made preventing nuclear terrorism a first-order priority, I argued that on the current path we would likely see terrorists succeed in their aspirations for an "American Hiroshima." At the same time, I argued, there existed a feasible, affordable agenda of actions the United States and other civilized nations could take that would reduce this risk to nearly zero.

As reviewers later noted, the book "caught a wave." During the 2004 Democratic presidential primary, the Nuclear Threat Initiative (NTI) led a concerted effort to raise the visibility of this issue. Former Senator Sam Nunn, a NTI co-chair, called the book "essential reading . . . calling citizens to arms against the real and rising threat of nuclear terrorism." The world's most successful investor, whose company's share value has increased a thousand fold during the five decades he has managed the investment corporation, selected *Nuclear Terrorism* as the Berkshire Hathaway annual meeting's "book of the year." Warren Buffett declared: "Nuclear terrorism is by far the most important problem of our time. And this is the most important book that has been written on the subject."

In the final months of the 2004 presidential campaign, the question of what the United States should be doing to address the threat of nuclear terrorism became a compelling issue. Both contenders—John Kerry and George W. Bush—declared in their first debate that nuclear terrorism is the "single most serious threat to the national security of the United States." By the time he had won a second term, President Bush not only understood the threat, but he had embraced it emotionally. As he frequently stated, he was determined to do everything possible to "keep the world's most dangerous technologies out of the hands of the world's most dangerous people."[1] His successor, President Barack Obama, also made preventing nuclear terrorism a priority, having read Nuclear Terrorism as a young senator who in 2005 accompanied Senator Richard

Dr. Graham Allison is the Douglas Dillon Professor of Government at Harvard Kennedy School.

Lugar on a congressional delegation to inspect Russian nuclear sites.[2]

Not surprisingly, the book attracted critics as well. The most common objection focused on what skeptics argued was an irresolvable contradiction between the core claims of "inevitable" and "preventable." If something is preventable, then it cannot be inevitable, they said.

My attempt to answer their point was proving largely ineffective, since for the most part, I just kept repeating the argument stated in the book. But fortunately, I was rescued by none other than Buffett himself. In making judgments about buying stocks, and even more in owning and running several reinsurance companies, Buffett had become a legendary oddsmaker. Those businesses had also forced him to think seriously about nuclear terrorism as one of what investors call "fat tail" risks. He had concluded that such an event was virtually inevitable and that the consequences would be devastating. Thus he prohibited his companies from writing insurance against nuclear terrorism.

The following two charts clarify Buffett's argument. Chart 1 demonstrates that if the probability of a successful nuclear terrorist attack in the year ahead is 10 percent, and if that condition persists for 50 years, the likelihood of nuclear terrorism occurring is almost 100 percent (99.5 percent to be precise).[3]

But as Chart 2 illustrates, if actions were taken to reduce that likelihood from 10 percent a year to 1 percent, the probability that in the next 50 years there is no successful nuclear terrorist incident rises from almost zero to 60.5 percent. These extrapolations are, as Buffett explains, simple probability calculations.[4]

Prior to publication, a number of referees pointed out that even if one agreed that the risks of nuclear terrorism were much greater than had been previously recognized, the policy community would ask: how likely is such an event, now? As one wag put it, what moves most Washingtonians are consequences that could happen on their watch. Even those who found Buffett's response analytically correct argued that it was too "academic" for many participants in the policy debate.

Thus at their urging, in the final published text of *Nuclear Terrorism* I offered my best judgment. Specifically, I wrote that on the trajectory we were following in 2004, absent significant additional preventive actions, the likelihood that terrorists would successfully explode a nuclear bomb somewhere in

Chart 1: Probability of Nuclear Terrorist Attack if Annual Odds are 10 percent.

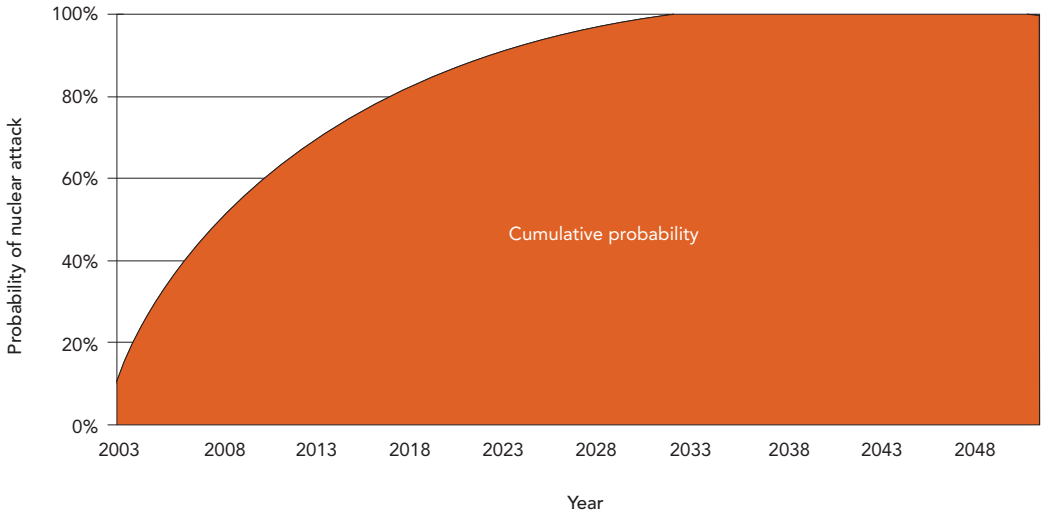
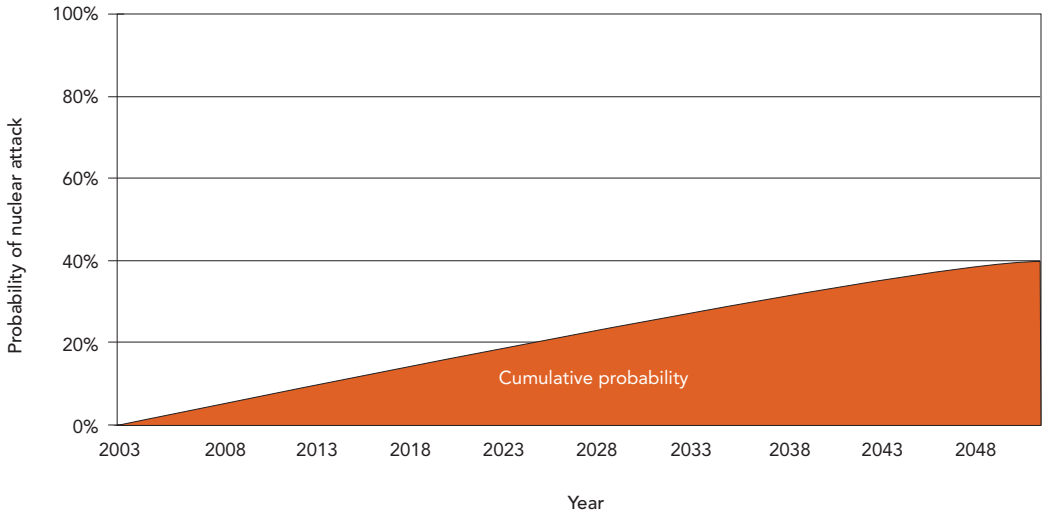


Chart 2: Probability of Nuclear Terrorist Attack if Annual Odds are 1 percent.



the world in the decade ahead was "more likely than not." As a leading advocate of what I call "betable propositions"—putting one's money where one's mouth is—I made a number of bets with colleagues who were more skeptical.[5] Operationalizing my estimate, I bet $51 of my money against $49 of theirs that before December 31, 2014 we would see an act of nuclear terrorism. Needless to say, I was happy to lose these bets.

With the benefit of hindsight, it is fair to ask whether my 2004 assessment of the risk was wrong. To begin to try to answer that question, it is necessary to start with candor about the larger question of which it is a component. The cosmic question is why there has been no mega-terrorist attack on the United States since September 11, 2001 when al-Qaeda operatives crashed commercial airliners into the World Trade Center and Pentagon.

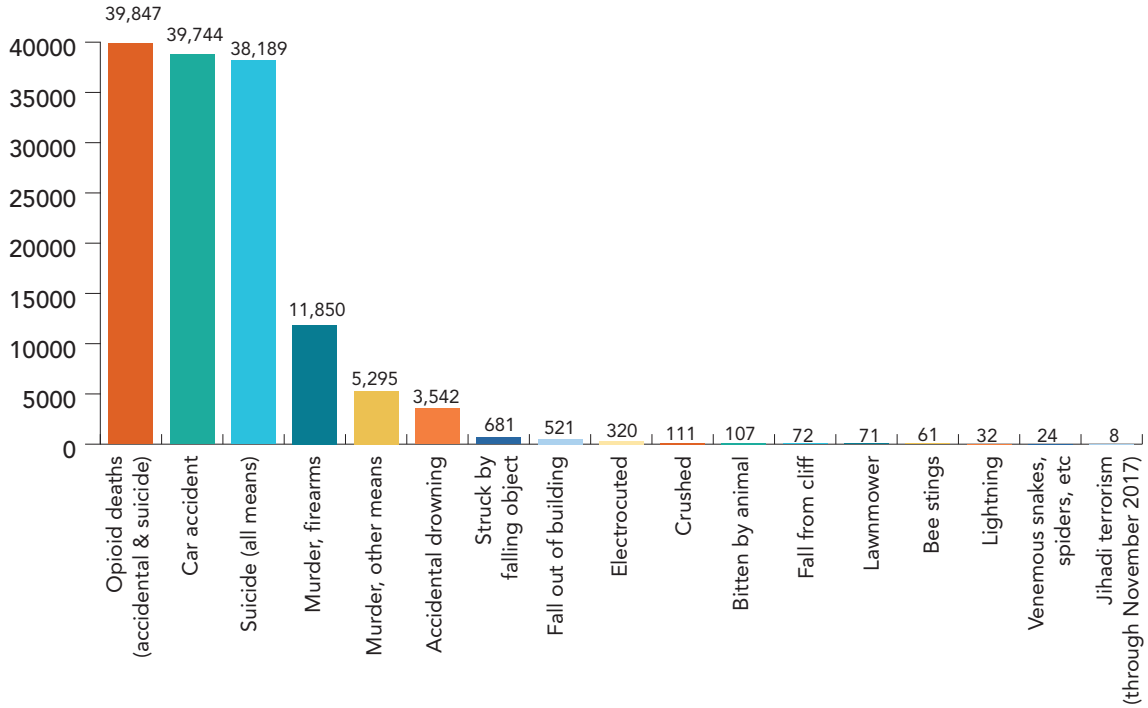
In the wake of that attack, anyone who had offered to bet that 16 years on there would have been no terrorist attack on the United States that killed more than 100 people would have been able to get 1000:1 odds. In each of the years since that attack, the annual threat assessment from the U.S. Intelligence Community (IC) has ranked terrorism as among the top three threats to the United States. Polls find that more than 80 percent of Americans expect another major terrorist attack in the near future.[6] Half of Americans expect that they or a member of their family will be killed by terrorists.[7]

How can we square these expectations with what has actually happened? Who or what has actually killed Americans here in the United States during the decade and a half since the al-Qaeda strike on 9/11? On the record, tree limbs and other falling objects have killed 100 times more Americans than terrorist attacks. As Chart 3 demonstrates, apart from old age and disease, the leading causes of death for Americans here at home have been opioid overdoses (40,000); car accidents (39,000); and suicide (38,000).[8]

Thus, to put it bluntly, it is hard to deny the gap between the expectations of the intelligence and policy analytic community who have been trying to understand terrorism and counter-terrorism, on the one hand, and the brute facts, on the other.

In attempting to understand the challenge of terrorism, analysts have used versions of Sherlock Holmes's framework of "MMO"—motive, means, and opportunity. Identify actors who have the motivation, means, and opportunity to commit an act of

Chart 3: Average Annual Deaths in the United States, 2005–15.



terrorism, and one has the suspect list. My modified version of Holmes includes an additional "O" for organizational capability. Individuals or groups motivated to take an action but lacking the organizational skills to use available means to exploit opportunities remain only potential risks.

Employing this MMOO framework to the challenge of terrorism since 9/11, what do we find? Potential perpetrators motivated to conduct terrorist attacks on the United States have multiplied beyond anyone's expectation in 2001. By invading and occupying Iraq and Afghanistan, and striking targets in many other countries with drones, the United States has created new enemies. In Iraq and Afghanistan, our counterinsurgency campaigns on behalf of one faction against others have given thousands of other people motives to seek revenge against us. In what the Bush Administration labeled the "Global War On Terrorism," U.S. forces have conducted attacks on the territory of at least seven Muslim-majority nations—killing individuals we labeled "terrorists," but also civilians who are known as collateral damage. These actions have provided fodder that extremists have used skillfully to recruit and motivate payback. Indeed, the Osama bin Laden dream to ignite a "clash of civilizations" between Muslims and what he called the "Jewish-Christian crusaders" has more credibility today than anyone could have imagined at the beginning of the century.

While post–9/11 security measures have made it more difficult to hijack a commercial airliner, the means by which to kill double, triple, and even quadruple digit numbers of people have also expanded. As the Orlando and Las Vegas shootings suggested, in many states in the United States, it is not that hard to buy an assault rifle and ammunition that will allow a shooter to fire 1,000 rounds in two minutes. And recent truck attacks by ISIL-inspired fighters in Nice, Barcelona, and New York demonstrate that terrorists recognize

that modern life offers them many means by which to carry out their attacks.[9] The internet has also expanded the availability of chemicals, deadly opioids like fentanyl, and even pathogens. Web-accessible information about how to make elementary bombs or acquire and use pathogens like anthrax has also increased.

Opportunities to kill hundreds or even thousands of Americans also abound. As military planners would put it, the United States offers a "target-rich" environment. Terrorists intent on killing large numbers could find them everywhere: from malls and movie theaters to sports stadiums and churches.

Organizational capability appears to have been terrorists' Achilles' heel. The planner of 9/11, Khalid Sheikh Mohammed, demonstrated extraordinary imagination and operational skills. Intelligence professionals gave his design and execution of the plan an "A." Fortunately, he has been one of the few. Advances in al-Qaeda's bombmaking appear to be traceable also to a single individual—Ibrahim al-Asiri. He developed the bombs for the failed underwear bomb plot in 2009 and cargo hold plot in 2010, as well as the laptop bomb that led the Trump Administration to temporarily ban laptops on flights.[10]

Terrorists have for the most part been "technically challenged." Should that factor change, the overall picture could also change dramatically overnight.

In sum, the question about why there has been no nuclear terrorist attack is one piece of the larger puzzle about why there has been no mega-terrorist attack of any kind. And the deeper question behind that is whether we in the analytic community have a good grasp on the fundamentals of this challenge. Truth be told, I register my doubts.

Nonetheless, I am not ready to conclude that my 2004 estimate of the odds of a nuclear terror attack was incorrect. And contrary to the claims of a number of critics, as a matter of statistics, the evidence of the past 13 years does not require me to do so. A brief aside on the logic of betting and odds will explain why. Imagine a coin that was slightly weighted so that it had a 51 percent chance of landing heads and 49 percent chance of tails. From a single toss of that coin that landed tails, what could one conclude? Statistically, the answer is—very little. Such a result would be expected to happen 49 out of every 100 times the coin was tossed. If we tossed the coin a second time, and again it landed tails, statisticians would again remind us that the chances of that occurring were 1 in 4. To conclude as a matter of statistics that my estimate was incorrect would take a lifetime of successive decades in which there was no successful nuclear attack.[11] Thus, I stand behind my assessment in 2004 that the odds of an attack in the next decade were greater than even. (As we all know, dozens of planned terrorist attacks have failed or been foiled—from the Christmas Day underwear bomber to the Times Square bombers.)

The issue this article addresses is whether in the past decade we have just beaten the odds, or whether actions we have taken have changed the odds for the better. To address that question, it is necessary to review the array of factors and actions that have reduced the risk of nuclear terrorism on the one hand, and those that have increased the risk on the other.

Consider, for example, what would likely have happened after 9/11 had Osama bin Laden and al-Qaeda been able to continue operating from their headquarters in Afghanistan. As the video bin Laden made after the attack demonstrated, he was thrilled by what Khalid Sheikh Mohammed's operation had achieved. He later called on all faithful Muslims to join the jihad and top 9/11. At the pinnacle of his pyramid of destruction was a mushroom cloud enveloping one of the great cities of the world. What prevented that first and foremost was a relentless counterterrorism campaign that

killed or captured most of al-Qaeda's leadership and left the others spending most of their time trying to survive rather than perfecting plots for future terrorist attacks. Destruction of their headquarters and training camps meant that thousands of individuals who would have been planning, training, and then conducting terrorist attacks never got their chance. On the other hand, the failure to stop North Korea from developing a nuclear arsenal, as well as the collapse of U.S.–Russian nuclear security cooperation, have created new significant risks.

Section II of this article reviews actions taken that have reduced the risk of nuclear terrorism. Section III reviews factors and actions that have increased these risks. A concluding section offers an updated assessment of the risks posed by nuclear terrorism from the perspective of year-end 2017. While applauding thousands of actions that have been taken by hundreds of thousands of individuals in the past 13 years to reduce these risks, reviewing all the pluses and all the minuses, my gut tells me that the chances of a successful nuclear terrorist attack in the decade that began in 2015—in effect, the second flip of the coin—are better than even. Specifically, I believe the odds of a successful nuclear terrorist attack somewhere in the world before the end of 2024 are 51 percent or higher. While giving thanks that terrorists have failed to achieve their deadliest ambitions, in my view that is not grounds for complacency, but rather a reason for redoubling our efforts.

I am aware that on an issue about which I am passionate, I may have slipped from analysis to advocacy. The central point is not whether the odds of a nuclear terrorist attack are 51 percent or 15 percent. Threat equals likelihood times consequences, and in this case, the consequences would be devastating. Since the costs of actions to reduce these risks are modest, prudent policymakers should focus on the feasible agenda of actions.

Factors and Actions That Have Reduced the Risk of Nuclear Terrorism

In the past decade, the United States and its international partners have taken literally thousands of specific actions that closed what had been open doors to terrorists acquiring a nuclear bomb, or nuclear materials from which they could have fashioned an improvised nuclear weapon. In terms of the MMOO framework, U.S. counterterrorism and counterproliferation actions have significantly diminished both the means and the opportunities.

On the counterterrorism front, the terrorist groups that sought to attack the United States with nuclear weapons have been decimated. Osama bin Laden, Khalid Sheikh Mohammed, and most of the operational talent behind 9/11 have been captured or killed. While Osama bin Laden's deputy, Zawahiri, succeeded him as head of al-Qaeda, and while several of the key operatives including Abdel Aziz al Masri, who led the organization's nuclear program, remain missing, the deadly pursuit of the entire roster of the organization by collaborative intelligence, Special Operations Forces, and drones has severely diminished al-Qaeda's ability to mount a nuclear terrorist attack.

Al-Qaeda's successor as the greatest terror threat to the United States, Islamic State of Iraq and the Levant (ISIL), has also suffered heavy losses in recent months. In 2014, ISIL acquired a broad swath of territory across Iraq and Syria—a safehaven in which it could train militants, plot attacks, and compile resources. While we know less about ISIL's efforts to acquire nuclear materials, the fact that the Belgian police discovered that ISIL agents involved in the 2015 terrorist attacks had surveillance footage of a Belgian nuclear research facility is suggestive.[12] Furthermore, its ideological centerpiece—an epic final battle with the West—would seem to require nuclear Armageddon. By wiping out its safehavens in Syria and Iraq, the United States and its partners have diminished ISIL's ability to organize a major effort to acquire nuclear weapons.

FACTORS AND ACTIONS THAT HAVE DECREASED THE RISK OF NUCLEAR TERRORISM

- Relentless U.S.–led campaign to destroy terrorists who sought to attack the United States.
- Development of defenses against terrorism to include the standup of fusion centers within the Federal Bureau of Investigation and the new Department of Homeland Security, and improvements to the Transportation Security Administration and border security.
- Multi-billion dollar increase in funding for intelligence groups targeting terrorism.
- Heightened public awareness of terrorist threat.
- U.S.–Russian nuclear security cooperation.
- U.S.–led Nuclear Security Summit process that created action-forcing deadlines.
- Complete removal of nuclear-weapons usable material from over a dozen countries
- More than 50 civilian research reactors shut down or converted from highly enriched uranium to low enriched uranium.
- Iran nuclear deal that halted Iran's nuclear advance.

FACTORS AND ACTIONS THAT HAVE INCREASED THE RISK OF NUCLEAR TERRORISM

- Inexorable advance of science and technology, diffusion of nuclear know-how.
- North Korea's growing nuclear stockpile, seen as a validation for rogue states that nukes = security.
- Metastasis of terrorists: AQ → ISIL → Affiliates →?
- U.S. airstrikes and special forces raids in seven Muslim-majority countries.
- Pakistan's growing nuclear arsenal and development of tactical nukes.
- Collapse of U.S.–Russia nuclear security cooperation after Russia's invasion of Ukraine in 2014.
- Erosion of confidence in the nonproliferation regime.
- Potential for large-scale reprocessing of plutonium in China and Japan.
- Growing possibility that the Trump Administration will let Iran escape the constraints on its nuclear ambitions.

In addition to these offensive counterterrorism efforts, the United States has taken extensive defensive actions to fortify the American homeland. An array of new agencies including the Department of Homeland Security, Transportation Security Administration, FBI Fusion Centers, and counterterrorism units in major state and local police forces now have tens of thousands of people working every day to keep Americans safe. The budget of the Central Intelligence Agency (CIA) and the 16 other agencies that comprise the IC have doubled since 9/11, most of that increase enhancing their ability to find and stop terrorists before they act.[13] Major upgrades in border and port security make terrorists' entry into the United States and smuggling of nuclear material or a weapon much more challenging. For example, 1,300 radiation detectors have been installed at ports nationwide since 9/11.[14] A major transformation of the FBI to expand its mission beyond fighting crime to also include counterterrorism, along with a three-fold increase in the FBI budget, has increased its capacity to detect and thwart terrorist efforts.[15] And across the entire society, a heightened public consciousness about the threat of terrorism that has created a culture of "see something, say something," and a readiness among

many citizens to follow the lead of courageous passengers on Flight 93 and "do something," have made the job of prospective terrorists more difficult.

On the nuclear security front, post–Cold War U.S.–Russia cooperation has been decisive in securing loose fissile material. At the end of the Cold War, 22,000 tactical nuclear weapons were scattered across 14 of the 15 newly independent states of the former Soviet Union. Moreover, 3,200 strategic nuclear weapons, most atop missiles that targeted American cities, remained stationed in Belarus, Kazakhstan, and Ukraine. Many of these weapons seemed fated to become "loose nukes."

In December 1991, as the Soviet Union was teetering on the edge of collapse, then Secretary of Defense Dick Cheney was asked on *Meet the Press* what would happen to these nuclear weapons. Cheney offered a fatalistic prediction: "If the Soviets do an excellent job at retaining control over their stockpile of nuclear weapons . . . and they are 99 percent successful, that would mean you could still have as many as 250 that they were not able to control."[16]

Thanks to the leadership of Senators Richard Lugar and Sam Nunn, Congress focused attention on this threat and provided funding for the Cooperative Threat Reduction program (CTR). This provided the means for the United States to work with Russia and these host nations to ensure that all tactical nuclear weapons were returned to Russia and firmly secured, and that the strategic nuclear weapons in Belarus, Kazakhstan, and Ukraine were eliminated. Twenty five-years on, not a single loose nuclear weapon has been discovered.

Dangerously, these cooperative U.S.–Russia initiatives to secure nuclear weapons and materials were suspended after Russia's 2014 invasion of Ukraine.[17] Fortunately, several other U.S.–Russia initiatives on nuclear terrorism remain intact. The Global Initiative to Combat Nuclear Terrorism, co-launched by Presidents Bush and Putin in 2006, encourages states to share best practices and build capacity to detect and respond to terrorist threats on their soils. Through the Proliferation Security Initiative, launched in 2003, the United States, Russia, and more than 100 other states cooperate to prevent the smuggling of WMDs and their delivery systems.[18] The 2005 Bratislava Initiative, spearheaded by Bush and Putin, bolstered physical security at Russian nuclear facilities.[19] In addition, the 2010 New START Treaty reduced the number of deployed United States and Russian nuclear warheads and delivery vehicles.

At the multilateral level, the most consequential nuclear security initiative of the past decade was the series of Nuclear Security Summits initiated by President Obama. During the course of his two terms, four summits gathered heads of state from more than 50 countries to spur commitments from these leaders to secure nuclear material. By focusing the minds of leaders on this threat and the steps they could take to address it, the Nuclear Security Summits created an effective action-forcing process. The agenda, the meetings, the deadlines, and the necessity to stand up and speak up all move governments to act. The success of this initiative has largely gone unnoticed—but it is worth pausing to consider what could have happened had the Summits never taken place.

In 1991, when the Soviet Union collapsed, 52 states had nuclear weapons–usable material. By 2009, that number had been reduced to 38. Between the first summit in 2010 and the final one in 2016, the number of states with nuclear-weapons material that could fuel a terrorist's bomb had been reduced to 24. In 2010, when the first Nuclear Security Summit was convened by President Obama, there were 15 nuclear bombs worth of weapons material in Ukraine at sites including Sevastopol and Kharkov. Thanks to the initiative, this threat was identified and a combination of inducements and pressure led then-Ukrainian President Viktor Yanukovych to act. In 2012, at the second Nuclear Security Summit

President Yanukovych announced that all nuclear weapons-usable material had been removed from Ukraine.[20] Had these materials remained where they were, what would have happened to these potential nuclear bombs when just two years later, government authority melted away after Russia invaded Crimea and destabilized Eastern Ukraine? The armed groups that seized government buildings would now have the means to make nuclear bombs. And one or another of the various splinter groups could even have decided to sell the core of a bomb to others in the black markets of the world.

In addition to risks of terrorists buying or stealing weapons-grade material, there is a further danger of terrorists attacking a nuclear plant in order to cause a Chernobyl- or Fukushima-like disaster. The master planner of the 9/11 attacks had considered crashing a jumbo jet into a nuclear power plant, such as Indian Point near New York City. Al-Qaeda's training manual lists nuclear plants as among the best targets for spreading fear in the United States. Thus additional work is required to improve security at these plants, including, for example, requiring armed guards at all sites that hold weapons-grade material or enough low-enriched fuel to cause a major release of radioactivity.

Another major success from the summits was the agreement by more than 100 nations to provide additional layers of protection for all nuclear material in their possession, including during storage, transport, and use. This Amendment to the Convention on the Physical Protection of Nuclear Material became legally binding in 2016. It updated the requirements of the original 1987 Convention, which obligated protection during international transport, but not during domestic storage and use.

Furthermore, since 2004, more than fifty civilian research reactors that had been fueled by highly-enriched uranium—that could also be used for weapons—have been either shut down or converted to run on low-enriched uranium, which is not weapons-usable.[21] Because civilian reactors are often less strictly guarded and monitored than military facilities, this is a significant development. Terrorists now have fewer targets from which to attempt to steal fissile material for a bomb.

Beyond the Summits, the Obama Administration's other major achievement on the counterproliferation front was to cut off pathways to a bomb for one of the world's leading state sponsors of terror. During its march over the previous decade to the point at which it was approaching a "break-out capability," Iran had crossed a dozen red lines. Thanks to an imaginative and determined negotiating strategy led by the United States, in 2015 the Permanent Five members of the Security Council and Germany concluded with Iran the Joint Comprehensive Plan of Action (JCPOA). The JCPOA verifiably interrupted all of Iran's major pathways to a weapon by preventing Iran from reprocessing plutonium or enriching uranium beyond 3.75 percent (weapons-grade uranium is enriched to 90 percent). Furthermore, by eliminating two-thirds of Iran's current centrifuges and 98 percent of its enriched-uranium stockpile, the agreement pushed Iran back at least a year from a bomb.[22] Though critics still complain that the JCPOA allows too much space for Iran to "cheat," the deal imposes the most intrusive verification and inspection regime ever negotiated. This inspection regime substantially reduces the likelihood that Iran either acquires nuclear weapons itself or sells nuclear material to terrorist groups.

Factors and Actions That Have Increased the Risk of Nuclear Terrorism

Despite these successes, there have also been numerous missed opportunities and structural shifts during the past 13 years that have increased the risk of nuclear terrorism. Obama's success in Iran is offset by his failure to stop North Korea's nuclear

advance. North Korea is today the world's leading candidate to become "Nukes 'R' Us." Long known in intelligence circles as "Missiles 'R' Us" for having sold and delivered missiles to Iran, Syria, Pakistan, and others, it has repeatedly demonstrated its willingness to "sell anything it has to anybody who has the cash to buy it," as former Secretary of Defense Robert Gates famously noted.[23] Indeed, anyone who doubts that North Korea would sell to others the wherewithal to make a nuclear bomb should pause and examine what they did in Syria. As we learned after Israel attacked and destroyed the Yongbyon-model reactor at al-Kibar in Syria in 2007, North Korea sold materials, designs, and expertise to help Syria build a plutonium-producing nuclear reactor.[24] By now that reactor would have produced enough plutonium for a dozen nuclear bombs.

Moreover, what price did North Korea pay for having proliferated nuclear-weapons technologies and materials? In 2006, after watching North Korea test its first nuclear device and fearing that it might do something this reckless, President Bush issued a solemn warning. Declaring that sale or transfer of any nuclear weapon or nuclear-weapons material and technologies would cross a bright red line, Bush warned that any sale that violated this prohibition would be held "fully accountable."[25] But after North Korea was found to have disregarded this warning, how did the United States respond? When Israel informed the Bush Administration that it had discovered this facility as the project was approaching completion, the United States not only failed to take military action itself to stop it, but urged Israel to take the issue to the United Nations. Just weeks after Israel disregarded U.S. advice and destroyed the reactor, the United States returned to the Six-Party Talks with North Korea. And less than a year later, President Bush gave the Kim regime a significant concession by removing it from the list of state sponsors of terrorism in return for inspections on and initial steps to dismantle the Yongbyon reactor—a deal that Pyongyang reneged on just six months later when it kicked out the inspectors and announced that it would resume reprocessing at the reactor.[26]

When *Nuclear Terrorism* appeared in 2004, North Korea had yet to conduct a nuclear test. Since then, it has conducted six nuclear tests, including one in September 2017 that produced a yield ten-times that of the Hiroshima bomb.[27] In Obama's two terms, Kim Jong Un and his father, Kim Jong Il, conducted 80 missile tests. In Trump's first year in office, Kim Jong Un has so far conducted 20 additional missile tests, including three ICBM tests.[28] Today, North Korea stands on the threshold of a credible nuclear threat to the U.S. homeland. If North Korea succeeds in completing its nuclear deterrent, leaders of other rogue states will certainly take note.

In Obama's two terms, Kim Jong Un and his father, Kim Jong Il, conducted 80 missile tests. In Trump's first year in office, Kim Jong Un has so far conducted 20 additional missile tests, including three ICBM tests. Today, North Korea stands on the threshold of a credible nuclear threat to the U.S. homeland.

As North Korea has continued violating UN injunctions to halt its nuclear and missile programs, the United States and its allies have ratcheted up

sanctions on the Kim regime. The United States and China now insist that the most severe sanctions ever are "biting" and that "maximum pressure" on North Korea will force the Kim regime to relent and comply in order to avoid collapse. Those who have been watching this issue for the past two decades have heard that hope before. Moreover, tightening sanctions give a cash-strapped regime greater incentives to turn to the nuclear black market.

The United States has warned Kim Jong Un that selling nuclear weapons or weapons-usable nuclear materials would cross an inviolable red line. But as noted above, President Bush drew this red line a decade ago for Kim's father—but to no effect. At this point, how credible will another threat from the United States to "punish" North Korea for selling nuclear weapons or material be? Indeed, our predicament today is even more difficult. If Kim Jong Un launches his next series of ICBM tests and the IC concludes that he has the capability to attack the American homeland, how credible will any U.S. threat to punish North Korea for anything short of a full-scale attack on South Korea or the United States be? As Kim's advisers will ask, if the United States is not prepared to act on its threat to prevent North Korea from acquiring the ability to strike the American homeland, why would they act if North Korea sold nuclear weapons to Iran?

Even if Trump succeeds in halting Kim's progress short of a credible ICBM threat to the U.S. homeland, which seems unlikely at this point, the threat of nuclear terrorism emanating from North Korea will continue to require a significant U.S. campaign to deter and prevent. Due to the inability of previous administrations to stop North Korea's progress earlier, a nuclear-armed North Korea, with the capacity and perhaps willingness to sell, will remain a major challenge not only for Trump but for his successors.

Another major long-term challenge is the relentless advance of science and technology and the accelerating diffusion of nuclear and radiological know-how. The proliferation of advanced manufacturing has made it easier to produce components needed for a bomb. For example, the A.Q. Khan nuclear black market network manufactured key parts for centrifuges in workshops in Malaysia.[29] Furthermore, the widespread availability of radiological material in medical and research settings has led to the recognition that it is simply a matter of when, not if, terrorists detonate a dirty bomb. This reminds us of one of the hardest truths about modern life: the same advances that enrich and prolong our lives also empower potential killers to achieve their deadly ambitions.

While those potential killers are not as cohesively organized as they were prior to 9/11 when al-Qaeda had a coordinated WMD effort, the terrorist threat has metastasized. Al-Qaeda morphed into ISIL and an array of affiliates like al-Shabaab in Somalia. These newer terrorist organizations will undoubtedly splinter further as a result of the loss of ISIL and al-Qaeda's main safehavens. But these groups have demonstrated a remarkable ability to find hosts in other fragile states around the globe, from Niger to Yemen, and even within more stable states, like Indonesia.

Furthermore, the widening scope of U.S. counterterrorism operations has continued to create new mutations. The United States has now conducted drone strikes and Special Forces raids in at least seven Muslim-majority countries: Afghanistan, Iraq, Libya, Pakistan, Somalia, Syria, and Yemen. Furthermore, with the Trump Administration's recent announcement that it will begin flying drone missions out of a new base in Niger, this number will likely rise to include at least Niger and Mali, along whose borders many terrorists operate.[30] Despite major efforts to avoid civilian casualties, many strikes have resulted in significant collateral damage, providing fodder for terrorist recruiters.[31] Thus, while U.S. counterterrorism operations have been immensely successful in hunting down high-level

militants, these efforts in each area must be weighed against the risk that operations could create more enemies than they kill.

The battle against Islamic extremist ideologies and their adherents will be a generational challenge. This is less a problem to be "fixed" than a condition that will have to be managed. It will require constant vigilance for as far as any eye can see. And as long as there are states that are unwilling or unable to suppress terrorists or expel them from their borders, they will find savehavens in which to continue. We should never forget that most of the planning and preparation for the 9/11 attack was done by an al-Qaeda cell in Hamburg, Germany. Moreover, while al-Qaeda's core has been decimated, its remaining leaders continue to find refuge in the nuclear-armed ticking time bomb called Pakistan.

While rarely featured in the American media, the India–Pakistan relationship continues to be one of the most dangerous dynamics in the world. Underlying the relationship is a deep-seated animosity and seemingly irresolvable dispute over the status of Kashmir, a mountainous region between the two countries claimed by both. Their armies continue to frequently exchange fire across the "Line of Control" that separates India-controlled Kashmir from Pakistan-controlled Kashmir. In addition to remnants of al-Qaeda and the Taliban, Pakistan also harbors (and has given active support to) terrorist groups like Lashkar-e-Taiba (LeT) and Jamaat-ud-Dawa (JuD) whose primary target is India.

There have been two major terrorist attacks emanating from Pakistan this century: on the Indian Parliament in Delhi in 2001, and in a dramatic attack on the Taj Hotel in Mumbai in 2008.

The India–Pakistan border is among the most heavily armed borders in the world; both countries possess nuclear weapons, including tactical nuclear weapons. The orange line snaking across the center of the image is a fenced floodlit border zone between India and Pakistan that is one of the few places on earth where an international boundary can be seen at night. (NASA)

The 2001 attack led to a massive military buildup and standoff along the Line of Control. This came just two years after the Kargil War in 1999, which was just a year after both states conducted nuclear weapons tests.

Both states have been building up capabilities to prepare for the next crisis. In the hopes of persuading the government of Pakistan to prevent further attacks by quasi-independent militant groups like LeT and JuD, India has unveiled a "Cold Start" doctrine that threatens to respond to future attacks with a quick, decisive incursion of ground troops into Pakistani territory. The concept is to punish Pakistan for any terrorist attacks and force it to take actions to dismantle terrorist organizations. The hope is that stopping the invasion after penetrating just 10–15 kilometers into Pakistan will avoid triggering nuclear retaliation. However, Pakistan has responded in a way that not only makes its threat of a limited nuclear response more credible; it makes the risk of loss of Pakistani nuclear weapons much higher. Pakistan has been aggressively developing and planning deployments of tactical nuclear weapons and short-range Nasr missiles near the Indian border.[32]

Nuclear security experts have rightfully sounded the alarm bells. Tactical nuclear weapons deployed to the frontlines pose a clear risk of theft by a rogue field commander or terrorist group. Moreover, the larger the number of weapons, the smaller and more transportable their size, and the wider their deployment, the higher the probability some will go missing.

India and Pakistan are both also actively producing fissile material and enlarging their nuclear arsenals. The Nuclear Threat Initiative's Nuclear Security Index ranks India and Pakistan among the four least secure countries in the world for nuclear material, along with Iran and North Korea.[33]

Perhaps most concerning for the global nuclear order, however, is what has happened in U.S.–Russia relations. The United States for two decades after the collapse of the Soviet Union provided assistance to Russia through the CTR, helping to secure weapons and fissile material before anything made its way to the black market. Three years ago, in the wake of Russia's invasion of Crimea and the Obama Administration's decision to punish Putin by imposing strong sanctions and cancelling cooperative programs between the Department of Energy and its Russian counterpart, these activities stopped. Thus, patterns of sharing and cooperation that had included exchange of technologies and practices for protecting nuclear weapons and materials, disposing of plutonium, and identifying potential terrorists halted.

Ninety percent of all the nuclear weapons in the world remain in the United States and Russia. Moscow's active participation in preventing theft and sale of nuclear weapons materials and sensitive technologies has made the difference between failure and success in preventing the spread of nuclear weapons. Whatever the state of relations between the two countries and their leaders, this reality cannot be denied. Technology has imposed on the two countries an inescapable partnership and absolute requirement for cooperation at least to a level that can avoid nuclear use, either against each other or by terrorists. In a phrase, however insufferable, Russia is America's inseparable Siamese twin.[34]

Trends in U.S.–China relations are also impacting the long-term nuclear order. As Thucydides taught us, when a rising power threatens to displace a ruling power, alarm bells should sound: danger ahead. This is the central argument of my recent book, *Destined for War: Can America and China Escape Thucydides's Trap?* China's economy has already overtaken the United States to become the largest economy in the world (measured by the metric that the CIA and the IMF agree is the best yardstick for comparing national economies).[35] At the 19th Party Congress in October 2017, President Xi Jinping reiterated China's determination to build a military

commensurate with China's economic power that can, in his words, "fight and win." China has long maintained a "minimum deterrent" posture, with only a few hundred nuclear weapons (as opposed to several thousand for the United States and Russia). However, along with the rest of its military, China is strengthening this arsenal.

In addition, China has the fastest growing nuclear power industry in the world, with plans to install more than 100 gigawatts of nuclear power by 2030. As part of this effort, China plans to reprocess spent fuel into plutonium fuel for nuclear reactors.[36] Furthermore, Japan, which already has a huge stockpile of plutonium (enough for 1,300 nuclear weapons), plans to add to this stockpile by reprocessing spent fuel at its long-delayed Rokkasho plant.[37] As plutonium is produced, transported, and used on an industrial scale, the risks of theft increase.

Together these developments have been eroding confidence in the nonproliferation regime. Widespread recognition that North Korea is not going to denuclearize and the prospect that its ICBMs could soon threaten the United States are stimulating debate in South Korea and Japan about the reliability of U.S.–extended deterrence commitments. Sixty percent of South Koreans now support development of their own independent nuclear deterrent.[38] With the scars of Hiroshima, the Japanese public has a deep nuclear neuralgia. But their recently reelected prime minister, Shinzo Abe, is determined to amend the pacifist constitution in order to rebuild a Japanese military commensurate with its economic standing. As Henry Kissinger has been warning: "As this [North Korean] threat compounds, the incentive for countries like Vietnam, South Korea and Japan to defend themselves with their own nuclear weapons will grow dramatically."[39]

On the Iranian front, President Trump has raised doubts about the future of the JCPOA constraints on Iran's nuclear program. During his speech to the UN General Assembly in September 2017, Trump called the Iran deal "one of the worst and most one-sided transactions the United States has ever entered into" and "an embarrassment to the United States."[40] In October, he took the first step toward burying the agreement by refusing to certify that Iran has been complying with the deal. If Congress takes the next step and reimposes sanctions on Iran's nuclear program, this violation of U.S. requirements under the deal would free Iran from the constraints the agreement imposes on its nuclear activity, and we could see it moving again towards a nuclear bomb. Alarmed by Iran's earlier efforts, Saudi Arabia developed plans for a nuclear energy program that would provide the infrastructure for its own weapons program. It has so far been unwilling to follow in the footsteps of its neighbor the United Arab Emirates (UAE) in pledging not to build an indigenous nuclear fuel cycle. A full fuel cycle to enrich uranium and reprocess plutonium would also provide the critical infrastructure for a nuclear weapons program. While the Trump Administration has said that a Saudi equivalent of the UAE agreement would be "desired," it has not insisted that this would be a requirement for U.S. support.[41] If the Saudis develop an indigenous nuclear fuel cycle and the deal constraining Iran's nuclear program falls apart, we should expect to see an arms race in the world's most volatile region in which Israel, and perhaps others, will be tempted to act before the Middle East becomes a nuclear tinderbox.

Outlook

Preventive actions taken since 2004, both in counterterrorism and in counterproliferation, have been extraordinary. From the decimation of al-Qaeda to the Iran Deal and the Nuclear Security Summits, difficult actions taken by courageous and hard-working Americans and others have prevented the future we feared. For all of these successes, however, there have been a matching number of failures and structural shifts that are increasing the risk of successful

mega-terrorist attacks. To put it metaphorically, while there can be no doubt that we have been running faster, we have also been falling further behind.

Attempting to weigh both pluses and minuses to make a net assessment, I stand by my 2004 conclusion. I still believe that the chance of an attack during the next decade is slightly greater than even. But there is a lengthy agenda of actions that the United States and other nations could take today to reduce this risk and even reverse trend lines moving in the wrong direction.

Nuclear Terrorism outlined a strategic framework organized around "three no's": no loose nukes, no new nascent nukes, and no new nuclear weapons states. On the first, while there is more work to be done, U.S.–Russian cooperation, the Nuclear Security Summits, and related efforts deserve credit for making significant headway. On the second and third, the record earned a lower grade. While the Iran Deal prevented Iran from becoming a new nuclear weapons state, it came close to legitimizing its nascent nuclear weapons capability. And North Korea sped right through a series of red lines to become an operational, if diplomatically unrecognized nuclear weapons state.

Taking the three no's as a framework, we can consider future actions that build on the success of the past 13 years to address some of the missed opportunities and structural barriers. There are three immediate actions that the Trump Administration should take.

First, in order to prevent loose nukes, it is imperative that the administration revive nuclear cooperation with Russia. This should include restoring the High-Level Russian-American Presidential Commission working group on nuclear energy and security, as well as cooperation under the CTR, especially between the two countries' nuclear weapons labs. In addition, the United States and Russia should look to bolster the Global Initiative to Combat Nuclear Terrorism, which currently focuses primarily on theoretical responses to attacks but could be utilized more for prevention. And U.S.–Russian intelligence cooperation in countering proliferation and terrorism, while always complex and tricky, should be deepened—even as the two nations struggle against each other on many other fronts.

The United States must oppose Russia in places where their interests are opposed, such as Ukraine. The United States cannot let Russian interference in the 2016 election go unpunished, or fail to find ways to prevent Russia from interfering in future elections. But the two nations should remember that even in the deadliest days of the Cold War, we seized opportunities to cooperate where vital interests converged. Most importantly, as Ronald Reagan repeatedly reminded us, "a nuclear war cannot be won and must never be fought."[42] Avoiding a general nuclear war of which the United States and Russia would be the first victims is an absolute requirement for surviving to have the opportunity to do anything else. After that, the clearest area of common interest is preventing nuclear terrorism. U.S.–Russia cooperation can advance both nations' goals not only on the nuclear security front, but also in the wars against ISIL and al-Qaeda. The difference between a relationship in which the Americans and Russians are sharing intelligence, and one in which they are withholding it, directly impacts Washington's ability to prevent terrorist attacks here at home. Bostonians saw a deadly example of this in 2013 when the two Tsarnaev brothers from Chechnya exploded pressure-cooker bombs at the finish line of the Boston Marathon. After-action reviews found that Russian security services had previously tipped off their American counterparts about one of the individuals, but that the information had been discounted because of the distrust among the parties.

Second, despite Trump's desire to pull out of the JCPOA, it is imperative that he find ways to keep its constraints on Iran. If the consequence of whatever

he does is to free Iran from the strict limits on its nuclear ambitions, historians will judge him harshly. Fortunately, Trump's October 2017 refusal to certify Iran's compliance with the JCPOA will have no operational consequences unless Congress reimposes sanctions. Whatever else the Iran agreement did not do, it extended Iran's breakout time to a year, and thus prevented it from producing fissile material (and in turn, from giving such material to terrorists). It also imposed the most intrusive monitoring and inspection system ever implemented. While Iran's hostile regime continues to take actions that harm U.S. interests, like sponsoring terror groups including Hezbollah, if we pause to think what a nuclear-armed Iran could be doing, our overriding interest in preventing that should be obvious.

Third, the Trump Administration must develop a coherent strategy for deterring North Korea from selling nuclear technology. While there is a real possibility that Trump decides to attack (20–25 percent in my best estimate), the most likely outcome of the current standoff is that Kim wins. He completes the tests he needs for a credible ICBM, forcing the United States to move to a posture of deterrence, defense, and containment. This would mean trying to deter North Korea from any use of nuclear weapons by threatening to erase North Korea from the map if it were to attack the United States or its allies; defending against its nuclear threat by deploying layers of missile defense; and containing the regime and encouraging its internal contradictions to hollow it out as we did in the Cold War against the Soviet Union.[43] But this will leave us for some years to come with the question of how to prevent Kim from selling nuclear weapons or materials to terrorists. The United States and its international partners will bolster monitoring of shipping in and out of North Korea and seek to persuade others to deny North Korean aircraft overflight rights so that it cannot transport weapons to potential buyers. We should also expect the Trump Administration to communicate to Kim a clear message—if any nuclear bomb of North Korean origin were to explode on American soil or that of an American ally, the United States will respond as though North Korea itself had hit the United States with a nuclear-tipped ICBM. Despite these and other best efforts, however, the question will remain: in the aftermath of a failure to prevent Kim from developing the capability to attack the American homeland, what other threat for actions short of an attack on the United States or our allies will he believe?

In addition to these short-term steps, President Trump should embrace three long-term initiatives that he could pass to his successor. First, the United States should find a way to institutionalize the Nuclear Security Summit process. One of the most important elements of combatting nuclear terrorism is making it a top national security priority. By convening heads of state on a biannual basis, the Nuclear Security Summits raised awareness of this threat, galvanized high-level attention to actions nations could take to reduce risks, and spurred real commitments. There is much more work to be done in further reducing the number of states with nuclear weapons materials, securing loose fissile material, and securing civilian nuclear programs.

Second, the United States must continue to invest in new technologies to enhance our ability to detect and prevent the smuggling of nuclear materials. For example, advances in high-energy particle physics provide hope for improving port and border monitoring and security. These include, for example, muon detectors, which utilize the high-energy particles from cosmic rays to detect openings in structures. Using muon detectors, archeologists recently discovered, for the first time since the 1800s, a new room in the Great Pyramid of Giza.[44] Los Alamos National Laboratory and Decision Sciences are working on muon detectors that can identify nuclear materials concealed in shipping containers, with one detector already deployed in the Bahamas.[45] Technology offers

our best hope for managing the tension between our need for security and the flow of travelers and goods in a globalized world.

Finally, and perhaps most ambitiously, the Trump Administration should address the geopolitical conflict that fuels nuclear danger in South Asia. The growing stockpiles of fissile material in India and Pakistan, combined with lax nuclear security procedures, have created a serious and growing risk of loose nuclear material or weapons. The United States should work with its international partners—especially China, which is one of Pakistan's closest patrons—not just to improve physical security, security culture, and border security, but also to deal with underlying issues. While direct nuclear security cooperation between India and Pakistan is perhaps too much to hope for, parallel efforts by the United States in India and China in Pakistan could help to reduce these risks. And increased cooperation on these issues would help the United States and China manage the larger Thucydidean tension between the two countries.

Confronting what *Nuclear Terrorism*'s subtitle called "the ultimate preventable catastrophe," we cannot continue to count on beating the odds. A decent respect for civilization as we know it compels us to do everything we can to change them. Actions taken during the past 13 years have made a significant difference. Osama bin Laden did not die a natural death. But we need a new surge of imagination and sustained commitment by America's brightest strategic and scientific minds to address the multiple dimensions of this most complex challenge. If we pause and reflect on what our lives will be like the day after a great city in the world is devastated by a single terrorist nuclear bomb, we can do no less. PRISM

Notes

[1] George W. Bush, "Address to Citadel Cadets," (speech, Charleston, South Carolina, December 11, 2001), available at <http://www.citadel.edu/root/presbush01>.

[2] Jeff Zeleny, "A foreign classroom for junior senator," *Chicago Tribune*, September 23, 2005, available at <http://www.chicagotribune.com/news/nationworld/chi-0509230360sep23-story.html>.

[3] Created by Belfer Center researchers, December 2003.

[4] Ibid.

[5] See further discussion of betting in Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis*, 1st edition (Boston: Little, Brown, 1971).

[6] Scott Clement and Juliet Eilperin, "Americans more fearful of a major terror attack in the U.S., poll finds," *Washington Post*, November 20, 2015, available at <https://www.washingtonpost.com/politics/americans-more-fearful-of-a-major-terror-attack-in-the-us-poll-finds/2015/11/20/ec6310ca-8f9a-11e5-ae1f-af46b7df8483_story.html?utm_term=.3c2f69e99887>.

[7] Peter Eavis, "There's a Disconnect in Americans' Worry About Terrorism," *New York Times*, June 15, 2016, available at <https://www.nytimes.com/2016/06/16/upshot/theres-a-disconnect-in-americans-worry-about-terrorism.html>.

[8] Created by Belfer Center researchers, November 2017.

[9] "Terrorist Attacks by Vehicle Fast Facts," CNN, November 6, 2017, available at <www.cnn.com/2017/05/03/world/terrorist-attacks-by-vehicle-fast-facts/index.html>.

[10] Howard Blum, "What Trump Really Told Kislyak After Comey Was Canned," Vanity Fair, November 22, 2017, available at <https://www.vanityfair.com/news/2017/11/trump-intel-slip>; "Profile: Al-Qaeda 'bomb maker' Ibrahim al-Asiri," BBC, July 4, 2014, available at <http://www.bbc.com/news/world-middle-east-11662143>.

[11] For an analogous demonstration from the world of financial investments, ask: how many years of above average performance would be required to conclude that a particular star investor had a 60% chance of being right in picking which stocks to buy? See Victor Haghani and Richard Dewey, "Rational Decision-Making under Uncertainty: Observed Betting Patterns on a Biased Coin," SSRN, (October 19, 2016), available at <https://ssrn.com/abstract=2856963>.

[12] Patrick Malone and R. Jeffrey Smith, "A terrorist group's plot to create a radioactive 'dirty bomb'," Center for Public Integrity, February 29, 2016, available at <https://www.publicintegrity.org/2016/02/29/19376/terrorist-group-s-plot-create-radioactive-dirty-bomb>.

[13] Marshall C. Erwin and Amy Belasco, "Intelligence Spending and Appropriations: Issues for Congress," Congressional Research Service, September

18, 2013, available at <https://fas.org/sgp/crs/intel/R42061.pdf>.

[14] "Radiation Detectors at U.S. Ports of Entry Now Operate More Effectively, Efficiently," Pacific Northwest National Laboratory, News Release, January 4, 2016, available at <https://www.pnnl.gov/news/release.aspx?id=4245>.

[15] Steven Brill, "Is America Any Safer?" *The Atlantic*, September 2016, available at <https://www.theatlantic.com/magazine/archive/2016/09/are-we-any-safer/492761/>.

[16] Andrew Rosenthal, "SOVIET DISARRAY; U.S. Fears Spread of Soviet Nuclear Weapons," *New York Times*, December 16, 1991, available at <http://www.nytimes.com/1991/12/16/world/soviet-disarray-us-fears-spread-of-soviet-nuclear-weapons.html>.

[17] Matthew Bunn, "Rebuilding U.S.-Russian Nuclear Security Cooperation," *Nuclear Security Matters*, January 22, 2015, available at <https://www.belfercenter.org/publication/rebuilding-us-russian-nuclear-security-cooperation>.

[18] Susan J. Koch, "Proliferation Security Initiative: Origins and Evolution," Center for the Study of Weapons of Mass Destruction Occasional Paper, No. 9 (Washington, DC: National Defense University Press, June 2012), available at <http://wmdcenter.ndu.edu/Portals/97/Documents/Publications/Occasional%20Papers/09_Proliferation%20Security%20Initiative.pdf>.

[19] "U.S. And Russia Complete Nuclear Security Upgrades Under Bratislava Initiative," U.S. Department of Energy, December 23, 2008, available at <https://energy.gov/articles/us-and-russia-complete-nuclear-security-upgrades-under-bratislava-initiative>.

[20] The White House, "FACT SHEET: Ukraine Highly Enriched Uranium Removal," Press Release, March 27, 2012, available at <https://obamawhitehouse.archives.gov/the-press-office/2012/03/27/fact-sheet-ukraine-highly-enriched-uranium-removal>.

[21] National Academies of Sciences, Engineering, and Medicine, *Reducing the Use of Highly Enriched Uranium in Civilian Research Reactors* (Washington, DC: The National Academies Press, 2016), available at <https://www.nap.edu/catalog/21818/reducing-the-use-of-highly-enriched-uranium-in-civilian-research-reactors>.

[22] Gary Samore, "The Iran Nuclear Deal: A Definitive Guide," Belfer Center for Science and International Affairs, Harvard Kennedy School, August 3, 2015, available at <https://www.belfercenter.org/publication/iran-nuclear-deal-definitive-guide>.

[23] Robert M. Gates, "Strengthening Security Partnerships in the Asia-Pacific: Q&A," (presentation, Singapore, June 5, 2010), availbale at <https://www.iiss.org/en/events/shangri-la-dialogue/archive/shangri-la-dialogue-2010-0a26/first-plenary-session-722b/strengthening-security-partnerships-in-the-asia-pacific-qa-2d31>.

[24] "Background Briefing with Senior U.S. Officials on Syria's Covert Nuclear Reactor and North Korea's Involvement," Office of the Director of National Intelligence, April 24, 2008, available at <https://fas.org/irp/news/2008/04/odni042408.pdf>.

[25] Mark Mazzetti and David E. Sanger, "Israeli Raid on Syria Fuels Debate on Weapons," *New York Times*, September 22, 2007, available at <http://www.nytimes.com/2007/09/22/world/middleeast/22weapons.html>.

[26] See Victor Cha, *The Impossible State: North Korea, Past and Future* (New York: HarperCollins, 2012), 269–73.

[27] "North Korean Nuke Test Put at 160 kilotons as Ishiba Urges Debate on Deploying U.S. Atomic Bombs," *Japan Times*, September 6, 2017, available at <https://www.japantimes.co.jp/news/2017/09/06/national/north-korean-nuke-test-put-160-kilotons-ishiba-urges-debate-deploying-u-s-atomic-bombs/>.

[28] James Martin Center for Nonproliferation Studies, "The CNS North Korea Missile Test Database," Nuclear Threat Initiative, last updated November 30, 2017, available at <http://www.nti.org/analysis/articles/cns-north-korea-missile-test-database/?utm_source=educator-email&utm_campaign=Educator%20Email&utm_content=north%20korea%20database>.

[29] Michael Lauffer, "A.Q. Khan Nuclear Chronology," Carnegie Endowment for International Peace, September 7, 2005, available at <http://carnegieendowment.org/2005/09/07/a.-q.-khan-nuclear-chronology-pub-17420>.

[30] Helene Cooper and Eric Schmitt, "Niger Approves Armed U.S. Drone Flights, Expanding Pentagon's Role in Africa," New York Times, November 30, 2017, availbale at <https://www.nytimes.com/2017/11/30/us/politics/pentagon-niger-drones.html>.

[31] Azmat Khan and Anand Gopal, "The Uncounted," *New York Times Magazine*, November 16, 2017, available at <https://www.nytimes.com/interactive/2017/11/16/magazine/uncounted-civilian-casualties-iraq-airstrikes.html>.

[32] George Perkovich and Toby Dalton, *Not War, Not Peace? Motivating Pakistan to Prevent Cross-Border Terrorism* (New Delhi: Oxford University Press, 2016), 73–97.

[33] Nuclear Threat Initiative, *Nuclear Security Index: Building a Framework for Assurance, Accountability, and Action*, 3rd Edition (Nuclear Threat Initiative, 2016), available at <http://ntiindex.org/wp-content/uploads/2013/12/NTI_2016-Index_FINAL.pdf>.

[34] Graham Allison, "America and Russia: Back to Basics," *National Interest*, August 14, 2017, available at <http://nationalinterest.org/feature/america-russia-back-basics-21901>.

[35] Graham Allison, *Destined for War: Can America and China Escape Thucydides's Trap?* (New York: Houghton Mifflin Harcourt, 2017), 10–12.

[36] Matthew Bunn, Hui Zhang, and Li Kang, "The Cost of Reprocessing in China," Belfer Center for Science and International Affairs, Harvard Kennedy School, January 2016, available at <https://www.belfercenter.org/publication/cost-reprocessing-china>.

[37] James M. Acton, "Time for a Nuclear Intervention with Japan," *Wall Street Journal*, May 15, 2017, available at <https://www.wsj.com/articles/time-for-a-nuclear-intervention-with-japan-1494866950>.

[38] Michelle Ye Hee Lee, "More than ever, South Koreans want their own nuclear weapons," *Washington Post*, September 13, 2017, available at <https://www.washingtonpost.com/news/worldviews/wp/2017/09/13/most-south-koreans-dont-think-the-north-will-start-a-war-but-they-still-want-their-own-nuclear-weapons/?utm_term=.c565c1612dbe>.

[39] Henry Kissinger, "How to Resolve the North Korea Crisis," *Wall Street Journal*, August 11, 2017, available at <https://www.wsj.com/articles/how-to-resolve-the-north-korea-crisis-1502489292>.

[40] Morgan Chalfant, "Trump: Iran nuclear deal an 'embarrassment'," *The Hill*, September 19, 2017, available at <http://thehill.com/homenews/administration/351323-trump-iran-nuclear-deal-an-embarrassment>.

[41] Isaac Arnsdorf, "White House May Share Nuclear Power Technology With Saudi Arabia," ProPublica, November 29, 2017, available at <https://www.propublica.org/article/white-house-may-share-nuclear-power-technology-with-saudi-arabia>.

[42] Ronald Reagan, "Address Before a Joint Session of the Congress on the State of the Union," (speech, Washington, DC, January 25, 1984), available at <http://www.presidency.ucsb.edu/ws/?pid=40205>.

[43] Graham Allison, "Will Trump and Xi 'Solve' North Korea?" *Politico*, November 8, 2017, available at <https://www.politico.com/magazine/story/2017/11/08/donald-trump-north-korea-china-xi-jinping-215804>.

[44] Daniela Hernandez, "The Great Pyramid of Giza Gives Up a Secret," *Wall Street Journal*, November 2, 2017, available at <https://www.wsj.com/articles/the-great-pyramid-of-giza-gives-up-a-secret-1509624000>.

[45] Lisa Grossman, "New Muon Detector Could Find Hidden Nukes," *Wired*, July 1, 2010, availbale at <https://www.wired.com/2010/07/muon-detector/>; Necia Grant Cooper, "Muon Vision for U.S. National Security," *National Security Science*, December 2016, available at <http://www.lanl.gov/discover/publications/national-security-science/2016-december/_assets/docs/NSS-dec2016_muon-vision-for-us-national-security.pdf>,

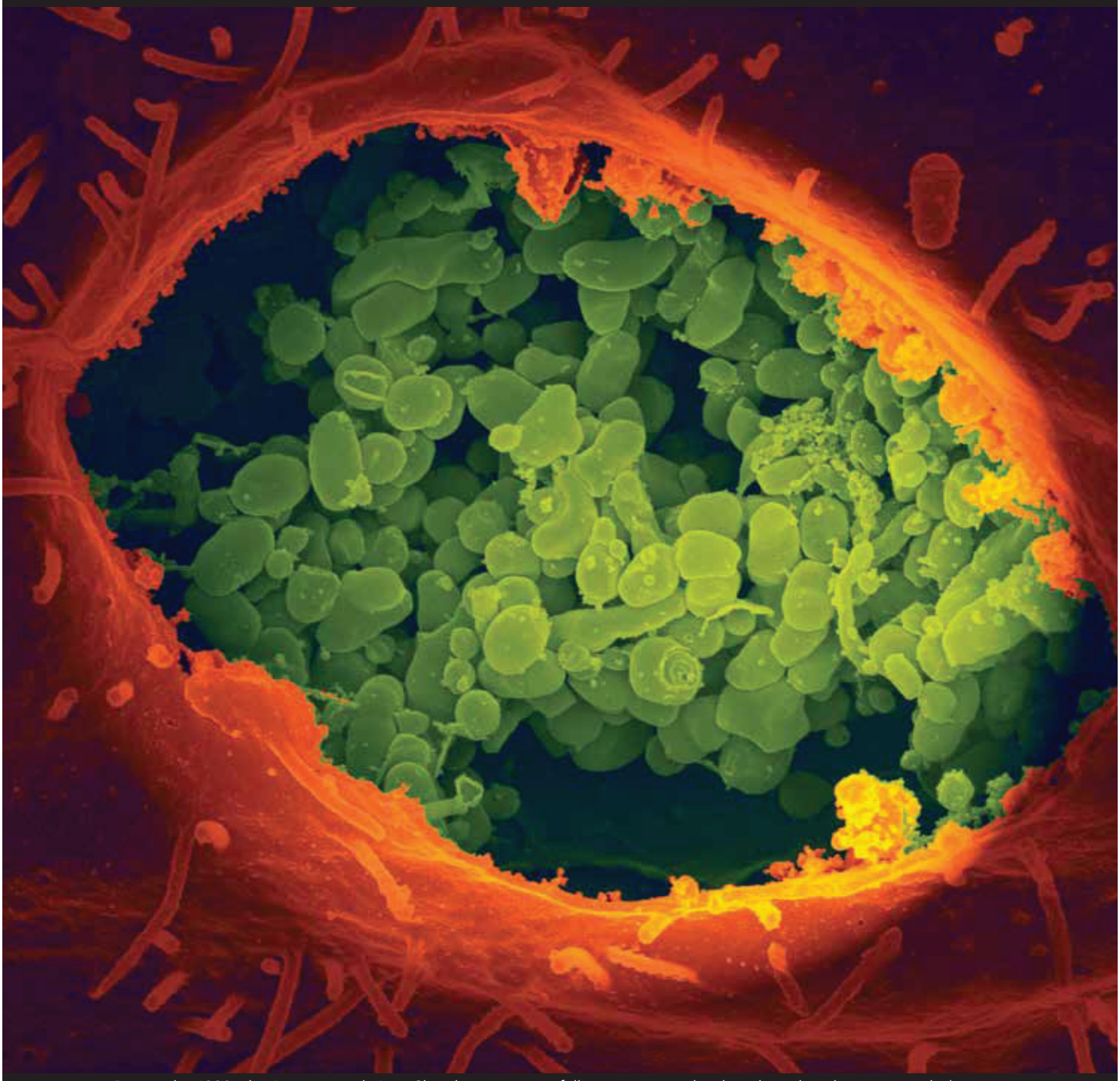
Photos

Page 2: iStock photo ID:884776124.

Page 14: ISS Crew Earth Observations Experiment and Image Science & Analysis Laboratory, Johnson Space Center. Caption by M. Justin Wilkingson, Texas State University, Jacobs Contract at NASA-JSC.

Acknowledgements

The author would like to thank Mr. William Ossoff for his exceptional research assistance, and Mr. Matthew Bunn, Mr. William Tobey, and Mr. Rolf Mowatt-Larssen for their thoughtful review of early drafts of this article.



During the 1990s the Japanese cult Aum Shinrikyo unsuccessfully experimented with anthrax, botulinum toxin, cholera, Ebola, and Q fever. (Image of Coxiella burnetti/ National Institute of Allergy and Infectious Diseases)

WMD Terrorism
The Once and Future Threat

By Gary Ackerman and Michelle Jacome

The specter of terrorists and other violent non-state actors acquiring weapons of mass destruction is perhaps an even greater concern than acquisition of weapons of mass destruction (WMD) by states. Given how terrorists periodically target civilians on a large-scale, usually lack a return address, and generally fail to subscribe to traditional notions of deterrence, it is not surprising that terrorists are sometimes portrayed as Bondian supervillians capable of casually constructing doomsday plots. This over-magnification, however, ignores the hurdles inherent in such malignant enterprises. Despite clear interest on the part of some non-state adversaries, a true WMD is at present likely out of their reach in all but a select set of scenarios. Changes in technology, however, could augur a dramatic shift in the WMD terrorism threat picture.

Important Distinctions

Weapons of mass destruction are typically understood to encompass chemical, biological, radiological, and nuclear (CBRN) weapons. Not all CBRN weapons, though, constitute WMD. This distinction is especially important in the case of non-state actors, since such actors often operate under severe resource constraints and are far more likely to plan or implement smaller-scale chemical, biological, or radiological attacks that fall below the WMD threshold. These smaller scale attacks might very well be disruptive and psychologically potent, but would not yield the casualty levels or physical destruction generally associated with a WMD. When we speak of the threat of terrorists and other violent non-state actors (VNSAs) using WMD, we imply CBRN weapons that, if used, would inflict catastrophic casualties, widespread social disruption, or devastating economic consequences beyond those resulting from all but the largest conventional attacks.[1] By this definition, only nuclear weapons are unequivocally WMD; for chemical, biological, and radiological weapons the precise amount, nature, and sophistication of specific attacks determine whether or not they meet the WMD threshold. It is thus important to note the significant differences in use and deployment between chemical, biological, radiological, and nuclear weapons. For example, the motivations

Dr. Gary Ackerman is an Associate Professor at the College of Emergency Preparedness, Homeland Security and Cybersecurity at the University at Albany. He is also the founding Director of the University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism (START) Unconventional Weapons and Technology Division. Ms. Michelle Jacome is the Deputy Director of START.

behind and capabilities required for the use of a nuclear weapon, considered a "low probability, high consequence" event, are wildly different than an attack employing toxic chemicals.[2]

Along these lines, a second salient distinction emerges—between a harm agent and a weapon. A weapon requires the pairing of a harm agent with a delivery system; this can be termed "weaponization." The scale of the harm from toxic chemicals, pathogenic microbes, and ionizing radiation is almost wholly dependent on the efficiency with which the harm agent is delivered to the intended target(s). Delivery systems can range from the decidedly crude (the use of sharpened umbrella points to poke holes in plastic bags filled with sarin nerve agent by the Japanese Aum Shinrikyo cult in 1995) to the extremely sophisticated (the M34 cluster bomb, a U.S. Army munition designed to cover a broad area with sarin). The distinction between agent and weapon is less important in the context of state-level WMD programs since countries rarely invest in the production of a CBRN harm agent without simultaneously developing an effective means of delivery, as seen in the recent parallel development of North Korea's nuclear and intercontinental ballistic missile programs. For non-state actors, the delivery mechanism often presents technical obstacles and resource requirements above and beyond those associated with the harm agent itself. A terrorist might successfully acquire a harmful radioisotope like cesium-137 or a pathogen like *bacillus anthracis*, but this does not necessarily mean that the terrorist can deliver it to a target with enough efficiency to inflict damage meeting the WMD threshold.

Terrorists and other VNSAs attempt to acquire CBRN or WMD capabilities for a number of reasons.[3] Motives might include not only their inherent capacity to inflict massive numbers of casualties, but also such operational objectives as long-term area denial, or the relative ease of covert delivery. The acquisition and use of WMD might also boost the status of the perpetrator, if not among its external constituency, then possibly among intra-organizational and inter-organizational rivals. A non-state actor's ideological or psychological proclivities may drive it to pursue WMD, as was the case of the Aum Shinrikyo cult whose leader, Shoko Asahara, displayed an almost fetishistic affinity for WMD; or Americans Denys Ray Hughes and Thomas Leahy, who were fascinated by poisons of all types. One of the key attractions of CBRN weapons as agents of terror for VNSAs is their dramatic psychological impact on targeted societies, which derives at least partly, from a combination of their intangibility, invasiveness, latent effects (as is the case of many CBR weapons), and unfamiliarity among average citizens.

Harm Agents and Weapons

Despite much hype and fear, there has never been an unequivocal WMD attack by a VNSA. The closest cases include Aum Shinrikyo's dispersal of sarin on the Tokyo subway in March 1995 (that killed 12 and injured more than 1,000), the possible sabotage of the Union Carbide chemical plant in Bhopal, India in 1984 (that led to several thousand deaths from exposure to methyl isocyanate), and a 1996 poisoning by the Khmer Rouge in Cambodia (that led to hundreds of casualties). In all of these cases, there is doubt as to either the intentions of the perpetrators or the number of casualties caused.

The absence of WMD attacks does not mean that VNSAs have not attempted to obtain or use CBRN. The University of Maryland, through its Profiles of Incidents Involving CBRN by Non-state Actors (POICN) Database, has recorded more than 517 cases of pursuit or attempted use of CBRN weapons by VNSAs since 1990, many of which are believed to have been attempts to deploy WMD-scale attacks. The breakdown of agents used or planned for use is depicted in Table 1.[4]

TABLE 1: Agents Used or Planned for Use, 1996–2016.	
Agent Type	# of Events
Biological	107
Chemical	400
Radiological	55
Nuclear	18
Total	580*

Source: University of Maryland POICN Database.

*Certain incidents involve more than one agent type, therefore agents used exceeds the total 517 incidents during the timeframe.

While chemical agents have been the preferred weapon of choice of perpetrators, it is important to also examine the dangers posed by nuclear, radiological, and biological agents.

Nuclear

The shortest—not necessarily the easiest—route for a non-state actor to aquire a nuclear weapon is to obtain one from a preexisting state arsenal. The Russian nuclear weapon arsenal, specifically quasi-retired tactical nuclear weapons, demonstrates worrying signs of porosity. However, the most likely source of a complete and intact nuclear weapon is Pakistan. The country is home to some of the most formidable VNSAs in the world and is presently developing smaller, tactical warheads to be forward-deployed near the Indian border.[5] If these tactical nuclear weapons were to enter into widespread service, the warheads would be the most vulnerable on earth given their relative seclusion and portability.[6] That being said, nuclear warheads in state arsenals are among the best protected items on earth. Absent insider access or a rare breakdown of security—e.g. during a coup d'état—VNSAs would find it extraordinarily difficult to acquire and smuggle an intact weapon without detection. VNSAs might therefore judge it easier to obtain fissile material and construct their own weapon. Fabricating their own fissile material from raw products would demand prolonged engagement in either the enrichment of uranium or the chemical separation of plutonium—processes that experts believe to be too complex, costly, and detectable for any currently known terrorist organization to realistically undertake.

This leaves acquisition of weapons-usable or nearly usable material as a more enticing option. Aspiring nuclear actors might target highly enriched uranium used in less secure environments, such as research reactors, isotope generation facilities, or even nuclear maritime propulsion contexts.[7] Such operations will remain potentially vulnerable until they are converted to technologies that require less or eliminate altogether the need for highly enriched uranium. On the other hand, if material is acquired by an insider or other criminal not seeking to use it himself but to sell on the "black market," prospects for interdiction are slightly better as global intelligence and law enforcement have proven themselves adept at setting up "stings" to recover such material.

Radiological

Weaponization of radiological agents is likely to be seen as far less challenging, and therefore more attractive to VNSAs, than acquiring nuclear weapons. Radiological weapons can be deployed using a range of delivery systems, from sophisticated aerosol dispersal systems that present an inhalation hazard to radiation emitting devices that simply hide a piece of radiological material and expose passers by to harmful radiation. Any attack could cause massive disruption and anxiety—but only at the upper end of the scale of possible radiological weapons in both size and complexity would an attack reach the WMD threshold.[8] The psychological effects coupled with the sheer number of radiological sources in circulation represent an attractive option for VNSAs seeking to use CBRN weapons.

Obstacles to the acquisition of radioactive materials by theft are location dependent. The most vulnerable materials are radiological sources housed in portable devices, such as medical mobile irradiators and imaging devices that can be wheeled about.[9] Other potential methods of acquisition include "deliberate transfer by a government, unauthorized transfer by a government official or a facility custodian (insider), looting during coups or other times of political turmoil, licensing fraud, organized crime, exploiting weaknesses in transportation links, sellers of illicitly trafficked radioactive material, and finding orphan radioactive sources (that have been lost, stolen, or fallen outside of regulatory control)."[10] Between 1990 and 2010, there were close to 400 incidents of high-threat radiological materials that fell out of regulatory control. Since 2010 these incidents have doubled.[11] However, it is important to note that there has only been one incident involving a radiological agent since 2012. While material loss is a potential threat, it should not be over-estimated since, according to the data, it does not often fall into the hands of terrorists who want to use it as a radiological weapon.

In any event, if acquisition did occur, a VNSA would need to overcome challenges related to the safe handling of radioactive materials, and have the knowledge to identify the correct amounts and types of explosives for dispersal over a wide area. The VNSA would also need to have the skillset to fabricate the required physical form of the radioactive source to ensure effective dispersal of the material.[12]

Fortunately, powerful radionuclides are fairly easy to detect with passive radiation detection systems, often deployed at ports of entry and international borders. Smuggling such materials, however, may not be necessary for radiological attacks given the likelihood that suitable source material can be found at a facility within the country—if not the immediate vicinity—of the desired target. A VNSA could make the very facility housing the radiological material a target by prefabricating the dispersal device such that it could be loaded and deployed as soon as the material was acquired, or by simply employing explosives to compromise the containment capacity of an industrial irradiation facility or nuclear spent fuel pool. In spite of the apparent viability of some of these tactics, radiological attacks are not common because of their lack of outright lethality and visceral violence as compared to the alternatives, and may not be worth the operational risks and degree of retributive response such an operation is likely to incur.

Chemical

In the event that a VNSA pursues a ready-made chemical weapon, it might do so through theft or state sponsorship. The most likely sources are the stockpiles of such unstable states as Syria, Iraq, Libya, and North Korea. While international retribution against these states discourages their deliberate provision of chemical weapons to VNSAs, there might be willing collaborators with access to these materials within such states. Unstable states might also lose control of these weapons, as has been reported in the case of Syria and Iraq, where the Islamic State of Iraq and the Levant (ISIL) allegedly gained access to weapons stockpiles of the Syrian and former Iraqi regimes.[13]

A second option is to produce a chemical agent and appropriate delivery mechanism using precursor materials. The simplest types of chemical weapons involve the release of highly volatile or gaseous common chemicals, for example chlorine gas or hydrogen cyanide, which can easily be produced by individuals with a high-school level of training.[14] Therefore, since certain toxic chemicals can be produced in weapons-usable quantities with less specialized equipment than is needed for other agents (chlorine is one example), it is no surprise that small-to medium-scale chemical attacks have been the most common CBRN weapon type utilized by VNSAs. However, breaching

the WMD threshold would require considerable volumes of these types of agent.

A third, fairly straightforward yet appreciably more alarming chemical attack scenario is the release of toxic industrial chemicals from storage or during transportation. The sources for these potentially crude weapons often exist in large quantities in poorly secured facilities near populated areas and provide attractive targets for terrorists and other VNSAs.

The final option is the production by terrorists of highly toxic, traditional chemical warfare agents. Since 2014, there have been a few examples of such attacks by ISIL using sulfur mustard agents against Kurdish fighters.[15] Nerve agents, such as tabun, sarin, and VX, however, require a more advanced level of training to ensure safety during the manufacturing process and maximum effectiveness of deployment.[16] However, many complex chemicals that can serve as weapons are used for licit applications (e.g pharmaceuticals with high toxicity), are increasingly being synthesized in developing countries, and are becoming readily available for purchase. For example, Chinese pharmaceutical producers are illicitly shipping sufficient amounts of Carfentanil to potentially deliver tens of millions of lethal doses across the globe. While efficient delivery of such an agent is no mean feat for a VNSA, such quantities of these deadly agents could still kill or injure hundreds or even thousands if deployed in confined spaces.

Biological

Biological attacks have the potential for the most catastrophic effects outside of nuclear weapons, but there are significant difficulties associated with attacks using living weapons. Aum Shinrikyo experimented with anthrax, botulinum toxin, cholera, Q fever, and even ebola, from 1990–95, but was unsuccessful due to unsophisticated delivery mechanisms and nonvirulent strains.[17] The mechanism through which the lone actor Bruce Ivins chose to disperse anthrax-causing spores—a letter—was also unsophisticated and, fortunately, although his expertise and access allowed him to produce a sophisticated agent, it was not dispersed at a catastrophic scale.

The pathways to acquisition of a biological weapon include theft (most likely from a state-run program) or in-house production.[18] Similar to other agents, there is concern that insiders or individuals with access to state-run programs could potentially provide a VNSA with a highly lethal, highly contagious agent. The potential to divert biological weapons and materials is particularly strong in countries with a history of bioweapon programs, where many sites are vulnerable to diversion, insider collaboration, or theft.[19] Additionally, there are more than 1,500 state-owned and commercial culture collections intended for research that might be sources of biological pathogen seed stocks. In-house manufacture and production of these agents entails multiple complications for a VNSA. Obtaining the correct micro-organism, procuring the right equipment, avoiding contamination, and ensuring virulence during weaponization are only a few of the obstacles to a successful attack. Given these complications, the most common types of biological weapons have been simple toxins like ricin. VNSAs have been successful in extracting this agent from castor plant beans as illustrated in some jihadist manuals and online videos. However, even though these toxins are produced by living organisms, they are neither infectious nor contagious, thus limiting their mass-casualty potential.

At present, there is no evidence of a successful mass-casualty attack by a VNSA with a contagious bio-agent, and according to POICN there have been only 11 small-scale incidents involving biological agents since 2012. This could be because even if a VNSA was able to obtain a biological agent and properly transport or smuggle it to the target, it would still need to ensure pathogenicity and

virulence of the microbe, maintain pathogen stability, accurately calculate the necessary infectious dose, achieve optimal composition formulation, prevent incremental degradation while transporting, and be able to assess difficult to control environmental factors during delivery.[20]

Ambitions and Capabilities

Given the variety of motives for employment of these weapons, we should not be surprised that VNSAs of different ideological persuasions have sought WMD capability. Incidents involving VNSA use of CBRN materials intended for WMD attacks have progressively become more complex and sophisticated.[21] This, coupled with the expressed intention of some actors to seek WMD both for their physical and psychological effects, suggests that the threat of VNSA WMD attacks is not decreasing.

In answering the question of who and what should be the focus of concern, we observe in Figure 1 that, of the total number of incidents in POICN, 31 percent are attributed to extremist religious actors (including lone actors/autonomous cells in support of a collective religious ideology), 22 percent to ethno-nationalist actors (including lone actors/autonomous cells that expressed motivation to establish ethno-nationalist sovereignty or bolster ethno-nationalist rights) , and 11 percent to lone actors or autonomous cells espousing idiosyncratic motives.[22] The remaining cases include far-right and left-wing groups, cults, single-issue groups, and unknown perpetrators.

Since 2012, the distribution of perpetrators changed dramatically from the preceding period. We observe in Figure 2 that an estimated 71 percent of CBRN related incidents are specifically attributed to religious extremists actors including lone actors/autonomous cells in support of a collective religious theology. The second largest set of incidents, with 19 percent, includes lone actors/autonomous cells motivated by professional/personal grudges and financial gain (11 percent), or those that have been linked to ethno-nationalist ideas (8 percent). Given the clear predominance of two specific actor types in the recent threat picture, we will focus the remaining discussion of the current threat on extremist religious actors, in particular ISIL, and lone actors.

Figure 1: CBRN Incidents by Non-State Actors, 1990–2016.

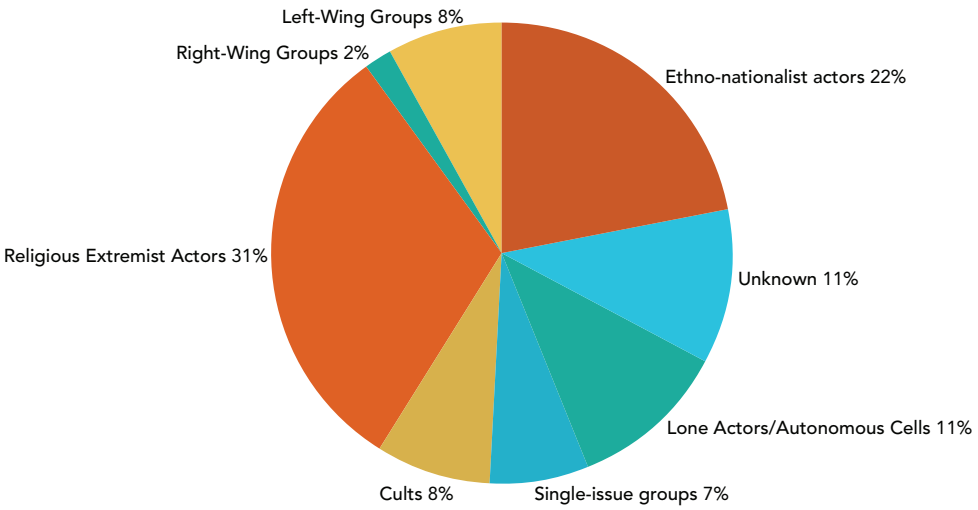
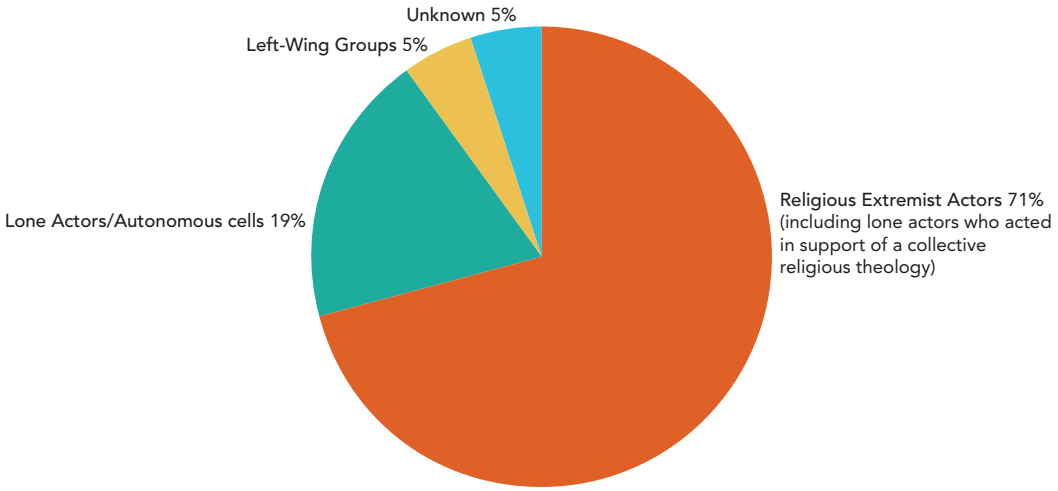


Figure 2: CBRN Incidents by Non-State Actors, 2012–16.



Islamic State

A number of jihadist ideologues have demonstrated their willingness to use indiscriminate, mass-casualty violence, and publicly expressed their interest in conducting CBRN and WMD attacks specifically.[23] American troops operating in Northern Iraq in 2003 discovered primitive labs that the terrorist group Ansar al-Islam had used for experimentation with chemical and toxic weapons. By 2007, the direct forerunners of ISIL, al-Qaeda in Iraq (AQI) and Islamic State of Iraq (ISI), demonstrated their intent to pursue and use chemical weapons on a massive scale by using chlorine to enhance vehicle-borne improvised explosive devises (VBIEDs) in terrorist attacks.[24] In 2014, when ISIL began to contend for territory on a regional scale and was able to seize, purchase, or craft military hardware, they revisited their predecessors' desire to formalize a chemical weapon program. ISIL forces in Syria have deployed chlorine, sulfur mustard, phosphine, and other toxic industrial chemicals such as vinyltrichlorosilane, for tactical purposes—the first chemical warfare agents introduced onto the battlefield since the Iran–Iraq war.[25] It is thus no surprise that media sources routinely mention a growing WMD threat posed by jihadist groups, particularly ISIL.

Fortunately, ISIL as a territorial force has been shattered within the past year; the threat emanating from the group is more localized and the group's capability is considerably reduced. Yet, ISIL recruiters and sympathizers continue to leverage the messaging value of WMD capability. Recently, an ISIL publication claimed the ability to acquire and smuggle a state-built nuclear weapon across the southern border of United States.[26] With the perceived divine right to use WMD intact, and driven by desperation and thirst to avenge the Caliphate, it is possible that ISIL might make a last gasp effort to execute a CBRN attack, or perhaps set the stage for the next group of the Salafi milieu to execute this divine mission in their stead.

Recent studies of ISIL CBRN ambitions and capabilities suggest the most likely form of such threats include sporadic attacks by foreign fighters returning to their countries of origin with the desire to strike at the West.[27] ISIL may have gained access to several dual use-technology sites in Syria and Iraq (especially in pursuit of chemical weapons).[28] Even if these fighters did not succeed in smuggling any purloined materials into the West, it is entirely possible they developed the expertise needed to

undertake attacks in their countries of origin, where there might be plenty of poorly-secured precursor chemicals or facilities with other agents available. While the effects of any resulting attacks are likely to remain localized, such attacks are often sufficient to cause mass disruption, if not mass destruction.[29]

Other likely threats include attacks on facilities housing CBRN materials for *in situ* release, or collaboration between ISIL remnants, other VNSAs, and private funders to facilitate the acquisition of CBRN materials or weapons. The utilization of pre-established revenue sources in the black market and through private donors might afford sufficient material support to sustain the group among the community of VNSAs.

Despite these lingering threats from ISIL and the global Salafi jihadist milieu, we have been fortunate that the opportunity, capability, and motives for acquiring and using a WMD have thus far not aligned. In addition, one should not forget about the other jihadist non-state actor—the Shiite militia Hezbollah— which has no current motive to use WMD against the West, but, given their copious resources, global networks and extensive technical assistance from Iran, would be in a much better position than any Sunni jihadist to carry out a WMD attack, should it so choose.

Lone Actors

POICN attributes 18 CBRN incidents—of the total 38 cases recorded since 2012 to lone actors and autonomous cells. Seventy-seven percent of the cases involving lone actors and autonomous cells were driven by either religious or ethno-nationalist motivations. The broad array of actors behind these incidents make it challenging to isolate specific types of threats. Even worse—lone actors and autonomous cell plots are among the most difficult to detect.[30]

For so-called "lone wolf" terrorists, motivations can be driven by a range of less predictable and idiosyncratic factors.[31] They can be shaped by an individual or group's "doctrines, pathologies, and collective or individualistic emotional impulses (including revenge)."[32] Lone actors and autonomous cells often have obscure motives. Many experts have aligned lone actors' incidents with "purely criminal motives," but only 28 percent of incidents recorded in POICN since 2012 were driven purely by criminal motives.[33]

Such actors are typically perceived to have more modest technical capabilities than an organized group, but often have a different set of operational opportunities that could be more advantageous for a WMD attack than those of a larger group. Insider access is one such concern. Technical insiders, with access to source materials, and technical knowledge pose a significant CBRN threat. The ability of law enforcement to detect plots of the lone wolf or autonomous cell nature is limited. For example, shortly after 9/11, Dr. Bruce E. Ivins, a U.S. Army civilian research scientist mailed letters containing a highly virulent and sophisticated form of anthrax to media offices and the offices of two U.S. senators. Five people were killed, 17 people became gravely ill, mail service stopped, and one of the Senate office buildings was shut down for fear of additional attacks.[34] Only five years later did Dr. Ivins became a suspect in the investigation.

Lone actors and autonomous cells have played a prolific role in CBRN terrorism and will continue to do so as long as these weapons continue to have far-reaching impacts driven by fear.[35] A disturbing trend is that terrorist organizations continue to promote insider attacks using CBRN weapons. In 2010, al-Qaeda began promoting and instructing lone actor attacks through its magazine, Inspire.[36] ISIL and other groups invite individuals to become "walk-on terrorists," and provide them with the blueprints for conventional and unconventional weapon attacks.[37] In a manifesto written by Anders Breivek published prior to his attacks in Norway in

2011, he encouraged sympathetic scientists to aid in the development of anthrax, ricin, and liquid nicotine. He may have inspired other, similarly motivated lone actors (particularly of the far-right flavor) to attempt the CBRN attack plots that he ultimately did not.[38]

Lastly, the most likely threat posed by lone actors is a chemical attack. Sixty one percent of CBRN incidents by lone actors and autonomous cells since 2012 used chemical agents. While lone actors and autonomous cells have not yet been able to get a WMD attack "right" in the past, as various technologies change and obstacles to obtaining source materials are overcome (as discussed later), the possibility of a successful WMD attack increases.

Technological Advances and Changing Adversaries

Rapid technological advances are reported in fields as disparate as materials science, pharmaceuticals, communications, automation, biotechnology and robotics on a daily basis. These technological developments could yield new forms of WMD; for example, synthetic biology using techniques such as CRISPR/Cas-9 and commercial "gene fabs" allow for the creation of new variants of existing pathogens or even entirely new pathogens that are designed for resistance to such current countermeasures as antibiotics and vaccines. Toxic, self-replicating nanites that have effects similar to some chemical weapons, are also a plausible, albeit more distant risk.

The most dramatic near-term developments effecting the overall WMD threat picture are, however, likely to relate to the acquisition, production and weaponization of CBRN agents. A variety of technological trends, from miniaturization of manufacturing and turn-key systems to rapid prototyping and marginal cost reproduction—e.g. 3-D printing—could facilitate the production of WMD. In the past, producing sufficient amounts of nerve agent to constitute a chemical WMD required large equipment and dangerous reactants to be set up and monitored by experienced chemical engineers, with a dangerous leak or explosion a constant concern. The advent of new technologies like chemical microreactors (where precursor chemicals are combined under controlled conditions in miniature channels on a "chip") could allow for self-contained production of small quantities of CW in a basement, with almost no hazard and far less vulnerability to detection by authorities. Stringing several of these modules together and operating them for extended periods, could still yield sufficient quantities for the desired level of mayhem. Another

The most dramatic near-term developments effecting the overall WMD threat picture are, however, likely to relate to the acquisition, production and weaponization of CBRN agents. A variety of technological trends, from miniaturization of manufacturing and turn-key systems to rapid prototyping and marginal cost reproduction—e.g. 3-D printing—could facilitate the production of WMD.

example is biotechnology "kits" that take much of the technical guesswork out of complex microbiological procedures and are even being marketed to high-schoolers.[39] This phenomenon likely will eventually lead to WMD that can be produced more cheaply, more safely, and with a smaller operational footprint. For terrorists and other VNSAs, such developments will serve only to lengthen Archimedes' proverbial lever when it comes to their asymmetric effects versus their state opponents.

It is not merely the development of new technologies—most terrorists hardly operate at the cutting edge of science—but rather the swift spread of these technologies to commercial-off-the-shelf applications that could boost terrorist capabilities. Once new technologies become available for sale online, they can be purchased and quickly delivered around the globe, effectively resulting in the "democratization" of the means of mass destruction. Moreover, the worry is not just that technological developments are rapidly occurring; the actual rate of change itself is increasing so that the length of time between major breakthroughs is continually decreasing.[40] This makes it difficult for even the most astute observers (including our intelligence agencies) to keep up with technological developments that might impact the threat of WMD terrorism.

Moreover, our adversaries themselves are changing. The arrival of online technical education, typified by the Kahn Academy and numerous MOOCs (massive open online courses), means that radicals in even the most remote, ungoverned regions now have access to at least basic technical knowledge in a variety of disciplines. At the same time, the pervasiveness of social media and other online modalities enables ideologues to reach, and at least sometimes succeed in radicalizing, even the best and the brightest at the most prestigious institutions of higher learning in the West and elsewhere. In this sense, globalization and information technology "are creating more accomplished users."[41] Such dynamics resulting from the information revolution can be expected to move terrorists further up the WMD learning curve, just as technology flattens it out.

The capacity of VNSAs to engage in the complex engineering efforts required to produce and deploy a WMD can be studied through comparative cases. The PIRA's (Provisional Irish Republican Army) in-house mortar program and the FARC's (Revolutionary Armed Forces of Colombia) construction of full-fledged submarines within jungle bases, are examples of how VNSAs are capable of genuinely impressive feats of engineering even under clandestine conditions and external pressure.[42] A willingness and ability to devote substantial resources to the effort for an extended period, the capacity to obtain or develop technical expertise, a safe haven in which to operate, and an organizational culture that embraces learning can lead to success even under the most challenging conditions.

How VNSAs might acquire sophisticated technologies externally, from networks consisting of states, transnational criminal organizations, legitimate commercial enterprises, or other violent groups merits further study. A preliminary model indicates the need to take into account such factors as bargaining, the role of intermediaries, and different loci of transfer. Indeed, several new areas of WMD threat might arise at the nexus between different types of VNSAs. Although, while most transnational criminal organizations (TCOs) might see no profit in assisting terrorists in acquiring or transporting WMD materials, this barrier might not apply in the presence of ideological or kinship ties, where a hybrid TCO–terrorist emerges, or where a criminal organization is infiltrated or duped into unwittingly helping terrorists acquire WMD. FARC's involvement with uranium smuggling, and the development of sophisticated illicit chemical production capabilities among TCOs are just two disturbing examples of such so-called "unholy alliances."[43]

At the conceptual extremity of the confluence of these trends affecting both technology and our adversaries lies the superempowered individual, a single fanatic or misanthrope with the power to upend the entire social system through his or her own actions.[44] While we have not yet seen any unambiguous cases, individuals like Bruce Ivins and Ramzi Yousef come close. This type of individual has the capacity to pose a grave threat, yet, if combined with an intense ideological motivation, might be prone to scales of violence that make them even more likely to select CBRN weapons to conduct a WMD attack than any terrorist organization witnessed thus far.[45]

Most terrorists are decidedly conservative most of the time and imitative in their use of weapons and tactics. It is only a minority that historically has ever pursued unconventional means of harm and an even smaller number that has had even minimal success. The key challenge, from a strategic perspective, is proactively distinguishing the few terrorists and other VNSAs most likely to move successfully through all of the gates associated with adoption of WMD-relevant technology from the vast majority that are not. One of the authors has developed a framework to address this question, the Terrorist Technology Adoption Model (T-TAM), which assesses the relative likelihood of a particular terrorist group (or other VNSA) a) gaining awareness of, b) deciding to pursue, and c) then successfully acquiring a given technology, and has been applied to the technologies underlying WMD. While space limitations preclude a detailed description of the framework, T-TAM examines the interaction between a set of variables characterizing the technology under consideration and those relating to the nature of the actor itself (with particular attention paid to the elements of knowledge transfer), as well as accounting for environmental factors and the prior behavior of other actors in the system.[46]

One of the core insights derived from T-TAM is that a given technology on its own, while theoretically capable of enabling great harm—e.g. if it facilitates the acquisition of a WMD—does not pose a threat until it falls into the hands of a terrorist or other VNSA who both recognize its potential, want to adopt it, and succeed in doing so. It is thus specific terrorist-technology dyads that are of greatest concern, rather than any terrorist group or technology taken on its own. Adopting this approach and utilizing T-TAM can help mitigate the dual-use dilemma. This is so because, on the one hand, even if a given technology hypothetically increases the WMD potential of VNSAs, but only a handful of VNSAs will ever proceed through all of the adoption gates with respect to that technology, then it is more efficient and probably more effective to concentrate our counterterrorism resources on observing those VNSAs for threatening behavior. On the other hand, a technology that is likely to be sought after and easily adopted by a substantial portion of VNSAs presents more of a dual-use problem and might be a good candidate for some type of technology control or monitoring regime.

One less comforting finding from T-TAM is the key role played by demonstration in spurring the diffusion of a given weapon. Once one terrorist or other VNSA succeeds in launching a successful WMD attack, even if by chance, this can be a catalyst for future attacks by others in that it reduces the uncertainty surrounding such an enterprise by showing that it can indeed be accomplished by a non-state actor. This has been illustrated recently outside of the WMD realm with the rapid adoption by several jihadist terrorist organizations of the use of UAVs as attack platforms.

Conclusion

Some of the hype surrounding WMD terrorism is overblown. Despite clear interest on the part of our most vehement and capable adversaries, a true WMD

is likely out of their reach in all but a few scenarios: the release of *in situ* toxic industrial chemicals or highly radiological materials close to an urban area (only possible in a limited number of locations), and the highly unlikely serendipitous acquisition of a viable nuclear or biological weapon from a state arsenal. The good news from a strategic perspective is that these scenarios are preventable with current security and non-proliferation approaches (provided they continue to be implemented effectively), and there is still a window (albeit a shrinking one) to bring our collective talents and resources to bear on limiting the increased WMD terrorist threats of tomorrow. Some of the same dynamics increasing the threat might also yield new ways to defend against it. For instance, synthetic biology might produce new antiviral treatments or antibiotics; better manufacturing techniques might allow for more sensitive radiation detectors; and more widespread education might reduce the number of disaffected youth in the developing world.

When considering the threat of WMD terrorism, we thus come around to the age-old strategic race between the offense and the defense, so ably evinced by Hugh Turney-High: "[t]he offense thinks up new weapons or improves the old ones so that the defence's genius must think up new defence or be crushed out of existence. There is nothing new nor old in this."[47] Except that in this case, technologies seem to favor the adversary, the growing empowerment of the individual is unlikely to be reversed, and there are a number of tipping points—such as the first demonstration by a terrorist of a WMD capability—that could profoundly alter the system. It thus appears that the VNSA offense in future will be playing with a stronger hand than the international security defense—and with the stakes as high as with WMD, the defense cannot afford to falter even once. PRISM

Notes

[1] For a detailed discussion and justification of this definition, see Gary Ackerman and Jeremy Tamsett, "Introduction," in Gary Ackerman and Jeremy Tamsett (eds.), *Jihadists and Weapons of Mass Destruction*, Boca Raton, Florida: CRC Press (2009), xix–xxii. For alternative defintions, see the extended discussion in W. Seth Carus, Defining '*Weapons of Mass Destruction*,' Center for the Study of Weapons of Mass Destruction Occasional Paper 4, National Defense UniversityPress, Washington, DC, February 2006.

[2] Gary Ackerman and Jeremy Tamsett, "Introduction," xxi.

[3] Victor H. Asal, Gary A. Ackerman, and R. Karl Rethemeyer (2012): "Connections Can Be Toxic: Terrorist Organizational Factors and the Pursuit of CBRN Weapons," *Studies in Conflict & Terrorism*, 35:3, 231.

[4] Gary Ackerman and Markus K. Binder. "Pick Your POICN: Introducing the Profiles of Incidents involving CBRN and Non-state Actors (POICN) Database," College Park, MD: START, 2017.

[5] Monika Chansoria, "Paksitan's Tactical Nukes Threaten Stability in South Asia," May 5, 2014, *Foreign Policy*, http://foreignpolicy.com/2014/05/05/pakistans-tactical-nukes-threaten-stability-in-south-asia/.

[6] James Halverson, "Radiological and Nuclear Material Vulnerability: An Overview Assessment," Report to NSDD. College Park, MD: START, 2017.16.

[7] James Halverson, "Radiological and Nuclear Material Vulnerability: An Overview Assessment," 32.

[8] Charles D. Ferguson, "Radiological Weapons and Jihadist Terrorism," in *Jihadists and Weapons of Mass Destruction*, 174.

[9] *Nuclear Nonproliferation: Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Sources*," GAO, 2014, 24–25.

[10] For a fuller treatment of this pathway analysis, see Charles D. Ferguson and William C. Potter with Amy Sands, Leonard Spector, and Fred L. Wehling, *The Four Faces of Nuclear Terrorism* (New York: Routledge, 2005), 271–278; and Charles D. Ferguson, "Radiological Weapons and Jihadist Terrorism," 174.

[11] Gary Ackerman, Cory Davenport, Varun Piplani and James Halverson. "Trend Analysis of the RN Materials Out of Regulatory Control (MORC) Database." Final Report to NSDD. College Park, MD: START, 2017.

[12] Charles D. Ferguson, "Radiological Weapons and Jihadist Terrorism," 174.

[13] Herbert Tinsley, Jillian Quigley, Markus Binder, and Lauren Samuelsen. "IS Chemical and Biological Weapons Behavioral Profile," College Park, MD: START, 2017.

[14] Stephanie Meulenbelt and Maarten S. Nieuwenhuizen, "Non-State Actors' Pursuit of CBRN Weapons: From Motivation to Potential Humanitarian Consequences," *International Review of the Red Cross*, 2015, Vol 97: 899, 848.

[15] Associated Press, "Islamic State Used Chemical Weapons against Peshmerga, Kurds Say," *The Guardian*, 14 March 2015. https://www.theguardian.com/world/2015/mar/14/islamic-state-isisused-chemical-weapons-peshmerga-kurds, and BBC News, "Islamic State 'Used MustardGas' against Peshmerga", BBC News, 7 October 2015. https://www.bbc.com/news/world-middle-east-34471237.

[16] Stephanie Meulenbelt and Maarten S. Nieuwenhuizen, "Non-State actors' Pursuit of CBRN Weapons: From Motivation to Potential Humanitarian Consequences," 899, 848.

[17] Cheryl Loeb, "Jihadist and Biological and Toxin Weapons" in *Jihadists and Weapons of Mass Destruction*, 153.

[18] Cheryl Loeb, "Jihadist and Biological and Toxin Weapons," 153.

[19] Jonathan Tucker, "Preventing the Misuse of Pathogens: The Need for Global Biosecurity Standards," *Arms Control Today*, June 2013, http://www.armscontrol.org/act/2003_06/tucker_june03.asp#notes.

[20] Cheryl Loeb, "Jihadist and Biological and Toxin Weapons," 153.

[21] The proportion of cases that are judged to be of high concern in POICN has increased from 47% before 2011 to 70% since 2011.

[22] "Profiles of Incidents Involving CBRN by Non-state Actors (POICN) Database Version 2.53," (June 2017), National Consortium for the Study of Terrorism and Responses to Terrorism (START).

[23] Since 1998, when Osama bin Laden first said that "acquiring WMD for the defense of Muslims is a religious duty," jihadist groups have continually explored the possibility of conducting a mass-casualty CBRN terrorist attack (Osama bin Laden, "Osama bin Laden Interview," interview by John Miller, ABC News, (1998), excerpt accessed November 29, 2017, http://www.pbs.org/wgbh/pages/frontline/shows/binladen/who/edicts.html). A few years later Saikh Nasir bin Hamid al-Fahd issued a fatwa entitled "*A Treatise on the Legal Satus of Using Weapons of Mass Destruction Against Infidels*" that asserted Muslims have the right to kill as many as four million Americans and suggested the use of WMD attacks to accomplish this. Most recently, and later in name of ISIL, Abu Bakr al-Baghdadi, urged Muslims to make a hijra to the Caliphate: "We make a special call to the scholars . . . medical doctors, and engineers of all different specializations and fields" ("The Return of the Khilafah," Dabiq 1 (2014): 11).

[24] "ISIS dream to own 'chemical weapons' is approaching to be true," *Sound and Picture*, May 18, 2016,http://sound-and-picture.com/en/isis-dream-to-own-chemical-weapons-is-approaching-to-be-true.

[25] Herbert Tinsley, et. al., "IS Chemical and Biological Weapons Behavioral Profile".

[26] Herbert Tinsley and James Halverson, *Islamic State CBRN Capabilities: An Assessment of Threats and Realities*," College Park, MD: START, 2017.

[27] Herbert Tinsley, et. al., "IS Chemical and Biological Weapons Behavioral Profile".

[28] Gary Ackerman and Ryan Pereira, "Jihadist and WMD: a Re-evaluation of the Future Threat," *CBRNE World*, October 2014, 27.

[29] For example in the 1995 Tokyo subway attacks by Aum Shinrikyo, 5,510 potential casualties reported to medical facilities, despite not showing any symptoms of nerve agent exposure. 4,400 of these victims were classified as "worried well" and discharged. See A. E. Smithson and L. A. Levy, *Ataxia: The Chemical and Biological Terrorism Threat and the U.S. Response*, Henry L. Stimson Center, October, 2000, Report no. 35.

[30] Doina Chiacu, "Top U.S. Security Threats: Lone Wolves, Syria Fighters: Officials," *Reuters*, September 17, 2014, https://www.reuters.com/article/us-usa-security-homeland/top-u-s-security-threats-lone-wolves-syria-fighters-officials-idUSKBN0HC1JF20140917

[31] For a detailed study of one such personal motive, self-glorification, see Albert Borowitz, *Terrorism for Self-Glorification: The Herostratos Syndrome*, Kent, OH: Kent State University (2005).

[32] James Halverson and Gary Ackerman. *Radiological/Nuclear (RN) Terrorism: Global Assessment of Threat Intention Drivers*, College Park, MD: START, 2015, 3, and Jeffrey M. Bale, "Jihadist Ideology and Strategy and the Possible Employment of WMD," 7.

[33] Victor H. Asal and R. Karl Rethemeyer, "Islamist Use and Pursuit of CBRN Terrorism," in *Jihadists and Weapons of Mass Destruction*, 342.

[34] Deborah Tedford, "Scientist in Anthrax Case Dead of Apparent Suicide," NPR, August 1, 2008, https://www.npr.org/templates/story/story.php?storyId=93161970.

[35] Charles P. Blair, Kelsey Gregg, and Jonathan Garbo, "Norway's Anders Breivik: Weapons of Mass Destruction and the Politics of Cultural Despair," Federation of American Scientists, 2011, http://www.fas.org/blog/ssp/2011/07/norways-andersbreivik-weapons-of-mass-destruction-and-politics-of-cultural-despair.php#.

[36] Katie Worth, "Lone Wolf Attacks are Becoming More Common—and More Deadly," *Frontline*, July 14, 2016, https://www.pbs.org/wgbh/frontline/article/

lone-wolf-attacks-are-becoming-more-common-and-more-deadly/.

[37] Tom Mockaitis, "The Changing Face of Lone-Wolf Terrorism," *Huffington Post*, November 1, 2017, https://www.huffingtonpost.com/entry/the-changing-face-of-lone-wolf-terrorism_us_59f9f-9b2e4b0b7f0915f636c.

[38] Gary Ackerman and Lauren E Pinson, "Gauging the Threat," *Defence Procurement International*, Summer 2013, 3.

[39] "Edvotek Transformation of E. Coli with Green Fluorescent Proteing (GFP)" https://www.fishersci.com/shop/products/edvotek-transformation-i-e-coli-i-green-fluorescent-protein-gfp/s68654; see also http://www.the-odin.com/.

[40] See Ray Kurzweil, *The Singularity is Near* (New York: Penguin Books, 2005) for an extended discussion.

[41] Gary Ackerman and Lauren E Pinson, "Gauging the Threat," 3.

[42] Gary A. Ackerman, "Comparative Analysis of VNSA Complex Engineering Efforts," *Journal of Strategic Security* 9, no.1 (Spring 2016), 119.

[43] DPA. (2006, March 2). "Colombia Seizes 13.5 kilograms of uranium, possible Soviet origin. Americas News", http://denuclear.blogspot.com/2006/03/colombia-seizes-135-kilograms-of.html; Goodman, J. (2008, March 27). "Colombia probes FARC ties to uranium seized in Bogota (update 3)," *Bloomberg*, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a2kQfcdqP.ns.

[44] Thomas L. Friedman, *Longitudes and Attitudes: Exploring the World After September 11* (New York: Farrar, Straus and Giroux, 2002); Adam Elkus, "Night of the Lone Wolves," *Defense and the National Interest Special*, November 29, 2007, http://www.dnipogo.org/fcs/elkus_lone_wolves.htm.

[45] Gary A. Ackerman and Lauren E. Pinson, "An Army of One: Assessing CBRN Pursuit and Use by Lone Wolves and Autonomous Cells," Terrorism and Political Violence, 228.

[46] See Gary A. Ackerman, *More Bang for the Buck: Examining the Determinants of Terrorist Adoption of New Weapons Technologies*, Unpublished Doctoral Dissertation, King's College London (2013).

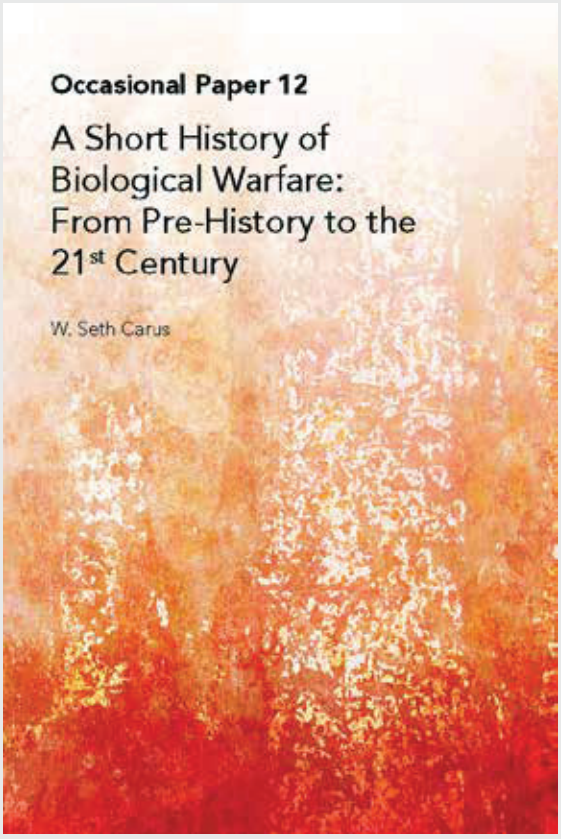
[47] Harry H. Turney-High, *Primitive War: Its practice and concept,s*(Columbia, SC: University of South Carolina Press, (1949), 7.

CENTER FOR THE STUDY OF WEAPONS OF MASS DESTRUCTION, NATIONAL DEFENSE UNIVERSITY (NDU)

Further details on upcoming events and recent publications are available at http://wwmdcenter.ndu.edu.

Negotiating a Nuclear Code of Conduct, by Justin V. Anderson

Throughout the nuclear age, the United States, Russian Federation, China, France, and the United Kingdom—the five states permitted by the 1968 Nuclear Nonproliferation Treaty (NPT) to possess nuclear arsenals (the "NPT nuclear five")—have criticized other nuclear states, or each other, for engaging in dangerous or destabilizing behavior with regard to their nuclear forces. Criticisms have implicitly or explicitly called out offending states for deviating from behavior associated with "responsible" nuclear states. But what exactly constitutes responsible behavior for nuclear-armed states, and what norms or rules should they follow?



A Short History of Biological Warfare: From Pre-History to the 21st Century, by W. Seth Carus

This monograph reviews the history of biological warfare (BW) from prehistory to the present. It covers what we know about the practice of BW and briefly describes the programs that developed BW weapons based on the best available research. To the extent possible, it primarily draws on the work of historians who used primary sources, relying where possible on studies specifically focused on BW. By broadening our knowledge of BW, such studies have enabled us to write about the topic with more accuracy and detail than could have been done even a few years ago. This is an overview, not a definitive history. Much about BW remains unknown, either because it is unknowable (due in some cases to the deliberate destruction of records) or because it is knowable only to some people (such as those who might have access to classified information) or because of the absence of academic research.

New Jersey National Guard members participate at a Homeland Response Force (HRF) External Evaluation in 2012. HRFs help provide the initial military response to a CBRN incident. (U.S. Air Force/ Mark C. Olsen)

Improving Our CWMD Capabilities

Who Will Lead?

By Al Mauroni

In December 2016, the media announced that U.S. Special Operations Command (USSOCOM) would take the lead role within the Department of Defense (DOD) for countering weapons of mass destruction (WMD).[1] Talks to synchronize the transfer of the mission from U.S. Strategic Command (USSTRATCOM) to USSOCOM had started in 2015 with formal changes enacted in the 2016 Unified Command Plan. More than a year later, it remains unclear as to how USSOCOM will rebalance its priorities to adjust to this new authority.[2] While the number of potential adversaries armed with nuclear, biological, and chemical (NBC) weapons has fallen during the past two decades, the number of U.S. Government (USG) programs addressing the prevention, protection against, and response to WMD threats has risen significantly. USSTRATCOM claimed that it did not have the time or resources for the mission; will USSOCOM be any better prepared for the job? Or will USSOCOM leaders limit their efforts to the coordination and synchronization of counter–WMD (CWMD) concept plans across the combatant commands, as USSTRATCOM leaders once did?

Before attempting to answer these questions, it is worth examining why DOD leaders felt it necessary to identify a combatant command as the lead for this activity. Typically one of the armed services is identified as executive agent for a specific role that requires intra-service coordination. Why is the CWMD mission different? Significantly, it is not merely the sum of many counterproliferation activities. CWMD encompasses a broad global perspective that includes nonproliferation and arms control; WMD interdiction and elimination; security cooperation and partner activities; humanitarian affairs/disaster relief; nuclear deterrence; theater and national missile defense; installation protection and incident response; and more recently even public health emergencies and nuclear accident response.[3]

Also distinctive is the lack of focus as to how CWMD roles and responsibilities are addressed within DOD. In the 1990s, defense planners and policymakers understood counterproliferation to include activities focused on protecting U.S. military forces from non-nuclear adversaries armed with chemical and biological weapons. Released in 2002, the *National Strategy to Combat WMD* broadened nonproliferation and counterproliferation missions, traditionally areas for the Department of State (DOS) and DOD respectively, into a larger interagency context that overlapped with homeland security and combating terrorism

Mr. Al Mauroni is the Director of the U.S. Air Force Center for Unconventional Weapons Studies and author of the book, Countering Weapons of Mass Destruction: Assessing the U.S. Government's Policy.

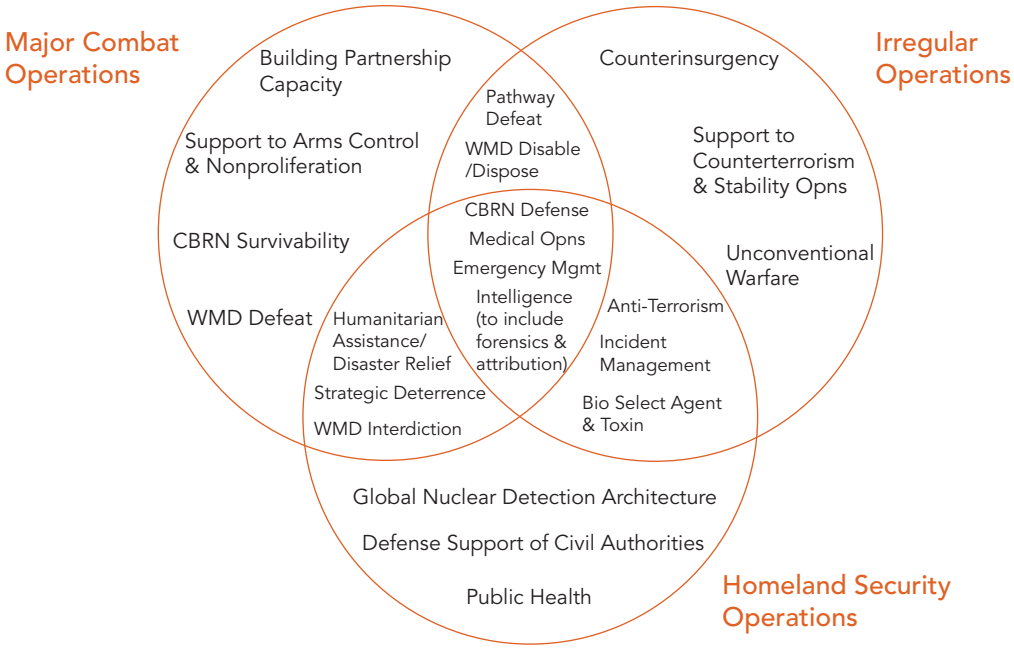
missions. Responsibilities within DOD were divided among three assistant secretaries of defense.[4] U.S. Northern Command (USNORTHCOM) addressed WMD threats within the United States, while USSTRATCOM and USSOCOM took on various aspects of "combating WMD" fielded by adversarial states and sub-state actors as part of overseas contingency operations. To further complicate matters, after a string of pandemics, the Obama Administration identified emerging infectious diseases as a WMD concern and created a new term "countering WMD" to replace "combating WMD."[5]

Within DOD, military forces were directed to address WMD challenges in its joint operating concepts, notably major combat operations, irregular warfare operations, and homeland security operations.[6] This is to say, military planners should expect our adversaries to use WMD across the range of military operations, and plan accordingly within the context of those specific operations. Some of these activities support multiple operational constructs, as Figure 1 illustrates. Owing to the technical nature of WMD, much of the contemporary discussion has focused on the operational challenge of removing WMD through the intervention of technical specialists. Far less attention has been paid to the military ways and means required to meet national policy objectives, ensuring that the United States and its allies can operate unimpeded by the threat or use of nuclear, biological, or chemical weapons by specific adversaries. More than 15 years after the release in 2002 of the *National Strategy to Combat WMD*, no one can credibly assert the degree to which U.S. forces are able to counter–WMD.

Challenges of Policymaking

Global WMD threats have been consistently identified as a top national security challenge during the past 25 years. CWMD is an interagency mission, involving activities primarily within DOD, DOS, and Department of Homeland Security (DHS), as well as the Departments of Health and Human Services (HHS), Energy (DOE), and Justice (DOJ). As a result, DOD must coordinate with USG

Figure 1: CWMD Activities Across Joint Operating Concepts.



policymakers from across the executive branch regarding the strategies and plans required to meet national security policy objectives. Despite this complexity and the consistent prioritization of the WMD threat, DOD leaders have not always viewed the development of CWMD capabilities as a top priority. Military planners often assume U.S. threats of retaliation will deter an adversary from their use of WMD. They do not view CWMD as their concern because other technical agencies make it their mission to address the challenge. This inevitably lowers the priority of WMD issues within the services (short of an immediate crisis), while technical agencies assigned this mission fail to garner the resources needed to address the policy objectives found in national security documents. The disparity between the rhetoric and the reality is striking.

For the past decade, the Intelligence Community (IC) and policymakers have noted that globalization and information and communications technology have made it significantly easier for sub-state groups as well as states to acquire the necessary materials and technology to develop their own WMD capability.[7] Yet the number of known governments that have or are seeking to develop nuclear, biological, or chemical (NBC) weapon programs has decreased dramatically. In 2001 then Secretary of Defense William Cohen identified a minimum of 25 countries that had or sought a WMD capability.[8] By 2008, the Congressional Research Service estimated that 12 countries were suspected of or likely to have NBC weapons. Notably at least half of those identified countries in the CRS report were either allied with or not hostile to the United States.[9] Moreover, no sub-state group has yet obtained NBC weapons from a state sponsor. Despite these facts, concern remains that someone, at some time in the future, may use these weapons against the United States.

The *National Strategy to Combat WMD* from 2002 did not specify adversaries, rather it called for a more aggressive campaign that eschewed arms control agreements and called for rolling back rogue states.[10] The Strategy promoted an interagency approach that expanded the military concept of counterproliferation into a national plan to include protection of the homeland. Starting around 1998, DOD developed plans to support the federal response to any domestic WMD incident, as well as plans to stop terrorist groups from obtaining and using chemical, biological, or radiological (CBR) hazards against U.S. security interests. In 2006, DOD released its *National Military Strategy to Combat WMD* that codified a CWMD framework that added WMD interdiction and elimination as new mission areas.

This approach to developing policy objectives and strategy failed to identify the operational context against which the armed services could understand and develop appropriate capabilities. With the generic term WMD as the object of strategy, rather than specific adversaries under specific operational contexts, one might assume that North Korea's nuclear weapons pose the same threat as Russia's, or that terrorist groups might develop or obtain chemical and biological weapons similar to those once maintained by the United States.

In its first term, the Obama Administration attempted but failed to update the *National Strategy to Combat WMD* from 2002; it is unclear whether the effort was poorly managed or just not a top priority. DOD forged ahead and in 2014 published the *DOD Strategy for Countering WMD* that articulated USG policy objectives to prevent WMD acquisition, to contain and reduce WMD threats, and to respond to WMD crises. The Strategy identified policy objectives more appropriate to the interagency—not just DOD—and, perhaps surprisingly, omitted references to counterproliferation and counterterrorism. By omitting these terms, DOD leaders thought that the counterproliferation and counterterrorism communities would interpret their mission requirements accordingly without having to change their existing

operational plans. Ironically, these operational plans were based on the *National Strategy to Combat WMD* from 2002 and the *National Military Strategy to Combat WMD* from 2006.

The *DOD Strategy for Countering WMD* from 2014 retained the generic focus on WMD but also emphasized the development of specialized capabilities to prevent the use of WMD. This new emphasis might have been more appropriate had the strategy been cast as a national strategy. As released, the strategy transforms certain national foreign policy missions into a DOD crisis management responsibility that is unrealistic, cannot be executed, and handicaps military leaders with its substantial ambiguity.[11] As many as three assistant secretaries of defense and three combatant commands must address the WMD challenge, which also involves multiple (and diverse) agencies across the executive branch. The Joint Staff updated Joint Publication 3–40 *Countering Weapons of Mass Destruction* later that same year to clarify the strategy's intent to the operational forces.

Advocating for Major Combat Operations

Adversaries armed with NBC weapons have not attacked U.S. forces since World War I, potentially as a result of our demonstrated deterrence capability and effective defensive countermeasures, or the restraints imposed by diplomatic nonproliferation agreements. This nonuse has contributed to a degree of complacence within the armed services to the extent that the United States is not prepared for NBC weapon attacks against its armed forces. The 1991 Persian Gulf War highlighted many critical deficiencies, such as the lack of modern protective suits and masks, biological agent detectors, modern decontaminants, and collective protection systems.[12] Many improvements and reforms were later made but critical deficiencies persisted into 2002, as U.S. ground forces prepared to return to Iraq, and arguably still exist owing to our recent, extended focus on non-conventional military operations.

Chemical, biological, radiological, and nuclear (CBRN) defense measures and CWMD operations

Figure 2: Strategic and Operational Guidance on CWMD.

differ on a matter of scale. The traditional DOD view of CWMD includes support to nonproliferation activities (proliferation prevention), counterproliferation (this includes offensive and defensive capabilities), and consequence management (now called incident response). DOS leads nonproliferation and arms control activities, with support from the Office of the Secretary of Defense (OSD), the Joint Staff, and the Defense Threat Reduction Agency (DTRA). For the most part, nonproliferation and arms control efforts have reduced the number and scope of adversarial WMD programs. DOD must continue to support these efforts, but should not take the lead in efforts to prevent WMD acquisition.

Counterproliferation—a term that is no longer in vogue within DOD—requires constant attention and long-term management. Earlier counterproliferation activities included offensive actions against WMD production and storage sites, defensive countermeasures for military forces, and theater air/missile defense systems. This most recent strategy indirectly refers to these capabilities, but not as an aspect of military combat operations. USSOCOM has significant responsibilities for the first area, and the Missile Defense Agency has responsibility to develop the last. Each of the armed services is responsible for training, organizing, and equipping its own forces with defensive countermeasures such as CBR detectors, individual protective suits and medical treatments, decontamination systems, and collective protection shelters. The U.S. Army is the DOD executive agent for managing these systems under the joint DOD Chemical and Biological Defense Program.

Despite these efforts, shortfalls exist. DOD continues to struggle to integrate collective protection into defense platforms, and military units eschew training with resource-intensive decontamination systems. Protective suits and masks are effective, but at a detriment to operational performance. DOD lacks the capability to destroy chemical or biological weapons in storage sites without causing collateral damage to nearby civilian population centers. DOD needs to better understand how short-range ballistic missiles that are destroyed *en route* to their targets might disperse their chemical or biological payloads on friendly forces or civilian population centers. Interdiction exercises focus on nuclear missile and ballistic missile parts and are almost exclusive to maritime operations. WMD elimination does not exist beyond a limited capability within the U.S. Army (the Syria elimination effort was an ad hoc operation, not a planned activity).[13] And although CBRN incident response is well-defined, execution is constrained by the low-density/high-demand nature of specialty units, as well as the tyranny of timeliness for both homeland and overseas terrorist incidents.

The armed services continue to struggle to measure their readiness for WMD threats, and historically have allowed a readiness gap right up to the point of active military conflicts. Service leaders have not been strong advocates for CWMD capabilities, even as they apply to force protection. There are always other perceived higher priorities that need resourcing, and the need to counter–WMD is often seen as someone else's mission and not a fundamental service responsibility. The DOD budget process can identify capability gaps; however, absent a champion with four stars, overcoming these gaps will not be a priority prior to the onset of military crises.

Clarifying the Issue of Irregular Warfare

Irregular warfare is generally defined as including counterterrorism, counterinsurgency, unconventional warfare, stability operations, and foreign internal defense. Each of these may entail an adversary using NBC weapons or CBR hazards against U.S. national security interests. The Joint Operating Concept for Irregular Warfare, published in 2010, fails to mention WMD threats, other than to note that WMD is an aspect of the future operating environment.[14] This is worrisome, particularly given how many politicians

have confided the threat of nuclear terrorism keeps them up at night. Joint Publication 3–05 *Special Operations* identifies CWMD as a core activity for USSOCOM, noting that "access to WMD significantly increases terrorists' capacity to install fear," and the need to watch for any "nexus of WMD and transnational violent extremist organizations."[15]

Publically available information gives little insight as to what this means, or how prepared USSOCOM is to execute this mission. While the consequences of a terrorist nuclear incident would be significant, chemical- or biological-related terrorism incidents are far more likely.[16] Yet there is little on the possibility of using special operations forces to target state-led WMD programs through unconventional warfare methods.[17] Literature on responding to CBR incidents is far more abundant than that on interdicting those sub-state actors intending to release CBR hazards. DOD guidance on special operations and irregular warfare have yet to be revised to better explain how USSOCOM intends to address policy objectives for addressing WMD issues within irregular warfare operations.

DOD guidance on special operations and irregular warfare have yet to be revised to better explain how USSOCOM intends to address policy objectives for addressing WMD issues within irregular warfare operations.

Among the greatest of challenges in discussing CWMD within the context of irregular warfare is the identification of threat sources and capabilities. Frequently the threat is generalized as "some terrorist group" that intends to develop CBR hazards or nuclear devices as weapons, without specifying an organization or its capabilities. A sub-state group could obtain CBR hazards sufficient to conduct a small-scale incident that does not inflict mass casualties. However, the likelihood that a sub-state group could obtain military-style chemical or biological weapons to inflict mass casualties is low, given the technical sophistication necessary. It is very unlikely a sub-state group could obtain a nuclear device or the necessary fissile material for an improvised nuclear device. A robust USG effort, aimed at preventing sub-state groups from obtaining fissile material or transporting a nuclear device, might be part of the reason.[18]

There are a few examples of sub-state groups developing and using military-grade chemical agents. Aum Shinrikyo used sarin nerve agent in 1994–95 in two separate attacks in Japan, and in 2016 the Islamic State of Iraq and the Levant (ISIL) used crude mustard agent against Kurdish and Iraqi forces. While chemical weapons are a WMD, it would be inaccurate to credit either Aum Shinrikyo or ISIL as having a WMD program. A true WMD program reflects an effort to develop militarily-useful, unconventional weapon systems that can predictably kill or disable thousands in selected areas of the battlefield. The IC and DOS have quietly begun to use the term "CBRN terrorism" rather than use the misleading term "WMD terrorism," reflecting how sub-state groups have not yet demonstrated the capability to develop WMD on such a scale.[19] However USSOCOM (and most of DOD) retain "WMD terrorism," despite the inaccuracy of the term and its focus on the tool rather than the operational context. The U.S. military cracked down on ISIL after its use of mustard agent-filled munitions in 2016 because policymakers feared the precedent, not because ISIL had developed a WMD program (it had not).[20] Rather, the concern was the possibility that other sub-state groups would see chemical weapons as a viable option, leading to

more significant chemical weapons attacks against other U.S. national security interests.

This concern among U.S. policymakers is understandable—certainly unprotected civilians would be at risk from chemical (or biological) weapons if such an incident took place, and the panic caused by such an attack would have widespread repercussions. Just ask anyone who worked in a federal building in Washington D.C. about mail-handling processes after anthrax-laced letters killed five individuals and infected 17 others in November 2001. This was not a mass casualty attack, but the over-reaction to the threat was significant in terms of funding and resources.

A re-examination of CWMD issues in the context of irregular warfare is overdue for several reasons. Is the threat exaggerated? If so, is it because government officials are intentionally engaging in threat inflation? Or are they unwittingly confusing the rhetorical boasting of sub-state group leaders calling for WMD attacks with the actual capability of those groups? Our understanding of the challenge is limited by over-classification. Few outside of USSOCOM are familiar with its concept plan or its execution. The diminished threat of sub-state groups using CBR hazards may be as much the result of U.S. military counterterrorism efforts, as of USSOCOM's concerted efforts to deprive sub-state groups of WMD material and associated technologies. Alternatively, sub-state groups might be uninterested in experimenting with highly toxic weapons-grade material, given the availability of demonstrably lethal automatic rifles and conventional explosives. Finally, despite widespread fear, there is no evidence of rogue states giving violent sub-state groups unconventional weapons. This should be a continued focus area for the IC, however, the effectiveness of plans based on the concept of "WMD terrorism" should also be re-assessed in the context of actual terrorist capabilities and not worst-case scenarios.

In 2017 members of the Colorado National Guard and the Jordan Armed Forces participate in a CBRN defense exercise in Jordan. (U.S. Air National Guard/Michelle Y. Alvarez)

Right-Sizing Homeland Defense and Civil Support

Concern over terrorist use of chemical and biological agents in the United States did not begin on September 11, 2001—rather it was shortly after the Aum Shinrikyo Tokyo subway attack in 1995. In 1996, Congress approved the *Nunn-Lugar-Dominici Act* that directed DOD to help train and equip state and local government agencies to respond to acts of terrorism involving NBC weapons. In 1998, the National Guard Bureau proposed to then Secretary of Defense William Cohen that DOD establish what was later called WMD Civil Support Teams. Initially there were 10 teams formed to cover the nation, but in 2002, Congress directed in the Fiscal Year 2003 National Defense Authorization Act that at least one team reside in every state and territory of the United States—regardless of whether a domestic threat actually existed or how robust the state and local emergency response capabilities were.

In 2005, DOD released its *Strategy for Homeland Defense and Civil Support* that identified defense support of civil authorities as a key mission, and in particular, the capability to manage the consequences of CBRN mass casualty attacks.[21] DOD policymakers took an interesting approach assuming that three

nearly-simultaneous nuclear terrorist incidents should be the operational scenario for developing civil support capabilities, rather than the more likely scenario of a small scale, single incident involving industrial hazards. As a result of this scenario and Congressional interest, the DOD "CBRN Response Enterprise" has grown from an estimated 3,200 active, reserve, and guard personnel in 2003 to more than 18,000 military personnel today.[22]

Similar to the ambiguity concerning the threat of CBRN terrorism in irregular warfare operations, there is no identified threat source within or outside of the United States, other than the general concern that something could happen that might overwhelm the response efforts of state and local officials. Of course, DOD is not the lead agency for responding to a domestic CBRN incident. That responsibility falls to DHS, which will coordinate any federal response to a request by state officials for support in the case of a natural disaster or deliberate incident, to include an attack involving chemical, biological, or radiological hazards. Discussions have taken place concerning the role of the military in countering unconventional nuclear attacks or biological attacks against the homeland, which duplicate efforts by DHS and HHS, both having lead roles in those respective areas. One must then question the assumptions and risk management principles that have led to the retention of 18,000 military personnel on constant alert for a highly unlikely domestic CBRN incident. The CBRN Response Enterprise may be good politics, but it is not good policy.

USNORTHCOM and the Office of the Secretary of Defense focus their attention on defense support of civil authorities, but there are other important homeland security concerns about addressing the possible impact of WMD within the United States. For example, the U.S. military is responsible for the protection of people who live and work on military bases and in military facilities from a possible terrorist incident involving chemical, biological, or radiological (CBR) hazards. Another challenge is to ensure that critical defense infrastructure can still operate if targeted by a CBR incident.[23] Some believe that DOD should address pandemic disease outbreaks as a WMD response, despite the existence of significant programs within the force health protection community.

This is not to suggest that leaders within OSD or USNORTHCOM are unwilling or incapable of addressing these important policy issues. Rather, DOD does not have an adequate policy process that would allow for successful institutional de-confliction in these areas. There are offices that participate in reviews of the CBRN Response Enterprise but they fail to specify at what level DOD must maintain response forces, given the mature capabilities in other federal government agencies and other well-funded efforts supporting state and local emergency response forces. In particular, DOD needs to prioritize its CWMD capabilities for the warfight while smartly augmenting other government agencies' homeland security efforts, rather than to spread these limited resources over a large mission space.

Assigning a Lead Advocate for DOD

The assignment of USSOCOM as DOD lead for CWMD issues was not without controversy. In 2005, then Defense Secretary Donald Rumsfeld chose USSTRATCOM to integrate and synchronize combating WMD activities across the Department, reflecting on the command's global missions of nuclear deterrence and missile defense and the belief that USSOCOM was too narrowly focused on WMD terrorism. Rumsfeld thought the assignment necessary given the fumbled "WMD exploitation" mission in Iraq. General James Cartwright, then commander of USSTRATCOM, promptly relegated the day-to-day planning and operations to DTRA, which created the USSTRATCOM Center for Combating WMD (SCC–WMD) to conduct these activities.[24]

By most accounts, USSTRATCOM headquarters was not interested in managing a mission for which there were no assigned forces, and therefore no immediate operational priority. The command did sponsor (through DTRA) a bi-annual "global synchronization conference" that convened action officers from across DOD and including participants from the IC, Federal Bureau of Investigation, DOE, and other government agencies to discuss challenging issues requiring resolution at the general officer level. USSTRATCOM did also support the development and staffing of Concept Plan 8099, a general framework for the combatant commands' CWMD plans, beginning in 2006.[25] USSTRATCOM was not, however, a reliable advocate to address significant capability gaps, ironically the major one being how DOD should address WMD elimination missions—the *raison d'être* for the DOD advocacy role and a still undeveloped defense activity.

USSOCOM's acceptance of its lead role has been cautious. Initially USSOCOM was concerned that the transition would negatively impact its focus on counter-terrorism activities and did not want to accept USSTRATCOM's original charter in its entirety. USSOCOM does have an identified counterproliferation mission that dates to at least 1996 (a responsibility that changed to "countering WMD" in/around 2012) in addition to its engagement against terrorist organizations seeking WMD capability. However, this operational focus was strictly in support of discrete military operations, and counterproliferation has not been a top priority for USSOCOM for the past 13 years. USSOCOM does have an interest in assessing counterproliferation activities against current policy,[26] but it remains unclear as to whether it will engage DOD policymakers on the development of future strategy and policy objectives.

USSOCOM has since agreed to support the updating and synchronization of CWMD concept plans for the combatant commands, but not necessarily to advocate for the entire CWMD mission set. However, USSOCOM has agreed to continue the global synchronization conferences and develop a CWMD Fusion Center at DTRA, replacing the SCC–WMD that once served USSTRATCOM.[27] This is not an entirely new concept—the effort to develop situational awareness on WMD-related issues across the globe has ebbed and flowed for decades. The challenge is, and remains, one of data management. Even as nation-states and sub-state groups have drawn away from WMD programs, there remain hundreds if not thousands of possible research, production, and storage sites that might contribute to the development of NBC weapons. In addition, the growing industrial development of nation-states results in many state facilities that could be using "dual-use" material and technologies. And, if DOD and the interagency persist in including natural infectious diseases and nuclear reactors within the meaning of "WMD," there will be a tremendous amount of information to be gathered and sorted.

Conclusion

The current DOD CWMD strategy positions the Department to meet national policy objectives for which it is not resourced, reflecting a failure at the national level to scope the challenge as something other than a technical issue and to oversee the execution of WMD-related tasks throughout the whole-of-government. In part, this is because the term "WMD," which once had specificity in the arms control community, has been reduced to a political buzzword. When national security professionals refer to the Ebola outbreaks in West Africa and the Fukushima nuclear reactor disaster as "WMD incidents," there is a serious problem.

This further reflects the need to define what DOD sees as important CWMD activities. Is the Department's intent to focus on preparing to face nation-states armed with NBC weapons? If so, DOD has a good idea of who those adversaries are

and how to do that. However, when expanded to global terrorism concerns, the challenges become much more diffuse. To what degree should DOD duplicate or augment the efforts of other federal, state, and local agencies? Most importantly, how do the armed services measure their own readiness to meet this threat? The challenge is acerbated by how CWMD policy is spread across three very different operating concepts—major combat, irregular warfare, and homeland defense—and implemented by multiple communities.

USSTRATCOM largely ignored this challenge for a decade, but to be fair, the problems ran deeper than the failures of a four star advocacy role. CWMD policy requires the leadership and attention of the National Security Council (NSC), which must help clarify expectations beyond "stop WMD from being used." More specific context is required, and measures of effectiveness must be enumerated, given the unique mission areas envisioned by each community of interest and the varied roles played by other interagency partners. The Special Assistant to the U.S. President for WMD and Counterproliferation on the NSC would be an ideal agent to examine those interagency roles (and leads) and to improve our national response; however, the position is currently vacant.[28] At minimum, a presidential executive order could clarify the context for government agencies to address the WMD challenge, and from that, DOD might define a more realistic, precise, and deliberate CWMD strategy.

Because civilian and military leaders are so focused on immediate crises and conventional threats, a highly-placed advocate with a broad vision and interagency contacts is needed to monitor and improve U.S. military CWMD capabilities. Without an advocate, the individual services will not, on their own, address these policy failures and capability gaps. USSOCOM as that advocate could succeed by working with each of the armed services on improving their counterproliferation capabilities for major combat operations, clarifying and highlighting counterterrorism and counterinsurgency plans directed toward countering CBR terrorism, and supporting the development of adequate (and not overly robust) capabilities for homeland defense. PRISM

Notes

[1] Dan Lamothe, "Special Operations Command Takes a Lead Role in Countering Weapons of Mass Destruction," *Washington Post*, December 23, 2016, available at <https://www.washingtonpost.com/news/checkpoint/wp/2016/12/23/special-operations-command-takes-a-new-lead-role-countering-weapons-of-mass-destruction/?utm_term=.bcb1ea477685>.

[2] USSTRATCOM Public Affairs, "USSOCOM Deputy Commander Visits USSTRATCOM," January 23, 2017, available at <http://www.stratcom.mil/Media/News/News-Article-View/Article/1056873/ussocom-deputy-commander-visits-usstratcom/>.

[3] Daniel Gerstein, "SOCOM Will Soon Lead the Pentagon's Anti-WMD Efforts. Here's What It Still Needs," *Defense One*, February 10, 2017, available at <http://www.defenseone.com/ideas/2017/02/socom-will-soon-lead-pentagons-anti-wmd-efforts-heres-what-it-still-needs/135331/>.

[4] These positions include the ASD for Nuclear and Chemical and Biological Defense, the ASD for Global Security Affairs (GSA), and ASD for Special Operations/Low Intensity Conflict. The WMD policy responsibilities within ASD (GSA) have since been transferred to the ASD for Homeland Defense and Security Affairs.

[5] While it is true that both the Clinton and George W. Bush Administrations had concerns about biological threats, the Obama Administration was the first to formally include natural disease outbreaks as a new category of WMD. This was first initiated in Presidential Policy Directive–2: *National Strategy for Countering Biological Threats* from December 2009 and then through subsequent actions within the Office of the Secretary of Defense.

[6] The Joint Concepts can be found in the Joint Electronic Library, available at<http://www.jcs.mil/Doctrine/Joint-Concepts/Joint-Concepts/>.

[7] *Hearing on Worldwide Threats Before the U.S. Senate Committee on Armed Services*, Feburary 9, 2016, 114th Congress (2016) (statement of Director of National Intelligence, James R. Clapper), available at <https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf>.

[8] DOD, *Proliferation: Threat and Response*, (Washington DC: GPO, 2001), available at <https://fas.org/irp/threat/prolif00.pdf>.

[9] Paul Kerr, "Nuclear, Biological, and Chemical Weapons and Missiles: Status and Trends," (Washington DC: CRS, February 2008), available at <https://fas.org/programs/bio/resource/documents/CRSreportNBCweapons2-08.pdf>. The report has not been updated since 2008, to the author of this manuscript's knowledge.

[10] Paul Bernstein, John Caves, and Seth Carus, *Countering Weapons of Mass Destruction: Looking Back, Looking Ahead*, CSWMD Occasional Paper 7 (Fort McNair, DC: NDU Press, October, 2009).

[11] Al Mauroni, "This Is Not the WMD Strategy You're Looking For," *War On the Rocks*, July 8, 2014, available at <https://warontherocks.com/2014/07/this-is-not-the-wmd-strategy-youre-looking-for/>.

[12] GAO, "Chemical Warfare: Soldiers Not Adequately Trained or Equipment to Conduct Operations on a Chemical Battlefield," T-NSIAD-91-18, April 16, 1991, available at <http://www.gao.gov/products/T-NSIAD-91-18>.

[13] Al Mauroni, *Eliminating Syria's Chemical Weapons* (Maxwell AFB, AL: USAF CUWS, 2017), available at <http://cuws.au.af.mil/pub/pdfs/monographs/58MauroniElimSyriaCW.pdf>.

[14] DOD, Joint Operating Concept for *Irregular Warfare: Countering Irregular Threat*, (Washington DC: Joint Staff, 2010), available at <http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v2.pdf?ver=2017-12-28-162021-510>.

[15] DOD, Joint Publication 3-05 *Special Operations* (Washington DC: Joint Staff, 2014), II-7.

[16] Ibid. Todd Masse, "Nuclear Terrorism Redux: Conventionalists, Skeptics, and the Margin of Safety," Orbis 54, no. 2 (2010), 302–19.

[17] LTC Walter Herd, "Current Unconventional Warfare Capability versus Future War Requirements," U.S. Army War College, 2002.

[18] See The National Security Archive's "Nuclear Terrorism: How Big a Threat?" for descriptions of select U.S. nuclear counterterror efforts, available at <https://nsarchive2.gwu.edu/nukevault/ebb388/>.

[19] Bureau of Counterterrorism, U.S. State Department "Country Reports on Terrorism 2016, Chapter 4: The Global Challenge of Chemical, Biological, Radiological, or Nuclear (CBRN) Terrorism," July 2017, available at <https://www.state.gov/j/ct/rls/crt/2016/272236.htm>. See also the annual worldwide threat testimonies by the Director of National Intelligence before the U.S. Congress, available at <https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community>.

[20] Barbara Starr, "U.S.: ISIS detainee providing information on chemical weapons," CNN, March 9, 2016, available at <http://www.cnn.com/2016/03/09/politics/u-s-isis-detainee-providing-crucial-information-on-chemical-weapons/index.html>.

[21] DOD, *Strategy for Homeland Defense and Civil Support* (June 2005), available at <https://fas.org/irp/agency/DOD/homeland.pdf>.

[22] Johnny Lairsey, "The CBRN Response Enterprise in the Homeland," *Small Wars Journal*, August 1, 2012, available at <http://smallwarsjournal.com/blog/the-cbrn-response-enterprise-in-the-homeland>.

[23] See David Bailey et al, "Protection of Department of Defense Facilities from Airborne CBR Threats," U.S. Army Engineer Research and Development Center, 2002.

[24] See comments by Deputy Secretary of Defense Paul Wolfowitz in National Defense University's Center for Counterproliferation Research-led report "*At the Crossroads": Counterproliferation and National Security Strategy* (Washington DC: NDU, April 01, 2004). "STRATCOM to lead DOD WMD efforts," by Jeffrey Lewis, in *ArmsControlWonk* (blog). February 5, 2005, available at <http://lewis.armscontrolwonk.com/archive/425/stratcom-to-lead-DOD-wmd-efforts/>.

[25] NTI, "Rumsfeld Considers 'CONPLAN' to Combat WMD," June 9, 2006, available at < http://www.nti.org/gsn/article/rumsfeld-considers-conplan-to-combat-wmd/>.

[26] See for instance "SOCOM J5 Key Strategic Issues as of 4 Sep 14" at <http://www.soc.mil/swcs/SWEG/_pdf/GRAD/USSOCOM%20J5%20Key%20Strategic%20Issues%20List.pdf/.

[27] Joseph Trevithick, "This Obscure DC-Area Office Helps US Special Operators Hunt Down and Secure Loose WMDs," *The Drive*, September 21, 2017, available at <http://www.thedrive.com/the-war-zone/14535/this-obscure-dc-area-office-helps-us-special-operators-hunt-down-and-secure-loose-wmds>.

[28] Dr. Christopher Ford occupied this position—a.k.a. the "WMD Czar"—from January–December 2017. In 2014, the incumbent was referred to as the "Senior Director for Defense Policy, Countering WMD, and Arms Control."

Sailors aboard the USS Ronald Reagan conduct a countermeasure wash down to remove potential contamination during Operation Tomodachi. (U.S. Navy/Nicholas A. Groesch)

CWMD Strategy Gap
Capacities, Capabilities, and Collaboration

By Margaret E. Kosal

In 1994, then Chief of Staff of the U.S. Army, General Gordon Sullivan, recognized the increasing threat of chemical, biological, and nuclear weapons and the capability gaps exposed by the challenges of operating in a weapons of mass destruction (WMD)-contaminated environment. Although threats from WMD are neither new nor unrecognized at the highest levels of the U.S. Government (USG) and Department of Defense (DOD), remarkable gaps and inconsistencies between strategic level policy and operational capabilities persist. During the past 15 years, countering–WMD (CWMD) has been a top priority as expressed throughout multiple national and department-level strategy and policy documents, to include the *National Security Strategy* (NSS); the *National Military Strategy* (NMS); the *National Defense Strategy* (NDS); the *Defense Strategic Guidance* (DSG); and Quadrennial Defense Review (QDR). While a prevention strategy is laudable and important, the disparity between strategy and the required operational capabilities and capacities needed for securing, interdicting, and eliminating WMD reveals potential gaps that must be recognized and accounted for to ensure a credible deterrent posture. Future threats, especially biological, are likely to be more complicated than current or past conceptions.

Strategic Context

The U.S. national security community and military services continue adapting to the evolving global environment. The strategic dialogue is shaped by multiple sources, to include the release this year of a new NSS and a new NDS; increased attention to the reemergence of great power competition; uncertainty on the role of combat operations in Afghanistan; an ongoing civil war in Syria; a resurgent Russia in the Crimea and elsewhere; multiple missile tests by North Korea and claims of new ballistic capabilities to reach the continental United States; and lingering opaque nuclear questions in Iran. In a 2015 statement, the Director of the Defense Advanced Research Projects Agency articulated a consensus of the future operational environment outlook as

Dr. Margaret E. Kosal is an Associate Professor in the Sam Nunn School of International Affairs at the Georgia Institute of Technology.

> *an extended period during which our national security will face a wide range of different types of threats from a wide range f different actors—nation-states are in the mix, but so too are terrorist organizations and criminal organizations and even individuals. And each of these—all of these different kinds of actors have—of course they have the conventional means of waging war, or inflicting damage, but now they also have some new tools. Cyber is a very obvious example. Many of these actors also have increasing access to weapons of mass destructions, or weapons of mass terror.*[2]

The perception of the threat of WMD from state and non-state actors continues to increase in scale, scope, and complexity.

Additional impacts on the strategic dialogue took form in new directions from the Trump Administration, a new Secretary of Defense with little public history of engaging the CWMD mission (unlike former Secretary of Defense Ashton Carter, who had long been involved in Cooperative Threat Reduction [CTR] and other nuclear nonproliferation policy work), ongoing questions about the federal budget and the continuing effects of sequestration, and the operational priorities required for a shift in the nation's strategic focus during the rebalance (or pivot) to Asia. As then Deputy Secretary of Defense, Ashton Carter articulated

> *Everything's on the table: roles and missions, war planning, business practices, force structure, personnel and compensation, acquisition and modernization investment, how we operate, how we measure and maintain readiness.*[3]

CWMD efforts consistently reveal gaps between strategy and available military options. CWMD is among the highest priorities for the U.S. domestic and the international security community in the 21st century.[4] Denying the acquisition and use of WMD by hostile states, sub-state actors, or non-state actors as part of nonproliferation and counterproliferation, coupled with possessing robust capacity to manage potential consequences are desired strategic ends. CWMD encompasses both conflict and post-conflict activities centered on securing and destroying material and delivery systems; but, more broadly, it also entails activities intended to address the associated programs, infrastructure, and expertise.[5] It includes activities that span the range of "prevent," "shape," "contain," and "respond" concepts.[6] CWMD proliferation involves a broad range of actors, materials, technologies, activities, and legal considerations all of which have implications on the roles of military and civilian government departments. Considerations such as risk, time sensitivity, geographic location, and international relations add greater complexity.

Prevention of WMD is a laudable and important goal, but disparities between that objective and the operational means required to secure, interdict, and eliminate WMD has resulted in capability gaps. Greater recognition is needed to affect strategy and additional levers at the policy level. Part of the challenge in narrowing the gap between CWMD strategy and its enabling capabilities and capacities is attributable to multiple endogenous and exogenous cultural, policy, and institutional factors.

Cultural, refers to the absence of a strong sense of "cultural ownership" of the problem set to and risk averse innovation posture that drives evolutionary technology development to differences in service and agency cultures; *Policy*, in which roles, responsibilities, authorities, and equities are spread across the different proponents to the highly compartmentalized nature of CWMD programs; Finally, *institutional*, refers to both internal and external inadequate improvisations for active

defense capabilities, for building partnership capacity (BPC), or for operational preparation of the environment activities.[7] For example, PL 103–160 restricts the Joint Chemical and Biological Defense Program to development of passive defense capabilities, which are not adequate improvisations for active defense capabilities. For multiple reasons, including history and organizational structure, there is de-prioritization of Joint Force Land Component Commanders roles in CWMD missions in some Joint Environment and Combatant Commands (e.g., USSTRATCOM). In many agencies and efforts, the emphasis has been historically and remains focused on efforts to "the left of boom," i.e., non-proliferation and arms control; the think tank, policy wonk, and scholarly world that serves as a gestation and holding venue for many who move into formal policy positions emphasizes nonproliferation efforts.

There are a number of organizations and agencies involved in these efforts, however a significant level of national capacity resides in the military. In particular, the national capacity—across the scientific, technical, operational, and tactical spectrum—and the most probable responsibility for executing missions to secure, exploit, and eliminate WMD are overwhelmingly in the U.S. Army. Serious efforts regarding prevention are relatively recent and only now beginning to coalesce, an observation highlighted as of 2009, where across the USG, DOD, and the U.S. Army, "the elimination mission is still in its infant stages, support among the services and commands is tenuous, and concepts and capabilities are still lacking."[8]

Case Studies

Ten cases studies illustrate the gaps between CWMD objectives and the joint force capabilities and capacities needed for attaining them. A set of significant variables (or strategic attributes) expounds upon the capacity, capability, and usability of components inherent in military force design. These CWMD historical cases have been divided into two sub-categories. "Major" cases include U.S.-led efforts where military forces played a major role. "Other" cases include examples of operations and disarmament efforts that were coordinated at the multi-national level, initiated or led by other nation-states; cases in which the United States provided significant assistance; or instances that were domestic law enforcement cases illustrative of future threat scenarios. Several non-military, non-combat cases are included because of the relative lack of military operations involving WMD. These "other CBRN/CWMD" cases illustrate the importance and role of the variables. While assessment of the cases is not a perfect analytical tool, they provide a useful representation of the major qualities of such operations. All were conducted in permissive or semi-permissive environments.

Case study selection focused on instances involving WMD elimination (WMD–E), CBRN–interdiction, CBRN–counterterrorism, or WMD consequence management (WMD–CM) efforts, including foreign consequence management.[9] The cases were selected as representative of the range of military operations involving at least one WMD. The screening criteria for case selection among each of the categories was that the operation had occurred after passage of the Goldwater–Nichols Department of Defense Reorganization Act of 1986, and the operation had a critical element that relied upon ground forces, i.e., strategic bombing or missile strikes alone would not accomplish the objective.

The "major" cases include U.S. and international efforts to detect, disarm, and dismantle former Iraq President Saddam Hussein's WMD program. That group is further divided into two different efforts that are considered separately. The first is the Iraq War and UN Special Commission (UNSCOM) that oversaw the destruction and

dismantlement of the 1990s-era program.[10] The second is comprised of CWMD operations associated with Operation *Iraqi Freedom* (OIF).[11]

TABLE 1: Major Cases.

Case	Year	Location
Operation *Desert Storm* and the UN Special Commission	1990–99	Iraq
Tirana	2003–07	Albania
Libya	2003–12	Libya
Operation *Enduring Freedom* (Tarnak Farms)	2002	Afghanistan
Operation *Iraqi Freedom*	2003–08	Iraq

The disarmament, destruction, and/or removal of WMD materials and agents from two states, Albania and Libya, are treated as individual cases. Specifically considered are the removal of nuclear materials and infrastructure from Tuwaitha and Tajoura, and the destruction of chemical weapons and infrastructure at Ruwagha and Jufra in the Libya case, and removal of 16 tons of Soviet-era chemical weapons stored in a bunker outside Tirana, Albania.[12] Pursuit of WMD by a non-state actor is the subject in the case of al-Qaeda's training camp, Tarnak Farms, located in the Kandahar vicinity of Afghanistan during Operation *Enduring Freedom* (OEF).[13]

The "other" cases include an example of foreign consequence management in which the U.S. military was called upon for assistance, Operation *Tomodachi* in response to the Fukushima Daiichi radiological disaster after the 2011 tsunami following an earthquake off Japan's eastern shore.[14] While the United States was not asked to assist in consequence management in Chernobyl, the capabilities and capacities needed for a Chernobyl-type nuclear disaster are also assessed.[15] Chernobyl was selected to show an example of scope and scale in civilian nuclear disaster that far exceeded Fukushima.

TABLE 2: Other Cases.

Case	Year	Location
Operation *Tomodachi* (Fukushima Daiichi)	2011–12	Japan
Chernobyl	1986	Ukraine
Goiânia	1987	Brazil
Aum Shinrikyo	1993–95	Japan
William Krar	2003	United States

The remaining cases involve individuals or non-state actors. Aum Shinrikyo was a Japanese apocalyptic cult that is most well-known for the March 1995 attack on the Tokyo subway system using sarin nerve agent.[16] Aum Shinrikyo also pursued biological weapons. The Goiânia case refers to the 1987 radiological incident in which a vial containing radioactive material used for medical imaging, specifically the salt cesium-137 chloride, was found at an abandoned hospital site and removed by scavengers looking for scrap metal.[17] The theft and subsequent distribution of the radioactive material resulted in deaths, morbidity, and significant cleanup. The final case, William Krar, was an American domestic terrorist who pled guilty to federal charges of building and possessing chemical weapons.[18] Krar is an example of a lone wolf or loosely-networked individual who pursued WMD.

Although, Syria fell outside the formal criteria for inclusion in the review due to non-reliance on ground forces, the significant international efforts to remove Syria's declared CW stocks and subsequent destruction at sea are worthy of consideration. Among the five variables, "niche capabilities" was the single variable deemed as vital. Destruction of the chemical weapons via neutralization aboard the MV *Cape Ray*, part of the civilian U.S. Maritime Administration's Ready Reserve Fleet that can be rapidly activated to support DOD or emergencies, necessitated adaptation

and demonstration of significant technical capability before deployment. This was accomplished primarily by the U.S. Army's Edgewood Chemical and Biological Center (ECBC), whose mission is to ensure operational readiness by protecting the warfighter from non-medical chemical and biological threats. This unity of effort extended beyond the services and the DOD to the U.S. State Department and international partners, including the Organization for the Prohibition of Chemical Weapons (OPCW), the international organization responsible for implementation of the Chemical Weapons Convention.

Case Study Attributes

These 10 cases were then examined against five critical force design attributes—strategic reach; dispersed objectives; unity of effort; interoperability; and niche capability—to assess strategic gaps between capabilities and capacities to execute C–WMD operations.

Strategic Reach (See Table 3)

The need for strategic reach varied across the cases. The major cases include three with a significant military element during or after major combat operations and two cases in which the military played a role because comparative capability or capacity did not exist within other parts of the USG. Across the major cases, the need for capability and capacity in a timely manner was insignificant due to the permissive or semi-permissive environment or relatively small amounts of material which already existed. In Operation *Desert Storm*, OEF, and OIF, strategic reach was enabled as part of a major operation under which the CBRN-related mission was pursued. Capability was often improvised and capacity was assembled in response to an event or discovery of CBRN materials, rather than in a proactive manner reflecting organic capabilities integrated into the force.

Strategic reach varied greatly across the domestic and foreign consequence management (FCM) cases. During Operation *Tomodachi*, strategic reach was vital because of the nature of the accident to which the U.S. was responding. In the cases of Chernobyl, Goiânia, and Aum Shinrikyo, strategic reach was assessed as vital from the perspective of the responding state (not the United States). Like *Tomodachi*, a domestic nuclear accident such as Chernobyl, domestic radiological incidents like Goiânia, and domestic chemical (as well as biological) incidents perpetrated by non-state actors demand a timely response for several reasons. First, radiation release must be controlled or limited and further degradation of the nuclear infrastructure at the site prevented to the maximum extent. Second, hazardous material (radioactive and chemical) must be recovered to limit further contamination. Finally, personnel

TABLE 3: Strategic Reach as a Critical Force Design Attribute.

Definition	Benchmark	
The capability and capacity for timely response to a full range of contingencies around the world.	Vital	Capability and capacity present while timeliness of response driven largely by adversary actions.
	Critical	Capability and capacity present while timeliness of response controlled largely by friendly factors.
	Important	Capability and capacity present, but timeliness of response is a lesser degree.
	Insignificant	Capability is present but capacity and timeliness of response are a lesser degree.
	Negligible	Not required.

TABLE 4: Dispersed Objectives as a Critical Force Design Attribute.		
Definition	**Benchmark**	
The ability to operate in a synergistic manner across multiple operational objectives and vast geographic areas.	Vital	Multiple objectives requiring simultaneous operations.
	Critical	Multiple objectives requiring sequential, but not simultaneous, operations.
	Important	Series of objectives that do not require close coordination.
	Insignificant	Single objective.
	Negligible	Not required.

suffering from exposure must be treated. In the William Krar case involving improvised chemical weapons devices and delivery, interdiction occurred prior to weapon employment without any indication of specific intent or plan to use the devices. While strategic reach was not significant in the major cases, it was vital in the other cases, thereby demonstrating the need for a timely response to a full range of contingencies around the world.

Dispersed Objectives (See Table 4)

The ability to respond to dispersed objectives was important based on the broad geographical scope of the operation. Across the major cases, the majority involved only one or a limited number of sites. Additionally, the CWMD response did not require close coordination of operations. In the other cases (FCM, domestic terrorism), the attribute was assessed as insignificant due to the limited scale or constrained geography of the area of operations. It is unlikely that future non-state actor adversaries will remain this one-dimensional.

Unity of Effort (See Table 5)

The major CBRN cases illustrate the critical nature of unity of effort across DOD, the USG, and the multi-national community. For example, the Department of Energy and the International Atomic Energy Agency (IAEA) provided capabilities in the cases involving nuclear materials such as Desert Storm/UNSCOM, Libya disarmament, and Operation McCall, which removed 550-tons of low-grade uranium from Iraq in 2008. Similarly, across all four of the major chemical weapons cases, international community involvement was necessary either as part of the UN-mandated operation or via the OPCW, which oversees destruction of

TABLE 5: Unity of Effort as a Critical Force Design Attribute.		
Definition	**Benchmark**	
Coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization—the product of successful unified action.	Vital	Requires shared understanding of the objectives across force, joint, interagency, and multinational environments.
	Critical	Requires shared understanding of the objectives across force, joint, and interagency environments.
	Important	Requires shared understanding of the objectives across force and joint environments.
	Insignificant	Requires shared understanding of the objectives across force.
	Negligible	Not required.

Source: Unity of effort definition as described by Joint Chiefs of Staff, Joint Pub 1–02, 304.

chemical stockpiles under the Chemical Weapons Convention (CWC). The Tarnak Farms case was essentially a site exploitation with respect to attempted biological development and acquisition. Such a case highlights an unresolved issue regarding the lack of a standing multinational body at the international level tasked with the biological weapons mission. After Operation *Desert Storm*, destruction of the Iraqi stockpiles was overseen by the UN-mandated operation, which required passage of a UN Security Council Resolution and creation of an ad hoc organization. There is no existing international partner charged with biological weapons elimination.

In the non-military and non-state actor cases, unity of effort was assessed as insignificant largely due to the domestic scope and scale of response or the unwillingness of the nation, e.g., the former Soviet Union, to acknowledge the incident. The exception is Operation *Tomodachi*, which involved coordination and cooperation across Japanese domestic law and emergency response, Japan's Self-Defense Forces, U.S. forces, the IAEA, and Tokyo Electric Power Company—the largest privately owned electric utility in the world. Operation *Tomodachi* should not, however, be seen as the model or most likely scenario for a CBRN–foreign consequence management (FCM) operation as the situation was permissive both in terms of close relationships between the nation-states and uniformed military and in the nature of Japanese civil society. This unique case may not reflect the most likely CBRN–FCM scenario to which the United States might be called in the future.

Interoperability (See Table 6)

Interoperability is assessed as critical for CBRN operations executed in other than permissive environments. The lack of joint CBRN capabilities interoperability in *Desert Storm* prompted the creation of the Joint Chemical and Biological Defense Program (CBDP) in the National Defense Authorization Act for Fiscal Year 1994. The CBPD consolidated responsibility and authority for capabilities development in the Office of the Secretary of Defense rather than in the services. With the exception of Operation *Tomodachi*, in the other non-major cases the success or limits of interoperability were assessed to be insignificant due to the relatively small scale or scope of the operations.

TABLE 6: Interoperability as a Critical Design Force Attribute.

Definition	Benchmark	
The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.	Vital	Requires interoperability across force, joint, interagency, and multi-national environments.
	Critical	Requires interoperability across force, joint, and interagency environments.
	Important	Requires interoperability across force and joint environments.
	Insignificant	Requires interoperability across force.
	Negligible	Not required.

Source: Interoperability definition as described by Joint Chiefs of Staff, Joint Publication, 1–02, 146.

TABLE 7: Niche Capabilities as a Critical Design Force Attribute.		
Definition	**Benchmark**	
Identified special skills or materials required to efficiently and effectively accomplish objectives.	Vital	Panoply of special skills and materials ready to efficiently and effectively accomplish the mission.
	Critical	One or two special skills or materials available to efficiently and effectively accomplish the mission.
	Important	Special skills or materials, once identified, are scalable to efficiently and effectively accomplish the mission.
	Insignificant	Special skills or materials present, but not scalable to efficiently and effectively accomplish the mission.
	Negligible	Not required.

Niche Capabilities (See Table 7)

Niche or specialized capabilities and skills were assessed as vital based on the requirement for technical or material means and capacity. Each case required specialized detection, protection, and means to secure material physically for exploitation, elimination, or transport. In three of the major cases, specialized demilitarization capabilities were needed; in no case was capacity tested due to the relatively small scale of CBRN materials involved. All of the non-military cases needed specialized diagnostic, treatment, decontamination capabilities, and skills.

Insights

Trends for CWMD threats run parallel to a complex and uncertain future as the United States contends with rapid social and technological changes and sometimes limited understanding regarding the precise nature of the threat. Proliferation of WMD is characterized mainly by two drivers that exist in complementary yet separate conceptual spheres. The first consists of the characteristics inherent in countering nuclear threats.[19] Those characteristics drive policies to account for the knowledge and material proliferation of nuclear weapons capability. The second driver arises from the continued evolution of chemical, biological, and radiological (CBR) threats. This factor drives policies to account for innovation and technology diffusion of CBR capabilities. Current policy and joint publications have expanded the definition of proliferation to account for this duality, thereby resulting in a singular encapsulation of the problem.[20] The threat-actors who underlie these drivers consist of states and non-state actors. There is also potential for dynamic inter-play among these two variables spanning a range of state to state-sponsored to the extreme self-radicalized lone wolf ventures.

Policy trends in CWMD appear to be consistent with current approaches to strategy formulation. Policy is guided by objectives and priorities presented in various national level strategic documents involving security and CWMD such as the NSS and the NDS.[21] In keeping with a whole of government approach to security generally, and CWMD specifically, there is inherently an expansive and growing interagency portfolio regarding CWMD policy. The interagency contributive approach, and individual agency contributions to security and CWMD, exist at levels relative to the scope, authority, and mission designated for each department or agency. For example, the prominent policy component in CWMD is non-proliferation. The U.S. State Department leads this effort with policies and guidelines that attempt to prevent proliferation of associated technologies, materials, and knowledge.[22] In DOD, there are two main civilian focal points for CWMD policy—the Deputy Assistant Secretary of Defense (DASD) for CWMD and the Assistant Secretary of Defense (ASD)

for Nuclear, Chemical, and Biological (NCB) Defense. The DASD–CWMD performs activities pursuant to the goals of "prevent and counter global trafficking in WMD/missiles; protect and defend against WMD use and the proliferation of WMD; and respond by preparing for a post–WMD environment, and helping countries to build capacity and control ungoverned spaces, and attacking networks across all threats."[23] The ASD—NCB "is the principal advisor to the Secretary of Defense, the Deputy Secretary of Defense, and the Undersecretary of Defense for Acquisition, Technology, and Logistics for matters concerning nuclear, chemical, and biological defense programs."[24] There are no projected seismic shifts in their policy ownership or stated goals; however, policy is evolving to account for more activities prior to a crisis or incident and to reflect a "prepare, prevent, contain, and respond" approach toward reducing the threat of WMD.

Until recently, the vast majority of the CWMD operational capabilities was resident in U.S. Strategic Command (USSTRATCOM). The Standing Joint Force Headquarters–Elimination (SJFHQ–E) was activated in February of 2012. It is an evolving organization that re-located from Aberdeen Proving Grounds, Maryland to Fort Belvoir, Virginia, where it initially co-located with the USSTRATCOM Center of Combating WMD (SCC–WMD) and the Defense Threat Reduction Agency (DTRA). These developments suggest institutionalization of an organizational capability to enable and facilitate WMD-Elimination missions. Challenges remain, but the relocation of SJFHQ–E to reside in the same building as DTRA clearly creates a potential for synergies during missions to enable and facilitate elimination of WMD activities, especially in non-permissive environments.[25]

The U.S. Special Operations Command (USSOCOM) plays a critical role in CWMD from a counterterrorism and counterproliferation perspective. In 2014, USSOCOM was assigned additional responsibilities for the CWMD mission space. In 2016 responsibility for coordination of the CWMD mission across DOD transferred from USSTRATCOM to USSOCOM.[26] While the responsible institutions and physical locations of many technical and operational capabilities for CWMD have not substantially changed, USSOCOM's assumption of the lead role for coordinating CWMD activities presents yet another organizational challenge. Last year the Congressional Research Service identified a number of potential issues, to include authorities, mission focus, and resourcing, associated with transfer of the coordination role for CWMD.[27] A year later, these challenges remain as reiterated during a conference discussion by a panel of Special Operations Forces experts.[28]

An increasing number of organizations will have to work together to define the future of CWMD operations. The CWMD mission requires a whole-of–government approach as various capabilities reside in different government organizations. These agencies will need to integrate with standing units, like USSOCOM and missile defense. Finally, the technical nature of the CWMD mission highlights the important relationship between operational forces and the defense science and technology enterprise that supports it.

Being able to respond in a timely and coordinated manner is likely to be an increasingly important factor in execution of CWMD operations. In the case studies, the low assessment of capacity to respond to dispersed objectives was largely a function of the permissive to semi-permissive environments that characterized those operations. Scenarios involving increasing numbers of dispersed WMD sites requiring timely response can be expected in the future. The capability and capacity to seize, assess, and secure as many, if not all, potential WMD sites in a timely—*days not weeks*—and simultaneous manner is critical for limiting

proliferation of WMD, particularly in an unstable, unknown, or non-permissive environment.

Operational capabilities continue to trend toward a need for interagency—and in some cases international—design using a whole-of-government approach, which must begin by accounting for the number of interagency members that possess CWMD capabilities and expertise, albeit with varying levels of capacity. From a national perspective, there is value in the size and diversity associated with the national CWMD enterprise. As new threats and challenges arise, the dynamics of having as many as 16 interagency partners focused upon generating viable policy options is considered a model to sustain, especially as CWMD may or may not be the principal driver in a strategic dilemma. The interagency approach serves to protect the unique nature of each agency's CWMD-associated programs, while positioning national policymakers with an ability to generate whole-of-government approaches derived from the contributive efforts of their agency's fielded expertise. Such an approach demonstrates a desire to sustain flexibility within the strategic framework that suggests more value can be obtained from practical coordinating functionality than through designation of proponency for a given function. Within the Joint Force, proponancy for various CWMD missions continues to trend toward Geographic Combatant Commands with specified roles for Functional Component Commands as outlined in Joint Publication 3–40, *Countering Weapons of Mass Destruction*.

The CWMD mission also reinforces the need for strategic reach of services. The collapse of regimes with large stockpiles of chemical, biological, radiological, or nuclear weapons; the theft of WMD by a non-state actor; or the consequence management needed to mitigate a WMD attack will require a rapid response for greatest impact. This could in turn, require the re-evaluation of the nation's strategic mobility assets and rapid deployment models.

Unity of effort across the USG with respect to CWMD is likely to be increasingly important and also increasingly difficult to achieve. The likelihood of future WMD proliferation, combined with importance of the CWMD mission for national security presents a problem on which multiple organizations can both identify and provide focus. The challenge in achieving effective cooperation towards a common set of objectives occurs when the involved organizations have different perspectives on the importance of the variables associated with the problem at hand. Put another way, the sheer number of agencies likely to be involved in the CWMD mission will naturally result in a certain amount of bureaucracy that can be difficult to work through when attempting to coordinate efforts toward a common objective.

Trends in CWMD technical capabilities continue to reflect an approach to research and development that focuses on niche requirements. Technical capabilities are pursued through an array of partnerships and programs to address the varied challenges associated with WMD. These technical efforts are at times disparate, given the varied customer base and needs associated with the CWMD enterprise, which includes identification to elimination requirements for situations that range from episodic to enduring. In the military, capabilities development is pursued through identification of anticipated or current needs from Unified Commands through the joint requirements process.[29] Working groups exist to flatten the enterprise knowledge of technical capabilities, which is essential moving forward to address the variance in CWMD problem sets, each of which requires a unique approach. The potential for increases in the number of systems and forces involved in CWMD will add complexity. Larger and more varied involvement also raises the importance of interoperability when attempting to provide or accept services between disparate organizations.

A Spanish patrol boat escorts the USG-owned MV Cape Ray through the Strait of Gilbraltar en route to the Mediterranean Sea. The USG modified and deployed the Cape Ray to dispose of Syrian chemical agents. (U.S. Navy/Desmond Parks)

CWMD has historically been a country-based problem, as illustrated by the long-standing challenges in places such as North Korea, Iran, and Syria. Accordingly there is an obvious need for attention to the risks associated with episodic or enduring WMD threats from state actors. However, the range of potential adversaries has expanded to non-state actors since the last quarter of the 20th century. Niche capabilities needed for CWMD are likely to proliferate, while at the same time, the need for greater coordination and integration of capacities, capabilities, and actors involved in guiding and implementing CMWD tasks will only rise. In response there has already been a bifurcation of CWMD organizations, operational constructs, and policy to limit acquisition and respond to use by states versus non-state actors, most prominently in the interagency. In addition, policy dialogue is attempting to better define the problem space that exists between counterterrorism and counterproliferation and to develop solutions for how best to align resources to address these separate but complementary challenges. An ability to respond to objectives that lie between traditional counterterrorism and counterproliferation, i.e. "minding the gap," may be needed to account for the variance in mission, focus, targets, time horizon, and modus operandi resident in the two missions. In view of trends which suggest more actors, not fewer, in response to the scope and scale of CWMD challenges, no one entity is seen as being able to singularly respond to

all facets of the problem. For that reason, CWMD mission success increasingly relies on joint constructs within DOD; USG interagency cooperation; and contributions from allied and partner nations.

Multiple efforts, both inside and outside the DOD, the Joint Staff, Army, the Combatant Commands, and the interagency community have delineated or are working to determine specific tactical and operational CWMD capability gaps, however the key force attributes for an expeditionary force structure that provides the requisite mix of security and CWMD capabilities has yet to be developed. Within the Army, for example, CWMD infrastructure and force structure initiatives are evolving to account for the shift in strategic focus.[30] Meanwhile, CWMD capabilities and capacity are subject to the same budgetary, structure, and infrastructure pressures visited upon the total force. The infrastructure trends suggest that CWMD capabilities will become overwhelmingly reliant upon a CONUS-based, deployable force. One foreseeable challenge involves how best to meaningfully integrate CWMD capabilities into existing force structure to improve response and readiness while simultaneously ensuring protection of the requirement for specialized training and certifications. The trend toward force structure change has obvious second-and third-order implications from a force design perspective. The DSG force sizing construct—the overall capacity of the joint force—from 2012was based on the requirements to conduct counterterrorism and irregular warfare; deter and defeat aggression in two places simultaneously ("defeat and deny"); maintain effective nuclear deterrent; and defend the homeland and support civil authorities. While "counter weapons of mass destruction" is one of the 10 missions noted in the DSG, it is not an explicit factor in the force-sizing equation. As a result, CWMD as a component of force structure is subject to capability considerations, more so than capacity considerations, although opportunities exist for implicit association of CWMD force structure capability requirements with capacity. Infrastructural force array derived from a CONUS-based approach also produces challenges as to how best to integrate CWMD capabilities and capacity with maneuver forces, the laboratory base, and the interagency community. Significant focus should be placed on identification of technical capabilities and employment considerations required by forces to tactically secure and/or transport WMD sites at scale, including activities in contested areas or potential subterranean environments. Finally, investigation suggests there may be synergistic effect that can be achieved from co-location of tactical units with CWMD capabilities, along with a science and technology base.[31]

Conclusion

There are disparate efforts in CWMD at all echelons of the USG that result in a lack of prioritization, fusion, coordination, and oversight of efforts. Within the ground forces, capacity and capability are fractured and not wholly integrated into the conventional force. There is a need for greater technical capability and capacity, both within technical uniformed and civilian research and development.[32] Programmatically, a paucity exists of approaches to develop anything other than passive countermeasures. For example, active defense—interception of a threat agent en route including but not limited to missile-based interception—is perceived as too hard technically or not part of the dialogue, often due to varying conceptions of what such would entail.[33] Additionally, much greater cognizance of non-traditional agents (NTAs) and emerging threats—at the low and high ends of the technological spectrum—is needed to address technical and operational challenges and to enable strategic and operational flexibility to respond to new and unforeseen threats.

Internationally, a lack of willingness of other states to engage operationally and tactically in

CWMD, especially WMD–E, efforts carries implications that result in the United States, and often the ground forces effectively, "going it alone," which exacerbates capability and capacity gaps. CWMD and WMD–E military-to-military programs as part of "shaping" and "prevention" strategies and efforts of global engagement would increase global security in support of stated strategic objectives.[34]

There is a need to think strategically beyond current challenges. In the late 20th and early 21st century, the nation has struggled—and continues to do so—to deal with technologically-enabled proliferation challenges. Anticipating the types of threats that may emerge as science and technology advance, the potential consequences of those threats, and the probability that new and more diverse types of enemies will obtain or pursue them is necessary in preparing for the future security of the nation.[35] The potential synergies between biotechnology and other emerging technologies, like nanotechnology and the cognitive neurosciences, not only suggest tremendous potential for advancement in technology for military applications, but also raise new concerns.[36] In the 21st century, both nation-states and non-state actors will have access to new and potentially devastating dual-use technology.[37] Robust research and analysis (ranging from the academic to intelligence communities) and planning that bridges the gaps between the life and physical sciences, engineering, the social sciences, and the operational world is crucial for devising implementable and executable strategies that will better enable the United States to be prepared for the WMD challenges of the future.

In keeping with previous incarnations of U.S. strategic documents, the latest NDS released this year retains an emphasis on CWMD through a set of explicit and implicit objectives, including one for "dissuading, preventing, or deterring state adversaries and non-state actors from acquiring, proliferating, or using weapons of mass destruction."[38] Defense planning scenarios should account for CWMD maneuver and technical force requirements as they align objectives with capabilities. Defense Planning Guidance missions should bridge strategic to operational concepts and explicitly include CWMD activities, including seizing, securing, interdicting, exploiting, and elimination of large numbers of WMD sites, above and below-ground, in non-permissive environments. CWMD considerations, in light of the robust efforts by tactical and operational organizations and combatant commands, have yet to meaningfully evolve into substantive requirements or analysis that accounts for this mission as contributive to force sizing.[39]

Nuclear-based deterrence has consistently been part of the U.S. NSS since President Truman was in office. With an appreciation for the ever-evolving and uncertain security environment, the Nuclear Posture Review (NPR) released this year updates perspectives on U.S. efforts in support of the ultimate global elimination of nuclear, biological and chemical weapons.[40] The perspectives in this recent NPR confirm and reinforce an imperative for underpinning CWMD policy objectives with the credible capabilities and capacities needed to accomplish them. As a nation, we are still functioning under a structure that originated in the Cold War era. In the post–WWII and Cold War environments, the nuclear weapons-based construct was dominant with good reason. While the existential threat from Russia's nuclear weapon stockpile remains, there are also increasing threats from other actors and states. The roles, capabilities, and capacities required by ground-based forces to execute CWMD operations and to win against WMD-possessing states have not been part of the national-level strategic dialogue. Decisive action in CWMD operations should be stressed as a national-level capability. Credibly communicated capabilities and capacities to seize, secure, and eliminate WMD in non-permissive environments should be emphasized as part of wider

prevention strategies, of particular import against future adversaries that seek technologically-enabled, asymmetric means of conducting warfare against the United States. PRISM

Notes

[1] Joint Chiefs of Staff, *Joint Pub 1-02 Department of Defense Dictionary of Military and Associated Terms* (Washington, D.C. 2013). WMD) are defined as "chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties and exclude the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon." The 2010 Quadrennial Defense Review on page 4 asserts "The instability or collapse of a WMD-armed state is among our most troubling concerns. Such an occurrence could lead to rapid proliferation of WMD material, weapons, and technology, and could quickly become a global crisis posing a direct physical threat to the United States and all other nations.' The 2014 QDR on page 7 re-asserts: "We will remain focused on countering WMD, which undermine global security."

[2] DARPA Director Arati Prabhakar during Press Briefing from the Pentagon, April 24, 2015, available at <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5227>.

[3] Remarks by Deputy Secretary Carter at the Center for Strategic and International Studies, May 23, 2013, available at <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5245>.

[4] White House, *National Security Strategy*, United States of America, February 2015, available at <https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf>;White House, *National Security Strategy*, United States of America, May 2010, Available at <www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>; White House, *National Security Strategy*, United States of America, March 2006, available at<http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/>; White House, *National Strategy for Countering Biological Threats*, December 9, 2009, available at <www.whitehouse.gov/sites/default/files/National_Strategy_for_Countering_BioThreats.pdf>; White House, *National Strategy to Combat Weapons of Mass Destruction*, December 2002, available at <www.state.gov/documents/organization/16092.pdf>; *Department of Defense Strategy to Counter Weapons of Mass Destruction*, June 2014, available at <http://archive.defense.gov/pubs/DoD_Strategy_for_Countering_Weapons_of_Mass_Destruction_dated_June_2014.pdf>; Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America*, June 2015, available at <http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf>; Chairman of the Joint Chiefs of Staff, *National Military Strategy to Combat Weapons of Mass Destruction*, February 2006, available at <www.defense.gov/pdf/NMS-CWMD2006.pdf>; Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, March 2005, available at <http://govinfo.library.unt.edu/wmd/about.html>; Commission on the Prevention of WMD Proliferation and Terrorism (Graham-Talent Commission), *Prevention of WMD Proliferation and Terrorism Report Card*, 26 January 2010, available at <www.preventwmd.gov/static/docs/report-card.pdf. Weapons of Mass Destruction Commission (Blix Commission)>, *Weapons of Terror: Freeing the World of Nuclear, Biological, and Chemical Arms*, Stockholm, Sweden, June 1, 2006, available at <www.wmdcommission.org/files/Weapons_of_Terror.pdf>; *The Weapons of Mass Destruction Commission (WMDC)*, December 16, 2006, available at <http://www.wmdcommission.org/sida.asp?ID=110>; General Assembly, "Resolution Adopted by General Assembly," *United Nation's General Assembly*, January 3, 2007, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N06/498/63/PDF/N0649863.pdf>; *Secretary General of United Nations General Assembly*, "The United Nations and Security in a Nuclear-Weapon-Free World," Secretary-General's Address to the East-West Institute of the United Nations, October 24, 2008, available at <http://www.un.org/apps/sg/printsgstats.asp?nid=3493>; NATO, "Weapons of Mass Destruction," NATO, October 27, 2010, available at <http://www.nato.int/cps/en/natolive/topics_50325.htm>; NATO, "Chemical, Biological, Radiological, and Nuclear Defense Battalion," *NATO*, October 26, 2010, available at <http://www.nato.int/cps/en/natolive/topics_49156.htm>.

[5] Rebecca Hersman, *Eliminating Adversary Weapons of Mass Destruction: What's at Stake*, (National Defense University Press, Washington D.C., 2004).

[6] *Department of Defense Strategy to Counter Weapons of Mass Destruction*, June 2014, available at <http://archive.defense.gov/pubs/DoD_Strategy_for_Countering_Weapons_of_Mass_Destruction_dated_June_2014.pdf>

[7] Lonnie Carlson and Margaret E. Kosal, "Preventing Weapons of Mass Destruction Proliferation—Leveraging Special Operations Forces to Shape the Environment," JSOU Monograph, January 2017, available at< http://jsou.libguides.com/ld.php?content_id=28362821>.

[8] Center for the Study of Weapons of Mass Destruction, *Are We Prepared?* (National Defense University Press, Washington D.C., 2009), 58.

[9] Joint Chiefs of Staff, *Joint Pub 1-02*. WMD–elimination (WMD–E) is defined as "actions undertaken in a hostile or uncertain environment to systematically locate, characterize, secure, and disable, or destroy weapons of mass destruction programs and related capabilities," and WMD–consequence management (WMD–CM) is defined as "Actions authorized by the Secretary of Defense to mitigate the effects of a weapon of mass destruction attack or event and, if necessary, provide temporary essential operations and services at home and abroad." DoDI 2000.21 defines FCM as "assistance provided by the USG to an HN (host nation) to mitigate the effects of a deliberate or inadvertent CBRNE attack or event and to restore essential operations and services." CJCSI 3214.01B similarly defines FCM as "assistance provided by the USG to an HN to mitigate the effects of a deliberate or inadvertent CBRNE attack or event and restore essential government services." CJCSI 3214.01B specifies that its provisions do not apply to "CBRNE response operations that are a direct result of US military operations."

[10] "Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD," September 2004, available at <https://www.cia.gov/library/reports/general-reports-1/iraq_wmd_2004>.

[11] Unclassified Version of the Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Chapter One Case Study: Iraq, March 2005, available at <https://www.gpo.gov/fdsys/pkg/GPO-WMD/pdf/GPO-WMD-1-6.pdf>; Iraq Survey Group Final Report: Regime Strategic Intent—Key Findings," 2004, available at <https://www.cia.gov/library/reports/general-reports-1/iraq_wmd_2004/Comp_Report_Key_Findings.pdf>.

[12] Sharon Squassoni, Disarming Libya: Weapons of Mass Destruction, Congressional Research Service Report, September 22, 2006; Albert J. Mauroni, "Eliminating Syria's. Chemical Weapons," U.S. Air Force, Center for Unconventional Weapons Studies, Future Warfare Series, no. 58 (June 2017), available at <http://www.au.af.mil/au/cpc/pub/pdfs/monographs/58MauroniElimSyriaCW.pdf>; and John Hart, "The Smoking Gun of Non-Compliance," CBRNe World, December 2015, 17–20, available at <http://www.cbrneworld.com/_uploads/download_magazines/Syrias_Review_2015.pdf>. See also: Matthew V. Tompkins, "Albania's Chemical Weapons," *Nonproliferation Review*, 16, no. 1 (2009), 65–77.

[13] Rolf Mowatt-Larssen, "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" January 2010, available at <http://belfercenter.ksg.harvard.edu/files/al-qaeda-wmd-threat.pdf>; Melissa Finley and Jennifer Gaudioso, *Point of View: The Front Lines of Biological Weapons Non-Proliferation. Biological Threats in the 21st Century*, 417–424, available at <https://doi.org/10.1142/9781783269488_0025>; Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Chapter Three Case Study: Al-Qa'ida in Afghanistan, March 2005, available at <https://www.gpo.gov/fdsys/pkg/GPO-WMD/pdf/GPO-WMD-1-8.pdf>.

[14] Andrew Feickert and Emma Chanlett-Avery, "Japan 2011 Earthquake: U.S. Department of Defense (DOD) Response," Congressional Research Service, 22 March 2011; "Lessons Learned from Operation Tomodachi," available at <https://www.acq.osd.mil/dpap/ccap/cc/jcchb/Files/Topical/After_Action_Report/resources/Lessons_Learned_Operation_TOMODACHI.pdf>; "Chronology of Operation Tomodachi," National Bureau of Asian Research, available at <http://www.nbr.org/research/activity.aspx?id=121>.

[15] "Backgrounder on Chernobyl Nuclear Power Plant Accident, US NRC, May 2013, available at <https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/chernobyl-bg.html>; VF.Demin and B.I.Yatsalo, "Chernobyl" Lessons Learned for Post-Emergency Response," International Radiation Protection Program, available at <http://www.irpa.net/irpa10/cdrom/00885.pdf>; E. Buglova, J. Kenigsberg, " Analysis of Emergency Response After the Chernobyl Accident in Belarus: Observed and Prevented Medical Consequences Learned," available at <https://www.ipen.br/biblioteca/cd/go10anosdep/Cnen/doc/manu4.PDF>.

[16] Richard Danzig, Marc Sageman, Terrance Leighton, Lloyd Hough, Hidemi Yuki, Rui Kotani and Zachary M. Hosford, "Aum Shinrikyo: Insights Into How Terrorists Develop Biological and Chemical Weapons," Center for New American Security, 2012, available at <https://www.cnas.org/publications/reports/aum-shinrikyo-second-edition-english>; and DE Kaplan, "Aum Shinrikyo" (1995) in Tucker JB, editor. Toxic terror: Assessing terrorist use of chemical and biological weapons, MIT Press, 2000.

[17] J.L. Lipsztein, P.G. Cunha, and C.A. Oliveira, "The Goiania Accident: Behind the Scenes," Health Physics, 60:1, 1991; "The Radiological accident in Goiânia," Vienna: International Atomic Energy Agency, 1988, available at <https://www-pub.iaea.org/MTCD/publications/PDF/Pub815_web.pdf>; and F. Steinhäusler, "Countering Radiological Terrorism: Consequences of the Radiation Exposure Incident in Goiania (Brazil)" in I. Khripunov, L. Bolshov and D., Nikonov, (eds) Social and Psychological Effects of, Radiological Terrorism, Volume 29 *NATO*

Science for Peace and Security Series: Human and Societal Dynamics, November 2007.

[18] M.E. Kosal, "Near Term Threats of Chemical Weapons Terrorism," *Strategic Insights*, v. 5, issue 6 July 2006; and Reynolds, J. Michael, "HomeGrown Terror" Bulletin of Atomic Scientists, November 2004, 60:6, 48–57.

[19] Proliferation is defined as "the transfer of weapons of mass destruction, related materials, technology, and expertise from suppliers to hostile state or non-state actors," (JP 1-02). The definition was modified from early policy iterations to account for more than nuclear weapons. The term referenced in the NDS for CWMD dated May 2013 is "WMD Proliferation" defined as "The transfer of weapons of mass destruction or related materials, technology, and expertise from suppliers to state or non-state actors."

[20] See Joint Chiefs of Staff, *Joint Pub 3-40, Countering Weapons of Mass Destruction* (Washington D.C. 2014), II–13.

[21] There are a number of strategic policy documents relevant to CWMD such as Sustaining US Global Leadership: Priorities for a 21st Century Defense, the National Security Strategy, the National Defense Strategy, the National Military Strategy, the Guidance for Employment of the Force, the Quadrennial Defense Review, the Nuclear Posture Review, the National Strategy for Countering Biological Threats, the National Strategy for Biosurveillance, and the Homeland Defense and Defense Support of Civil Authorities Strategy.

[22] Under Secretary for Arms Control and International Security oversees, "the negotiation, implementation, and verification of international agreements in arms control and international security. Other specific responsibilities include directing and coordinating export control policies to prevent missile, nuclear, chemical, biological, and chemical weapons proliferation."

[23] As expressed on the official website for the U.S. Deputy Assistant Secretary of Defense for Countering Weapons of Mass Destruction, available at <http://policy.defense.gov/OUSDPOffices/ASDforGlobalStrategicAffairs/CounteringWeaponsofMassDestruction.aspx>.

[24] As expressed on the official website for the U.S. Assistant Secretary of Defense for Nuclear, Chemical, and Biological, available at <http://www.acq.osd.mil/ncbdp/bio_weber.htm>.

[25] Interviews conducted with SJFHQ–E [2013] suggest that the move is expected to strengthen the relationship between the two organizations and create the opportunity for cross-fertilization of skills and knowledge to enable both organizations to better perform their expected roles at the operational level toward achieving policy aims.

[26] US Special Operations Command, *SOCO–2020: Forging the Tip of the Spear*, June 2014, available at <http://www.defenseinnovationmarketplace.mil/resources/SOCOM2020Strategy.pdf>. Dan Lamothe, "Special Operations Command takes a lead role in countering weapons of mass destruction," *Washington Post*, December 23, 2016, available at <https://www.washingtonpost.com/news/checkpoint/wp/2016/12/23/special-operations-command-takes-a-new-lead-role-countering-weapons-of-mass-destruction/>.

[27] Andrew Feickert, "U.S. Special Operations Forces (SOF): Background and Issues for Congress," Congressional Research Service, January 6, 2017, available at <

[28] Kyle Rempfer, "Countering WMDs Cannot be on SOCOM alone, Experts Contend," *Air Force Times*, March 1, 2018, available at <https://www.airforcetimes.com/flashpoints/2018/03/01/countering-wmds-cannot-be-on-socom-alone-experts-contend/>.

[29] Technical capabilities are pursued in response to adversarial capabilities or observed advances in the industrial base that demonstrate the potential for militarized utility by state or non-state actors.

[30] Re-balance to Asia-Pacific; down-sizing of Army structure; move to more CONUS-based Army posture.

[31] This is derived from survey work done with 20th Support Command (CBRNE); U.S. Army Research, Development and Engineering Command, specifically, Edgewood Chemical Biological Center (ECBC); U.S. Army Medical Research Institute of Chemical Defense (USAMRICD); U.S. Army Chemical Materials Agency (CMA); U.S. Army Element, Assembled Chemical Weapons Alternatives (ACWA); Joint Program Executive Office for Chemical Biological Defense (JPEO–CBD); U.S. Army Medical Research Institute of Chemical Defense (MRICD); and Standing Joint Force Headquarters-Elimination (SJFHQ–E) and others located at Aberdeen Proving Grounds, Maryland. To include Fort Belvoir, Virginia also captures the Defense Threat Reduction Agency (DTRA) and U.S. Army Nuclear and Chemical Agency (USANCA) to name a few more.

[32] National Research Council, *Determining Core Capabilities in Chemical and Biological Defense Science and Technology*, (Washington D.C.: National Academies Press, 2012).

[33] For greater discussion of what constitutes active defense against WMD weapons, see Bruce Bennett, "Responding to Asymmetric Threats," in *New Challenges, New Tools for Defense Decisionmaking*, Stuart E. Johnson, Martin C. Libicki, Gregory F. Treverton (eds), (Washington D.C.: RAND Corporation, 2003).

[34] Lonnie Carlson and Margaret E. Kosal, "Preventing Weapons of Mass Destruction Proliferation–Leveraging Special Operations Forces to Shape the Environment," JSOU Monograph, (January 2017), available at http://jsou.libguides.com/ld.php?content_id=28362821.

[35] Beyond traditional state-based adversaries, threats are increasing from non-state actors, including terrorists, see e.g., U.S. State Department, Office of the Coordinator for Counterterrorism, "Country Reports on Terrorism 2012, Chapter 4: The Global Challenge of Chemical, Biological, Radiological, or Nuclear (CBRN) Terrorism," (May 2013), available at <http://www.state.gov/j/ct/rls/crt/2012/209986.htm>; and other "converging" transnational actors that might seek to acquire and use CBRN weapons.

[36] Margaret E. Kosal, *Nanotechnology for Chemical and Biological Defense* (New York: Springer Academic Publishers, 2009) , available at <http://www.springer.com/materials/nanotechnology/book/978-1-4419-0061-6>; Sergio Bonin with contributions by Piers D. Millett, Margaret E. Kosal, R. Alexander Hamilton, and Alexey V. Feofanov, "Security Implications of Synthetic Biology and Nanobiotechnology: A Risk and Response Assessment of Advances in Biotechnology," United Nations Interregional Crime and Justice Research Institute (UNICRI), 2011; Margaret E. Kosal and Jonathan Y. Huang, "The Security Implications of Cognitive Science Research," Bulletin of Atomic Scientists (July 2008); *Neuroscience, Conflict, and Security*, The Royal Society (February 2012), available at <http://royalsociety.org/policy/projects/brain-waves/conflict-security/>.

[37] National Research Council. *Globalization, Biosecurity, and the Future of the Life Sciences* (Washington DC: National Academies Press, 2006).

[38] Department of Defense, *Summary of the National Defense Strategy* (Washington D.C., 2018).

[39] The Army reinforces the opaque nature of C-WMD with "we also believe that Countering Weapons of Mass Destruction may have implications for our capacity," from the 2013 *Army Strategic Planning Guidance* (Department of the Army: Washington D.C., 2013), 6.

[40] Office of the Secretary of Defense, *Nuclear Posture Review*, (February 2018).

Acknowledgements

Acknowledgements and gratitude to LTC Justin Y Reese, USA; Lt. Col. Joel Pauls, USAF; COL (ret) E.J. Degen, USA, and Ms. Carmen Lane for invaluable collaboration, expertise, and critiques in carrying out the work described here; all errors are the author's.

In September 2011, the crew of the USS *New York*, upper right, man the rails and present honors while passing the National 9/11 Memorial. On board are family members of victims and first responders from 9/11 and Marines from Camp Lejeune. The ship was built with steel recovered from Ground Zero. (U.S. Marine Corps/Randall A. Clinton)

The State of the Art in Contemporary CWMD Thinking

By Amy Frumin, Tracy Moss, and David C. Ellis

The public revelation in 2004 of A.Q. Khan's nuclear proliferation network created an immediate and serious crisis for the counter–weapons of mass destruction (WMD) community.[1] Traditional reductionist intelligence analysis, searching for evidence of nations developing WMD along known and well-trodden technical avenues, failed to identify the extent of Khan's proliferation activities. This intelligence failure was not a result of insufficient resources or effort but was instead a failure in imagination and approach. The Khan network exemplified the new WMD operating environment. The continued failure of counter–WMD (CWMD) policy, planning, and intelligence to recognize and adapt to the new, network-centric proliferation environment will persist until new, more imaginative ways of thinking and behaving are embraced.

This is not to say the United States Government (USG) has not made adaptive efforts, but they have been largely incomplete because transformational efforts typically consist of limited reorganization, and fail to address the cognitive and behavioral changes that must drive reorganization attempts. This article advocates an alternative way of thinking and behaving that inherently necessitates organizational change and is better-suited to the contemporary operating environment. The state of the art in CWMD thinking and interagency behavior is captured in two interrelated concepts: Design and Opportunity Analysis (OA).[2] This article does not attempt to explain Design as an approach or process; rather the article advocates Design as a cognitive, organizational, and behavioral approach to address complex challenges such as WMD proliferation.[3] OA is an organizational framework that allows the USG to bring myriad and otherwise disconnected CWMD stakeholder agencies together to design and coordinate more effective CWMD interventions by collectively leveraging their resources, authorities, and other mission enablers.

In a brief historical segment, we begin by highlighting key differences between the Cold War era and the 21st century proliferation environments that necessitate different approaches to effectively counter–WMD proliferation. The crucial change in the environment was that WMD development and weaponization, which had once been a closed system involving relatively few, easily identified actors, had now become an unbounded, open system of witting and unwitting contributors. This means the traditional analytic techniques practiced by intelligence analysts that worked reasonably well in a bound, closed system are now entirely inadequate

Ms. Amy Frumin and Major Tracy Moss, USAF (ret.) are faculty in the College of Special Operations at Joint Special Operations University (JSOU). Dr. David C. Ellis is a Resident Senior Fellow with the Center for Strategic Studies at JSOU.

among the unbound, open systems Khan exploited and exposed. CWMD analysts need to move beyond traditionally reactive, reductionist analysis to proactive, synthesis-oriented systems thinking.[4]

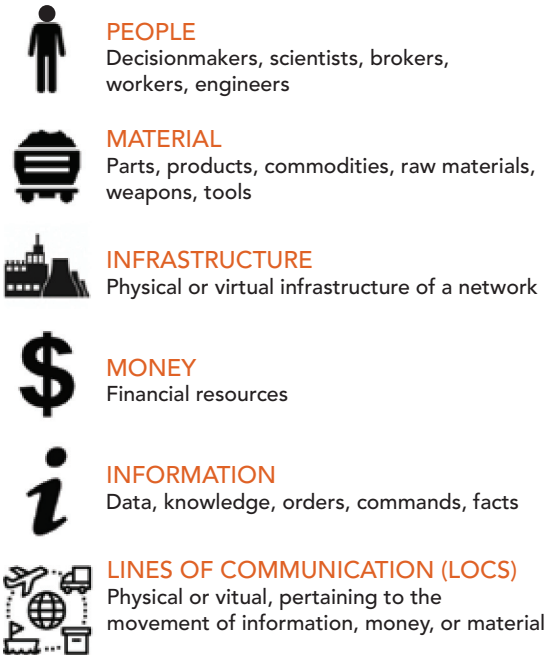
This article advocates two interrelated ideas that will improve the USG's ability to more effectively address the complex challenge of WMD proliferation. Design and OA are, respectively, the cognitive adaptations and the framework or forum through which those adaptations can be implemented. Together, Design and Opportunity Analysis constitute the state of the art in CWMD thinking. This article explains the change in the operating environment, the differences between reductionist systematic analysis and systems thinking, and problems associated with a sector-based interagency, with a view to explain why Design and OA are needed. The article concludes by explaining, for the first time to the broader CWMD community of interest and those interested in creating a more functional interagency, how OA is executed.

Inflection Point: From Complicated to Complex

Order and Predictability in a Complex Era (1900s)

The six factors seen in Figure 1 are often targeted in countering WMD: people, infrastructure, money, material, information, and lines of communication.[5] During the mid-20th century, creating and delivering nuclear weapons required high levels of specialized education (people), extraordinary electrical energy capacity and research facilities (infrastructure), obtaining scarce specialty alloys (materials), precision manufacturing and technical knowledge (information), substantial levels of funding (money), and the ability to both acquire and transfer all of the above (lines of communication). Some of these factors, as well as some different ones, also pertained to large-scale development of biological and chemical weapons. During the Cold War era these factors

Figure 1: Factors of WMD Development and Weaponization.



could only be generated by states. By the end of the 1960s, only a few states were able to harness the required resources. This was especially true relative to nuclear weapons, but also held true for chemical and biological weapons.[6] As a result, for a period of time, there was a specific avenue states had to follow in order to develop and weaponize WMD.

International organizations and treaties, such as the establishment of the International Atomic Energy Agency (1957) and the entry into force of the Non-Proliferation Treaty (NPT) (1968), tried to balance the needs of disseminating the civilian, developmental benefits of nuclear technology while regulating its military applications.[7,8] The NPT attempted to limit nuclear weapons systems to the five nuclear armed powers—United States, United Kingdom, France, China, and the former Soviet Union—and to reduce the number of weapons those powers possessed. While the effectiveness of the control regimes is debatable, these treaties and

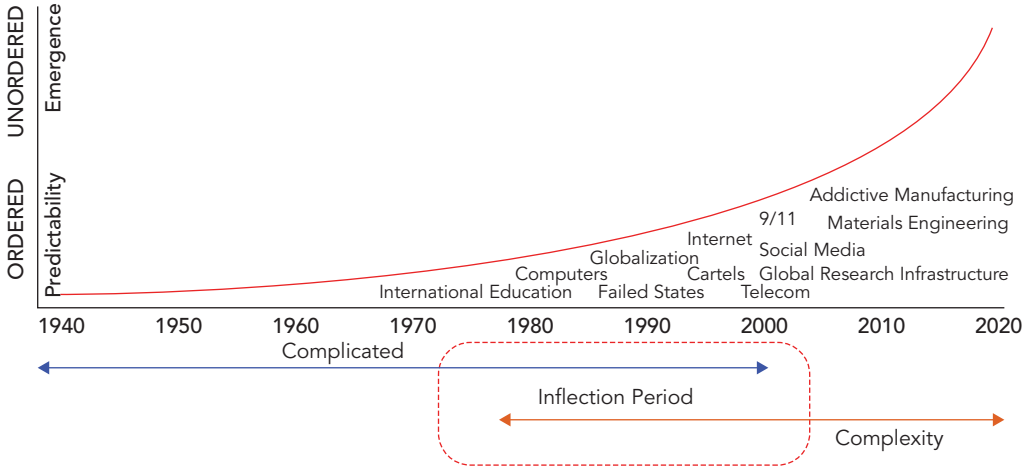
organizations did attempt to bound the WMD system by reducing the number of actors and regulating their interactions to prevent the proliferation of dangerous technology.

The combination of limited avenues to achieving WMD weaponization and the formation of international organizations and treaties created the appearance of a relatively ordered, predictable, closed WMD system. There were a few state actors each with independent, internal networks, and some cooperation among them, but not an integrated, global technical or commercial system. Systematic intelligence analysis could credibly function in this operating environment since the range of actors, relationships, and behaviors were relatively knowable. Good detective work could develop a credible picture of an adversary's activities and developments.

The Inflection to Unpredictability and Complexity in the Post–Cold War Era

The A.Q. Khan case illustrates the complexity in the WMD proliferation systems that began in 1970s with the convergence of a variety of factors. Figure 2 illustrates the inflection point from a relatively closed WMD research and weaponization system to an open one. By the late 1960s, international education opportunities in the hard sciences began disseminating expertise that could be diverted to develop WMD. For example, Dr. Khan, a native of Pakistan, received his Ph.D in metallurgy from Catholic University of Leuven in Belgium after having studied in Germany and the Netherlands.[9] In the 1980s, computing power revolutionized scientists' ability to learn about and model complex physical reactions while the globalization of trade and finance made previously scarce technology and materials accessible to developing states. The end of the Cold War struggle between East and West precipitated the collapse of governments, the expansion of trade in illicit goods, and a race for former-Soviet scientific expertise. By the 1990s, licit trade connected once isolated countries, like China, Russia, and India to the rest of the world. In addition, production chains became more diverse. Several newly independent states with nuclear infrastructure, especially the former-Soviet republics, were now engaged in global trade, creating opportunity for the intentional or unintentional loss of control of nuclear materials of concern. Even as regulations on nuclear-related technologies tightened following the disclosure

Figure 2: The Inflection from a Complicated CWMD Operating Environment to a Complex One.



of Iraq's program under Saddam Hussein, these communication and global trade advancements enabled state and non-state actors to move further up the supply chain to procure unregulated and dual-use components, materials, and commodities needed to indigenously develop previously inaccessible infrastructure, materials, and components.[10]

Meanwhile in the 1990s, extraordinary advances in global telecommunications and the commercialization of the internet transformed access to information, knowledge, expertise, and trade. All of the actors were further connected through social media by 2000, first in the form of chat rooms and later by apps specifically designed to link together similarly interested and like-minded individuals.

The A.Q. Khan network presented the first undeniable evidence of new tactics in the procurement and development of WMD. Khan did not feel bound by the system created by the various international regulations. Motivated by patriotism to arm his home country with a nuclear weapon to counter India's nuclear capability, Khan leveraged a series of personal, professional, and commercial networks to support an indigenous Pakistani nuclear weapons program despite the restrictions on his government imposed by international control treaties.[11] For example, he stole nearly every centrifuge design of his former-employer, the Dutch nuclear fuel company URENCO.[12] While many of the components for WMD development were on international control regime lists, Khan thought systemically, or holistically, about the various systems required to make WMD. He was able to licitly procure precursor materials for the components on the global market. With a global supply network in place, Khan had the knowledge and materials to create the infrastructure for a nuclear weapon. It was Khan's willingness to sell his knowledge and network to any interested party that facilitated nuclear proliferation and the technical capacity in countries like Libya, North Korea, and Iran. According to Gordon Corera, the author of *Shopping for Bombs, Nuclear Proliferation, Global Insecurity and the Rise and Fall of the A.Q. Khan Network*, "Thanks to the Khan network, much of the equipment and knowledge for developing nuclear technology is no longer controlled by the state—it is in the marketplace."[14]

Effectively, nuclear aspirants no longer had to work with or through states to obtain components for a nuclear weapon. Khan introduced new actors into the system, to include witting and unwitting non-state actors. Many of the licit businesses from which Khan procured components were unaware of the end use of their products.[15] The international community now had to be concerned with a whole new array of possible, less definable, less regulated avenues to develop a nuclear weapon. This increase in numbers and types of actors, coupled with the advancements in communications and financial technology, effectively broke the relatively closed WMD operating environment into an open, unordered, and largely unpredictable system of interrelated systems.

September 11, 2001 vividly illustrated the complexity of the new system and just how open it had become.[16] An actor wishing to do America harm no longer required a chemical, biological, or nuclear weapon of mass destruction, massive infrastructure, or immense financial resources. Rather, actors with the intent to attack the United States could spend $400–500,000 to use a civilian airliner as a weapon to kill thousands of civilians.[17] The number of avenues to this type of mass destruction is limited only by one's imagination and intent, two factors that gained increasing importance to CWMD professionals. By the end of the 2000s, advances in materials engineering, additive manufacturing (3-D printing), and access to information and encryption technologies continued to add further complexity to the system.

In 2015 Josh Kerbel, a former Chief Analytic Methodologist at the Defense Intelligence Agency, suggested the global system is now

> *effectively defined by fluid, heterogeneous, widely distributed, nonhierarchical networks—in contrast to the comparatively static, homogenous (state-centric) and dichotomous hierarchies (East–West; Warsaw Pact–NATO; United States–former Soviet Union) that dominated the Cold War strategic environment.*[18]

The WMD environment steadily evolved while the USG's traditional, systematic analytical approach remained static and state-focused.[19] The implication of these changes in the environment described by Kerbel is that the issue of countering–WMD has gone from being a complicated problem to a complex one.

Complicated and Complex in the Contemporary Environment

While they are often used interchangeably, the terms complicated and complex have specific characteristics and therefore call for different approaches to thinking and acting. The sense-making model or Cynefin Framework found in Figure 3 is useful in helping to conceptualize how complicated and complex are different and therefore require different approaches to solving problems in each of the domains.[20] On the right side of the Cynefin Framework, systems are closed, ordered, and cause and effect relationships can be predicted and repeated. In ordered domains, the past is instructive for determining the future, and systematic analysis is appropriate.[21] Some challenges might be complicated in that experts are required to determine the cause and effect relationships, but they can be systematically analyzed and known.

On the left side, systems are open and unordered. The relationship between cause and effect is no longer evident or knowable. This is because the number of actors or systems increases as well as the speed at which they interact. Thus, the number of interactions overwhelms the analyst's ability to grasp the result of each interaction and how it impacts the broader system. The emerging impact on the system of systems of these myriad interactions is not knowable, does not repeat, and is non-linear.[22] The system is therefore considered open. Emergence is unpredictable, although patterns can be perceived. Challenges in this regard are often dubbed complex because behavior is emergent and adaptive based on circumstances, unpredictable,

Figure 3: The Cynefin Framework.

Source: Adapted from Greg Broughman. *The Cynefin Mini-Book: An Introduction to Complexity and the Cynefin Framework*. Middletown: InfoQ.com, 2015.

and limited only by imagination or unrealized relationships. Systematic analysis fails in complexity because the past does not necessarily predict the future in the unordered domain. Actors operating in complex environments first probe the system for opportunities, then sense how the system reacts, and finally respond to amplify or dampen the emergent behavior commensurate with their interests.[23] Referring again to Figure 2, the inflection point illustrates the radical increase in the opportunity for emergent behavior following the inflection period of the 1980–90s.

Based on the characteristics of the environments laid out above, it is fair to say that the Cold War era was complicated while the Post–Cold War era is complex. This is not to diminish the difficulty of the problems faced by Cold War warriors, or is it to ignore the reality that all social systems are inherently open. Rather it is to juxtapose the challenges of the Cold War era in countering–WMD to the modern landscape and to highlight the inadequacies of the reductionist, retrospective, investigative approaches to which the USG bureaucracies default.

From Reductionist Analysis to Systems Thought and Behavior

Why Reductionist Systemic Analysis Worked in the Cold War Era

Reductionist, systematic (not systemic) analysis, in which the system might reasonably be appreciated by understanding its component parts, could credibly function in the Cold War era, complicated, operating environment. Additionally, reductionism has been built into Western thinking since the Age of Reason and the Age of Enlightenment and is certainly taught to U.S. intelligence professionals.[24] The science of WMD, rooted in chemistry and physics, lent itself to the idea that the linear, reductionist, scientific approach would be sufficient for tracking WMD research and development activity. The USG's bureaucracy has built reductionism into its infrastructure by assigning different agencies or departments authorities and permissions over different, discreet aspects of the research, development, and weaponization processes.

It is not only the USG infrastructure that reveals a penchant toward reductionism. The culture of the military, which prizes efficiency, order and clarity, also lends itself to reductionist thinking. The military's use of systematic analysis, like the Joint Planning Process and PMESII, common tools used to understand an environment, are examples of the reductionist approach within the Department of Defense (DOD). PMESII, for instance, calls for an analysis of political, military, economic, social, infrastructure, and information dynamics. This type of systematic analysis can be useful, especially in a large and geographically dispersed bureaucracy. Forwarding PMESII-templated information into a headquarters that is studying an entire region is useful to create continuity across hundreds or thousands of personnel and a wide range of ages, experiences, and skills. Unfortunately, reducing the elements into functional sectors focuses attention on the pieces almost as an inert snapshot in time instead of how they dynamically interact to shape the future. Clearly economics will impact politics and social components of society, as an example.

In recounting the development of the Khan network, Corera raised the question whether United States and allied intelligence agencies should have identified the new proliferation threat. While Western intelligence agencies knew of the network's main actors, they focused only on its contribution to one state, Pakistan, and allowed the network to continue functioning in order to track Pakistan's progress. He concluded, "Yet, initially they never watched these individuals closely enough to realize that Khan was doing much more than simply importing into Pakistan; he had also begun selling the equipment onwards to

other countries."[25] In other words, the Intelligence Community's expectations of what they should see made them focus so intently that they were unaware of what they could see.[26]

Why Systems Thinking and Behaving is Necessary for the Future

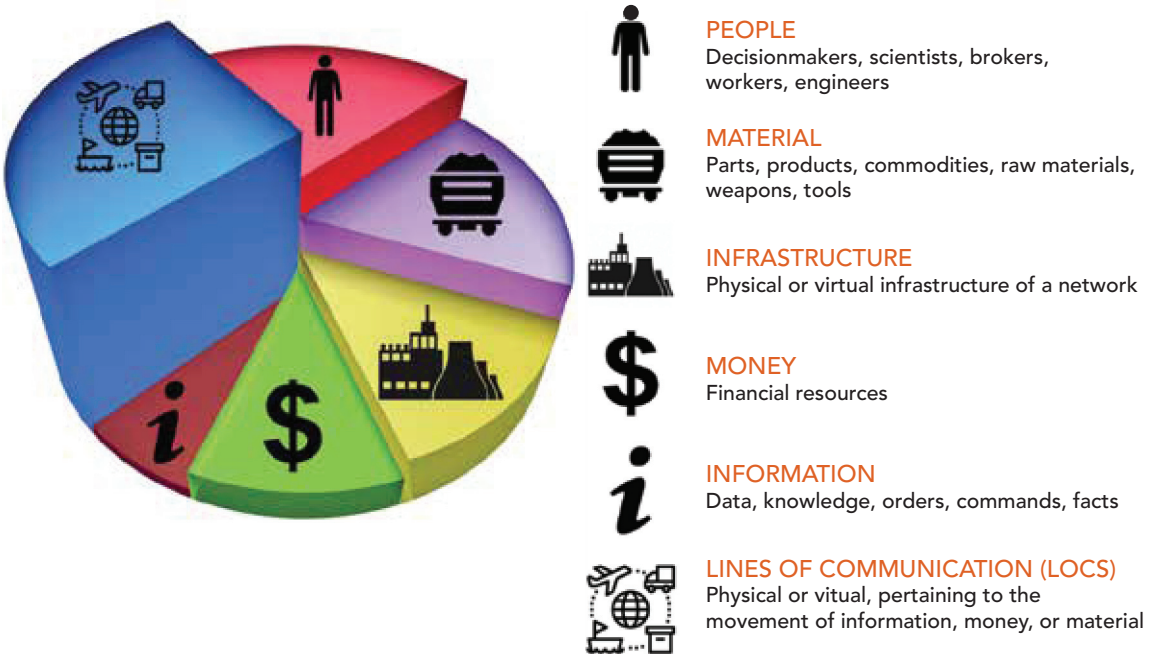
The inflection from a closed to an open WMD environment forced a change in the emphasis from a reactive, retrospective investigation of states' activities, toward a proactive, intent-oriented, futures-based, state and non-state actor perspective. In complex systems, behavior is emergent and patterns unordered because relationships are constantly changing and dynamic.[27] Thus, the number of interactions overwhelms a CWMD analyst's ability to know and understand the result of each interaction and how it impacts the broader system. Starting with Khan and growing exponentially since then with the world wide web, the number of players, types of players, and their interactions are too numerous to fully appreciate.

During the past decade, network analysis has emerged as the intelligence function's response to the increasingly complex environment. As a systems thinking approach, a network perspective is extremely useful. The prevailing reductionist focus on network nodes (the pieces and parts), however, drastically reduces the utility of taking a network approach in the first place as seen in Figure 4. A systems thinking approach to networks changes the focus from nodes to the relationships connecting them. This is not to say nodes are irrelevant. On the contrary it is critical to understand the nodes so an analyst might derive meaning and opportunity from the relationships. To focus on the nodes exclusively though, without regard to the relationships connecting them, is to drastically limit not only understanding, but the ability to recognize and leverage opportunities in the system.

Viewing Figure 4 from a systems perspective, the cross-section of any network relationship—the lines or pipelines connecting nodes to one another—can be characterized according to the same six factors in Figure 1: people, infrastructure, money, material, information, and lines of communication. Figure 5 illustrates that any given relationship between nodes can be analyzed to determine which of the six factors constitute the critical characteristics of the relationship. Different relationships are comprised of different proportions of the six factors, which presents unique vulnerabilities along the series of relationships that constitute the system. It is important to

Figure 4: Notional Network Analysis with Emphasis on the Nodes.

Figure 5: The Moss Network Relationship Cross-Section (NRCS) Model View of Network Relationships that Transforms Links into Multi-Factor Pipelines.



note that the Moss Network Relationship Cross-Section Model in Figure 5 is not a traditional targeting model focused on network nodes. It is a systemic targeting potential model focused on the relationships between nodes at the structural level of a proliferation system, i.e. a network. If an analyst only looks at the nodes and characterizes each node as one of the six factors, she misses the possibility that each relationship connecting the nodes to one another may be comprised of all six factors thereby providing countless intervention opportunities that might otherwise be missed as a result of the blinders created by a nodal focus in network targeting.

The modern CWMD operating environment requires thinking in systemic or holistic terms instead of using reductionist, systematic analysis. It is about the imagination and intent of threat actors and how they might creatively use the new, dense, interwoven nodes of WMD precursors to work around the anti-proliferation enforcement mechanisms impeding them. Corera notes

> *It has been estimated that at least two-thirds of the Khan network was entirely legitimate, breaking no law. With the lack of a comprehensive multilateral export regime, it is easy for proliferators to find new gaps as quickly as countries try to plug existing holes.*[28]

Systematic analysis is consequently insufficient in the first instance because it cannot possibly intervene in the potential avenues of WMD development until they have already been exploited because of the retrospective focus of systematic analysis. Systems thinking, on the other hand, is precisely about appreciating the interaction of the whole in order to discern opportunities for emergent and adaptive relationships and, consequently, for intervening against WMD contributors in the future.

From Sectors to Systems: Inducing a Reductionist Interagency to Act Cohesively

In the aftermath of 9/11, the USG gathered experts together in various commissions to identify how the Intelligence Community (IC) failed to recognize such a grave threat. According to the 9/11 Commission, "The most important failure was one of imagination."[29] The report went on to recommend a governmental reorganization to modernize the bureaucracy that was "designed a half a century ago to win the Cold War."[30] The 9/11 Commission called for the IC to reorganize under one umbrella—the Office of the Director of National Intelligence—in the hope that the dots would be connected across the various intelligence agencies in the future.[31]

In similar fashion, in October 2001 the Office of Homeland Security was established to "coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks."[32] By November 2002, the Office was upgraded to the Department of Homeland Security, subsuming 22 agencies in the largest reorganization of the USG since the establishment of DOD in 1947.

The question remains today, did these reorganizations of the USG address the underlying failure of imagination? Or, did the USG simply create larger, broader sector specific silos? Is the USG prepared for the complexity of the world today? Or will it continue to miss dynamic, systemic trends as it defaults to expert, yet paradigmatically constrained, opinions in various sectors? Is the USG thinking and acting in terms of sectors or systems?

Systems Not Sectors

The difficulties associated with transitioning to a systems thinking approach from a sector-based, systematic analysis approach can be seen easily in the medical profession. In the ultimate reductionist enterprise, the scientific community realized through its project to map the human genome that breaking the gene down to its component parts does not provide the full picture. At the molecular level there are thousands of interactions creating a complex network response resulting in living organisms. The interactions and relationships among the molecules are as important for understanding how the body's system functions as the molecules themselves.[33] Unsurprisingly, there is a tension between molecular biologists (who engage in reductionist analysis) and systems biologists (who advocate for a systemic approach). However, as Johns Hopkins University oncology professor Dr. Bert Vogelstein notes, "We'll need new theories and models, as well as advances in molecular biology, to understand biological complexity."[34]

As is the proclivity of the USG, the CWMD problem set has been broken down into various component parts resulting in a vast and disparate interagency network. A list of the types of activities interagency partners undertake is illustrative: intelligence gathering, treaty enforcement, export control enforcement, threat detection and analysis, global health security, bio surveillance, building partner capacity, contingency planning, medical countermeasures development, physical countermeasures, render safe activities, disruption of proliferation network activities, hazard modeling and prediction, medical and forensic response, missile defense, protection of the force, WMD attack attribution, separated plutonium reduction, chemical material security, counter nuclear smuggling, contamination control, and deterring WMD use.

The Defense Threat Reduction Agency has developed a CWMD directory for the express purpose of increasing awareness across the CWMD community regarding each organization's roles, responsibilities, authorities, and capabilities. The directory provides a breakout from the executive department-level to the bureau or office-level with as many as 188 offices across the USG working in the CWMD or related mission areas. Many

of the interagency partners are ones with which DOD would seldom otherwise interact, such as Health and Human Services or the Center for Disease Control. There are numerous coordinating interagency bodies that attempt to bring some coherence to the CWMD efforts. However, there is no single entity or agency that is in charge, nor is there any entity or agency that has the preponderance of the authorities, capabilities, access, placement, and resources to address the myriad WMD threats the country faces. To suggest that one agency should be in charge or that there should be a widespread and profound reorganization of the CWMD community is not the point. The point here is that the diversity and breadth of the CWMD community merit a more effective systemic approach to collaborate, coordinate, and cooperate towards the common goal of preventing and mitigating WMD threats.

Organizing for Emergence in the System of Malign Actors

A key weakness in the USG approach is that the entire interagency CWMD engagement model is based on the concept of a coalition-of-the-willing among co-equal executive agencies. Even the recent unified command plan (UCP) change identifying U.S. Special Operations Command (USSOCOM) as the coordinating authority for DOD for all CWMD activities has some intrinsic limitations. While USSOCOM is responsible for coordinating the CWMD efforts of DOD offices, its role as coordinating authority does not allow the Command to do much more than compel entities to participate (an important task for a variety of reasons, but not a far-reaching authority). USSOCOM cannot direct action beyond the specialized CWMD tasks performed by Special Operations Forces (SOF). In regards to interagency partners, the best USSOCOM can do is request that partners attend meetings.

So how might the USG coherently address the complex problem of WMD when it is rooted in an outmoded, large, lumbering bureaucracy with a collection of tools spread among a variety of co-equal agencies? The beehive offers some interesting lessons. Bees operate as a distributed network, but with unity of purpose. They are interdependent but each bee has clear and complementary roles.[35] They swarm to threats coherently as needed, but the collective thrives based on distributed roles during periods of normalcy.

To effectively counter–WMD networks, the USG must bring to bear its full arsenal of capabilities, authorities, and permissions in a coordinated manner. As A.Q. Khan's story and September 11 demonstrate, exclusive use of the old tools—analysis, planning, functionally organized, sector-based agencies—in a complex environment has proven not only inadequate, but dangerous.

To effectively counter–WMD networks, the USG must bring to bear its full arsenal of capabilities, authorities, and permissions in a coordinated manner. As A.Q. Khan's story and September 11 demonstrate, exclusive use of the old tools—analysis, planning, functionally organized, sector-based agencies—in a complex environment has proven not only inadequate, but dangerous. The CWMD community

does not need more experts to do more analysis, rather it needs a different way of thinking and behaving in a changed environment. USSOCOM has taken on this no-fail CWMD mission and is fostering a way of thinking and acting that can facilitate the productive engagement of the interagency for cohesive action through Design and Opportunity Analysis.

The State of the Art: Design and Opportunity Analysis

For the interagency coalition-of-the-willing to function effectively in this mission space, the group has to have a common appreciation of the problem, a common purpose, and a clear sense of each agency's distinct role in addressing that problem. General Stanley McChrystal's book *Team of Teams* tells the story of how Task Force–714 managed to change its own organizational culture in order to more effectively address the complexities of al-Qaeda in Iraq in 2004. Shared consciousness and empowered execution were essential elements of the new organizational paradigm. However, neither of these conditions happened organically in the military, especially in a war zone. The book identifies three behaviors as central to enabling empowered execution and shared consciousness: extreme transparency throughout the organization (including the leadership), establishing trust and common purpose among disparate stakeholders (internal sub-organizations and external organizations), and an unprecedented delegation of authority.[36] These are all behaviors rooted in Design and entirely counter-intuitive to military and government culture firmly rooted in a linear, reductionist, systematic analysis paradigm.[37]

Why Design?

Design is a holistic way of thinking about and creating novel approaches to address complex issues.[38] It is above all an attitude and ethic for accepting and promoting

- future-oriented thinking;
- imagination and innovation for navigating through an unpredictable future;
- divergent perspectives to appreciate the context across a range of experiences to promote imagination;
- empathy for other perspectives and experiences;
- perpetual, deliberate learning unconstrained by personal and organizational paradigms and standard operating procedures;
- iterative learning to consistently update appreciation of the context as circumstances evolve; and
- nonlinear dynamics in social systems, such that past experiences do not necessarily predict future paths.[39]

Cognitively, Design is a reflective practice that enables CWMD professionals to think about the environment holistically and derive meaning at the systemic level by synthesizing the interagency's diverse perspectives.[40] When each agency looks at the issue from its own perspective, it is common practice to mirror image comfortable organizational and cognitive models onto the intentions and behaviors of other state and non-state actors, leading to an incomplete and often inaccurate depiction of reality.[41] Because the USG is functionally organized, each agency tends to rely on cognitive tools that also categorize, like the military's popular PMESII model. Unfortunately, these types of categorization models ignore the relationships and dynamic interactions among the categorized factors, severely limiting both the community's appreciation of the context and its ability to recognize potential opportunities to proactively intervene and move the system in a direction commensurate with national security interests.

Functionally, Design enables CWMD professionals to take the time and space necessary

to appreciate a complex environment before attempting to intervene. As a way of thinking that consistently updates and informs planning and execution, Design empowers not only iterative learning, but proactive, iterative engagement with the operating environment in order to probe and gauge the system's response much as threat actors do. This is to say Design, planning, and execution are all continuous and simultaneous activities over time.[42] This is very different from the USG's current linear, end-state reliant approach, and for good reason. Global, complex challenges have no end state, they only have future beginnings.[43] An emergent system requires an emergent practice like Design.[44]

Rigorous, continuous framing, reframing, and synthesis of different perspectives, scopes, scales, and self-reflection are essential to the creativity required to imagine possible futures.[45] In fact, according to a trade paper from Hollywood, in October 2001 the U.S. Army, having recognized its own lack of creativity in imagining the 9/11 scenario, convened a meeting with Hollywood movie screenwriters and directors to get some original ideas of potential future terrorist activity.[46] It is exactly this kind of injection of new and divergent ideas that forces the participants in a Design inquiry to think about challenges in new and creative ways. Incorporating interagency, international, and multinational partners' perspectives not only facilitates self-awareness and more robust understanding of the issue, it also facilitates "shared consciousness."[47]

Why Opportunity Analysis Helps

Team of Teams emphasizes the importance of changing the way interagency teams organize themselves and behave in addition to the way they think. In order to develop shared consciousness and empowered execution, it required a fundamental change in the way Task Force–714 was organized. This is not to say every line and block on the organization's chart changed, but the organization's social behavior was altered by changing the way in which people interacted with each other. For example, the Operations and Intelligence brief was created as an organizational venue to bridge the communication and cultural gaps between the operations and intelligence branches within the Task Force's own organization, but also the gaps that existed between the Task Force and other outside organizations critical to the unit's mission.[48] The counterproliferation community of action has developed a similar concept called Opportunity Analysis (OA).

OA is the framework that enables the disparate, often unconnected CWMD community of action to practice the cognitive and behavioral changes required of a design approach. In order to impact the complex system the USG needs not only to think systemically, but also must act as a coordinated system. The goal of OA is to bring to bear all of the resources across the USG in cooperative and coordinated action. At the heart of OA is the responsibility, influence, capability, capacity, authority, awareness, access, placement, and policy (RICCAAAPP) framework used to identify, combine, and sequence the CWMD community of action's enablers toward a common end with a CWMD effect. Each member of the CWMD community of action has RICCAAAPP. Identifying these enablers alone is insufficient. CWMD professionals also need an organizational construct, trust, and transparency to enable development of "shared consciousness" and "empowered execution." The OA framework allows the CWMD community to do this both organizationally and cognitively in a fashion more appropriately suited to complexity than the legacy bureaucracy can achieve in its current form. The OA framework facilitates proactive, willful organization and relationship-building among stakeholder enablers using iterative Design principles in a common forum, toward a common positive effect in the CWMD space.

Organizationally, the OA framework serves as a bridging mechanism between agency stovepipes aimed at generating a shared CWMD community of action workspace, both virtually and physically. Like an evolved Task Force model, or a beehive, the OA participants function as a distributed network, loosely facilitated by a core OA team who guide them through a Design process, managing and producing process artifacts or documentation. The first iteration of the Design process as a whole, culminates in a broadly attended event bringing together the distributed network of community stakeholders. The purpose of this event is three-fold. First, to develop common appreciation of the issue at hand; second, for stakeholders to educate the group on their mission enablers (RICCAAAPP opportunities); and third, to ideate and record possible opportunities to affect the system of concern uninhibited by one's own organizational constraints.[49] The resulting ideas are then organized and prioritized in accordance with the unique design created for the specific challenge at hand and distributed to all participants in an OA report.

This is as far as the formal process has evolved giving rise to the dominant criticism of OA as an incomplete means to overcome our own organizational challenges in this complex mission space. What critics fail to acknowledge are the enduring changes in participants' thinking and behavior resulting from the continued evolution, expansion, and repetition of OA endeavors. So far, four different WMD proliferation concerns have been tackled using the OA framework, each sponsored by a USG or partner nation organization with specific WMD concerns, and three more OAs are in the design or planning stages. The four topics OA has addressed thus far are a legacy chemical weapons program in the Central Command's area of responsibility, proliferation implications of additive manufacturing, and two adversary ballistic missile programs. As more USG stakeholders see the value and potential of the approach at work with each successive OA, more want to see it work and do what they can to create the changes necessary to make it work as a matter of national interest. Continually practicing these concepts in real-world mission areas contributes to their refinement and maturity as an adaptive approach, capable of creating meaningful intervention in an increasingly dangerous and active global proliferation system.

Conclusion

Complex security challenges like WMD proliferation, terrorism, countering violent extremism, or human trafficking are fundamentally complex phenomena in an age of networks.[50] Although these challenges existed during the Cold War era, they were manageable at the national level using the functionally-oriented, sector-based federal organizations and agencies. In our current era, however, networked organizations with little bureaucracy are becoming increasingly problematic, and they often adapt more rapidly to the environment than the USG owing to the sheer size of the bureaucracy. The USG can no longer rely on tools and organizational structures based in Cold War era industrial management theory to guide the way it thinks and behaves in a new world.

Design and OA constitute just one way to address a complex open system when hamstrung by a closed reductionist infrastructure. Together they have been informing planning and operations for years, though there is still room for growth. They form the state of the art in CWMD thinking precisely because they take into account the changes in the operating environment. WMD proliferation now occurs in an open system, requires CWMD professionals to think systemically about possible relationships and networks, demands proactive engagement with the system, and relies on the aggregate effect of widely distributed authorities and permissions. Design and Opportunity Analysis currently offer the best solutions to this increasingly complex reality. PRISM

Notes

[1] "A hero at Home, a Villain Abroad," *The Economist*, June 19, 2008, available at <www.economist.com/node/11585265>.

[2] LDCR Mike Scott, U.S. Navy (ret.) is often credited as the innovator behind Opportunity Analysis.

[3] For an excellent introduction to Design in open systems see H.G. Nelson and E. Stolterman, *The Design Way: Intentional Change in an Unpredictable World, Second Edition*, (Cambridge: The MIT Press, 2012). For further reading on Design Thinking see David C. Ellis and Charles N. Black, *Complexity, Organizational Blinders, and the SOCOM Design Way*, (Tampa: Joint Special Operations University Press: forthcoming).

[4] Systematic analysis reduces a phenomena to its most basic variables in the search for cause and effect, but relies on past interactions in the hope of predicting future events. Systemic thinking is an approach that emphasizes the relationships between variables and how they mutually influence and provide new, unanticipated opportunities for interaction in the future.

[5] For the purpose of this model, lines of communication are defined as the means of physical connectivity between network nodes such as roads, sea lanes, telephone lines, internet cables, train tracks, etc., and are not limited to a military context.

[6] For the purposes of this article the focus will be on nuclear weapons as this case is the most illustrative.

[7] International Atomic Energy Agency, *Statute of the International Atomic Energy Agency*, available at <https://www.iaea.org/sites/default/files/statute.pdf>.

[8] United Nations Office for Disarmament Affairs, *Treaty on the Non-Proliferation of Nuclear Weapons*, available at <https://www.un.org/disarmament/wmd/nuclear/npt/text>.

[9] Gordon Corera, *Shopping for Bombs: Nuclear Proliferation, Global Insecurity and the Rise and Fall of the A.Q. Khan Network*, (Oxford: Oxford University Press, 2006), 5–8; William Langewiesche, *The Atomic Bazaar: Dispatches from the Underground World of Nuclear Trafficking*, (New York: Farar, Strong, and Giroux, 2008), 82–84.

[10] Langewiesche, *The Atomic Bazaar*, 144-45; Langewiesche, *The Atomic Bazaar*, 16, 24–25, 146–49.

[11] William Langewiesche, "The Wrath of Khan: How A. Q. Khan made Pakistan a nuclear power—and showed that the spread of atomic weapons can't be stopped," *The Atlantic*, (November 2005), available at <https://www.theatlantic.com/magazine/archive/2005/11/the-wrath-of-khan/304333/>.

[12] Corera, *Shopping for Bombs*, 14.

[13] Corera, *Shopping for Bombs*, 108–09.

[14] Corera, *Shopping for Bombs*, xvi.

[15] Corera, *Shopping for Bombs*, 111–17.

[16] Strictly defined, September 11 was not a WMD event.

[17] National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report," (August, 2004), 169, available at <https://govinfo.library.unt.edu/911/report/911Report.pdf>.

[18] Josh Kerbel, "The Complexity Challenge: The U.S. Government's Struggle to Keep up with the Times," *National Interest*, (August 26, 2015), available at <http://nationalinterest.org/feature/the-complexity-challenge-the-us-governments-struggle-keep-13698>.

[19] Corera, *Shopping for Bombs*, 111–13.

[20] The Cynefin Framework as adapted from Greg Broughman. *The Cynefin Mini-Book: An Introduction to Complexity and the Cynefin Framework*. Middletown: InfoQ.com, 2015. This adaptation first appeared in the article by David C. Ellis, Charles N. Black, and Mary Ann Nobles on "Thinking Dangerously—Imagining SOCOM in a Post-CT World," *PRISM* 6, no.3 (Washington D.C.: National Defense University, 2016).

[21] C.F. Kurtz and D.J. Snowden, "The New Dynamics of Strategy: Sense-making in a Complex and Complicated World," *IBM Systems Journal*, 42, no. 3 (2003), 468.

[22] Kurtz and Snowden, "The New Dynamics of Strategy," 469.

[23] David Snowden and Mary E. Boone, "A Leader's Framework for Decision Making," *Harvard Business Review*, (November 2007), 74, available at <https://hbr.org/2007/11/a-leaders-framework-for-decision-making>; Kurtz and Snowden, "The New Dynamics of Strategy," 468–69.

[24] David C. Ellis and Charles N. Black, Complexity, *Organizational Blinders, and the SOCOM Design Way*, (Tampa: Joint Special Operations University Press: forthcoming); Hank Prunckun, *Handbook of Scientific Methods of Inquiry for Intelligence Analysis*, (Lanham: The Scarecrow Press, Inc., 2010), 43-52; Richards J. Heuer, Jr., *Psychology of Intelligence Analysis*, (Central Intelligence Agency, 1999), 43–48, 85–110; Richards J. Heuer, Jr. and Randolph H. Pherson, *Structured Analytical Techniques for Intelligence Analysis*, (Washington, DC: CQ Press, 2011).

[25] Corera, *Shopping for Bombs*, 113.

[26] Similarly, Langewiesche notes that Iraq's nuclear weapons program followed an "obsolete," but entirely viable, calutron technology shelved and declassified by the United States in 1949, but analysts were unaware of it because no one thought to look for evidence of its existence. Langewiesche, *The Atomic Bazaar*, 144; Heuer warns of this proclivity in the IC, see Heuer, *Psychology of Intelligence Analysis*, 65–66.

[27] A recent exemplar on intelligence analysis recognizing these dynamics is Wayne Michael Hall and Gary Citrenbaum, *Intelligence Analysis: How to Think in Complex Environment*, (Santa Barbara: ABC-CLIO, 2010), especially Chapter 10.

[28] Corera, *Shopping for Bombs*, 118.

[29] National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report: Executive Summary," (August 2004), 9, available at <https://govinfo.library.unt.edu/911/report/911Report_Exec.pdf>.

[30] "The 9/11 Commission Report: Executive Summary," 20.

[31] "The 9/11 Commission Report: Executive Summary," 20–26.

[32] U.S. Office of Homeland Security, "National Strategy for Homeland Security," (July 2002), available at <https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf>.

[33] Henry H.O. Heng, Ph.D, "The Conflict Between Complex Systems and Reductionism," *Journal of the American Medical Association* (2008), 300, no. 13, 1580–81.

[34] Robert Longrin, "An Integrated Approach: Systems Biology Seeks Order in Complexity," *JNCI: Journal of the National Cancer Institute*, 97, no. 7, (April 2005), 478.

[35] Michael J. Kwon, "Optimizing the CWMD Enterprise, Across the Interagency," *Interagency Journal*, 8, no. 2, (2014), 45.

[36] Stanley McChrystal, Tantum Collins, David Silverman, and Chris Fussell, *Team of Teams: New Rules of Engagement for a Complex World*, (New York: Portfolio, 2015), 6–7.

[37] McChrystal et al, 68–71.

[38] This is not to say innovation should occur for innovation's sake. Novel approaches are required because repeatability is not a characteristic of complexity despite the very real manifestation of patterns and trends in open systems. Every complex challenge is unique, and the moment the analyst interprets the appearance of trends or patterns in complex systems as indicative of "how the system works" is the moment the analyst begins to lose the appreciation of complexity.

[39] Nelson et al, *The Design Way*, 12, 16–23.

[40] D.A. Schön, *Educating the Reflective Practitioner: Toward a New Design for Teaching and Learning in the Professions*, First Edition, (San Francisco: Jossey-Bass, 1987), 44.

[41] Heuer, *Psychology of Intelligence Analysis*, 9–16, 70–71.

[42] Richard Newton, Tracy Moss, Charles N. Black, and Chris Phelps, "Design Thinking for the SOF Enterprise," *United States Special Operations Command White Paper*, January 29, 2016, 1–3.

[43] Ellis and Black, *Complexity*: Chapter 5.

[44] In contrast to retrospective deductive and inductive analysis, design leverages futures-oriented abductive inference, see C. Jotin Khisty. "Can Wicked Problems Be Tackled Through Abductive Inferencing?" *Journal of Urban Planning and Development* 126, no. 3 (2000), 104–105. Abductive inference is not common in IC products, though Heuer hints at the practice and even some design ethics, see Heuer, *Psychology of Intelligence Analysis*, 71–72, 75–78; Smith also introduces abductive inference as an aside, but reduces it to a traditional systematic analytic tool in Timothy J. Smith, "Predictive Warning: Teams, Networks, and Scientific Method," *Analyzing Intelligence: Origins, Obstacles, and Innovations*, Roger Z. George and James B. Bruce (editors), (Washington, DC: Georgetown University Press, 2008), 272.

[45] Nelson and Stolterman, *The Design Way*, 12.

[46] "Army Turns to Hollywood for Advice," BBC News, 8 October 2001, available at <http://news.bbc.co.uk/2/hi/entertainment/1586468.stm>.

[47] McChrystal et al, 163.

[48] McChrystal et al, 164–69.

[49] The OA framework is best used to address a scoped WMD system of concern within the global context. There are no hard and fast rules for scoping. The scope is typically initiated by the OA client and is further refined during the appreciation phase of the design process (often labeled the Information Support Package process in OA parlance.) In practice thus far, application of the OA framework has been sponsored by organizational clients such as geographic commandant commands, government departments and ministries, or special operations organizations in an effort to leverage the entire CWMD community of action in this mission space.

[50] J.C. Ramo, *The Seventh Sense: Power, Fortune, and Survival in the Age of Networks*, (New York: Little, Brown and Company, 2016), 104–105.

Preserving the integrity of CBRN forensic samples is administratively and logistically burdensome.—Kaszeta

The Forensic Challenge

By Dan Kaszeta

The suspected use of chemical, biological, radiological, and nuclear (CBRN) weapons or materials adds complexity to any international or internal conflict. It is critical that responses to such use are based on good information. The relatively new field of CBRN forensics, which is emerging out of domestic terrorism investigations, seeks to establish scientific facts through analysis of rigorously collected evidence. CBRN forensics are important to establishing actual facts, but are inherently difficult for a variety of reasons. The question of whether military forces, particularly Special Operations Forces (SOF), can conduct CBRN forensics in an adequate fashion is debatable; however, there are numerous pathways to improve the status quo.

Why CBRN Forensics Matter

In their traditional setting the forensic sciences provide the government and the populace a degree of confidence that the courts are making informed decisions based on all available information. The notion that forensics are solely for legal processes and not relevant or important outside the courtroom, however, does not withstand serious scrutiny. The scientific and procedural aspects of CBRN forensics are important in the context of international security. Were CBRN materials used? If so, was their use deliberate, accidental, or some kind of natural phenomenon? Confirmed acts of CBRN warfare might be used as justification to drop a bomb or wage war on another country. Even the suspected use of CBRN weapons or materials adds complexity to any international or internal conflict. Not every CBRN incident is obvious or discernable from natural phenomena. When deployed soldiers turn up in the field hospital with injuries from exposure to toxic industrial chemicals, this could be an indicator of hostile attack. Alternatively, they could have been exposed to toxic waste or contaminated debris from a chemical factory that had been damaged earlier in the conflict. Skyrocketing radiation counts on detection instruments could mean a "dirty bomb" has been detonated. But it is equally possible that an old commercial or medical radiological source has been encountered.

CBRN forensics also help to identify provenance (where did the bad stuff come from?) and attribution (who did it?). This is especially important for distinguishing state action from that of non-state actors, or non-state actors who are state proxies. Terrorists might develop an indigenous capability—e.g. the Aum

The Managing Director at Strongpoint Security, Mr. Dan Kaszeta previously served as a physical security specialist with the U.S. Secret Service and as a disaster preparedness advisor to the White House Military Office.

Shinrikyo cult sarin attacks in Japan in 1995—or acquire abandoned munitions—e.g. Islamic State of Iraq and the Levant seizure of Saddam-era munitions. Provenance may also help to identify state proxies, as was likely the case in early 2017 with the assassination of North Korean leader Kim Jong Un's estranged half-brother in a Malaysian airport with the nerve agent VX.

Confirmation, attribution, and provenance help to calibrate judicial, policy, and operational responses. Use of chemical and biological weapons is against international law. Prosecution of war crimes and acts of terrorism should occur wherever possible if the rule of law and international norms are to be maintained. Justice requires trials; prosecution requires evidence. The collection, preservation, and analysis of physical evidence must offer a high-degree of assurance so that the prosecutor can defend the evidence.

Imagine a SOF team that visits ten different buildings and collects samples of material from each during a two-day operation. Trace evidence of anthrax from one of the buildings is subsequently used to prosecute a terrorist. A wise defense attorney will question whether the SOF operators changed their gloves and boots between buildings. Were they sterile when the operators entered the building? How can you prove it? What about the bag they put the sample into? Was it clean? Did they take that empty bag to the other buildings? If these simple questions are not answered satisfactorily, there is no way to prove the anthrax came from the building in question or from a different building or location previously visited by the SOF team. Perhaps the team has detained the wrong person. Or if they got the right person, charges may not stick because the evidence has been discarded.

CBRN forensics must also be ironclad to combat alternative narratives, fake news, propaganda, and conspiracy theories. Every instance of real or alleged use of CBRN materials in recent years has led to allegations, alternative explanations ranging from the plausible to the esoteric, denials, and conspiracy theories. Perpetrators of such attacks have every incentive to muddy the waters and sow discord in order to create doubt and allow for deniability. One need only look at the well-documented miasma of stories and opposing narratives that have surrounded each use of sarin nerve agent in the war in Syria to see how this can look.[1] Sowing diverse stories is a tactic in information warfare and serves various ends, such as diluting public support for armed conflict or reducing morale. Even the seemingly clear-cut case last year in Khan Sheikhoun, Syria wherein a bomb filled with nerve agent fell out of the sky in a conflict where only one side has airpower, spawned an amazing array of alternative explanations.

Hard facts are needed to refute alternative explanations. As one of the expected effects of CBRN warfare is psychological, military commanders may have to explain what is going on to their unit, in order to preserve morale. If military personnel start to believe conspiracy theories and myths, it will tax morale and discipline. Commanders armed with solid information in which they have confidence are better placed to combat this threat.

CBRN forensics also have important implications for force protection. Knowledge of the physical characteristics of the CBRN materials actually used in attacks will allow defense measures that are based on practical first-hand knowledge rather than generic guidelines. For example, artillery shells filled with a nerve agent may be poorly designed and destroy much of their contents, and many of the shells are duds, and therefore do not disseminate the nerve agent. Therefore, the hazard area associated with such an artillery strike will be much smaller than the generic warning template in a manual that was written during the Cold War and assumes a high degree of munition efficiency. In practical terms, this means a much smaller hazard zone on

the commander's map and more mobility options as there are fewer areas to be avoided. But this is the sort of information that requires knowledgeable forensic analysis, with someone actually looking at the site of an artillery strike and assessing the impact craters and fragments of the shells.

CBRN Forensics is Challenging

The CBRN forensic discipline is difficult for environmental, technical, procedural, and organizational reasons. First, the nature of CBRN materials is such that the environments where they are present are inherently dangerous. Forensic operations must be performed while wearing protective clothing and respiratory protection commensurate with the threat, which if previously unknown, first requires an initial survey or reconnaissance to characterize the threat environment before detailed work can even begin.

"Time versus safety" is a paradox inherent in CBRN forensics. Much of the evidence at the crime scene is either fragile or short-lived. Gas and vapor can waft away without leaving a trace. Liquids can evaporate or react with the environment; for example, the nerve agent sarin is a liquid that can quickly evaporate from a liquid into a vapor and blow away with the wind. Powders, such as spores, can blow away. And sunlight can destroy bacteria and viruses. The bodies and clothing of victims may also contain evidence that is degraded by life-saving decontamination procedures.

Each CBRN material requires different sample collection techniques. Sample categories can be broadly divided into gas and vapor; liquid; and solid, which includes soil, surface trace, and biomedical as subcategories. It is not always obvious where a gas or vapor might reside since some are lighter than air. Liquid and solid sampling are relatively straightforward conceptually, but sampling while wearing cumbersome protective gear or conducting the operation in the wind or on the water can be a challenge. Additionally, trace samples are usually taken with wipes or swabs, which can require numerous different techniques and solvents, depending on the nature of the surface and material being tested. Biomedical samples—e.g. body fluid, hair, and tissue—are taken from live or deceased hosts, which is inherently complex. Samples from dead animals and body fluid samples from surviving victims have been probative in investigations in Syria.

CBRN forensics also requires the collection of conventional evidence. In many scenarios, this evidence will be more useful than the actual CBRN materials. For example, documents and fingerprints collected from a suspected clandestine laboratory may have far more investigative or intelligence value than a vial of a chemical warfare agent precursor compound. The explosive components of a "dirty bomb" may prove to have evidence value, post-detonation.

Preserving the integrity of all samples is administratively and logistically burdensome. Used and unused sample tools and containers need to be sterilized, documented, and analyzed. Protective gear must be changed frequently—a technician can use 50 pairs of gloves in one day—and the gear must be disposed of, treated as evidence, or cleaned before reuse to reduce the threat of cross-contamination.

Conventional evidence that may be contaminated by CBRN materials is problematic. A laboratory that can process chemical warfare materials may not be suited to collect fingerprints from a bottle, or exploit a smartphone, and vice versa. The laboratory that can exploit a laptop or mobile phone is not likely to be able to do so if the item is contaminated, or even suspected to be contaminated. This conundrum is poorly resolved in most parts of the world.

Finally, CBRN expertise and capabilities reside in disparate organizations. In many parts of the world, CBRN response is a fire department function, very similar to responses to industrial and commercial hazardous materials accidents. Fire services are

indeed well-equipped for most aspects of CBRN response; however, apart from arson investigation, fire departments do not collect forensic evidence.[2] In the United States, much of our expertise resides in clandestine narcotics law enforcement teams and environmental regulatory agencies that pursue criminal and regulatory enforcement of pollution and toxic waste rules. State and local law enforcement (and indeed most other countries) have very limited capability for CBRN forensics, for which the National Guard only recently started to develop and provide military support to civil authorities. There is the real question as to whether the level of care and precision required for CBRN forensics can reasonably be expected in a non-permissive environment, such as an active conflict zone.

CBRN Forensics in the Military Environment

CBRN forensics barely fits into the classic military CBRN mission set, which includes contamination avoidance (detection, hazard area prediction, warning, and reporting), individual protection (suits, gloves, and boots), collective protection, decontamination (of people and equipment), reconnaissance, and medical countermeasures. Military CBRN protective equipment is designed to keep the soldier in the fight for days or weeks, not for rapid changes of garments and gloves upon every entry and exit from a contaminated building. Conventional CBRN units, such as the U.S. Army Chemical Corps, are not equipped or trained for evidence collection to a forensic standard.[3] Soldiers are issued one, perhaps two sets of gloves—far short of the 20 or more required in an evidence collection mission. Additionally, military decontamination is all about "good enough" and not about "sterilized to a legal standard" for evidence collection. When is the last time, if ever, a soldier sterilized a tool (shovel) in the field? Military detection equipment is designed to provide rapid warning to military personnel, not for the collection of samples in sterile containers. CBRN reconnaissance is focused on finding the extent of contamination and checking if routes and axes of advance are safe, rather than the painstaking work of evidence collection.

The Defense Department recently gave the U.S. Special Operations Command (USSOCOM) more responsibilities in countering weapons of mass destruction, a term that generally implies all of the CBRN threats. However, CBRN forensics run contrary to key SOF axioms. CBRN forensics are slow, heavy, and manpower-intensive, while special operations generally are fast, light, and emphasize economy of force.[4] It is one thing to send in a small team to enter a house and seize a prisoner and a few laptops. Such a mission might be accomplished in minutes. If the same house had been a suspected clandestine laboratory, a thorough forensic exploitation might last a day or longer and require five times the personnel, as well as several cargo pallets of equipment.

Additionally, while domestic law enforcement operations that collect CBRN evidence may be an hour or two from the laboratory that will process the evidence, SOF often operate at some distance from their support. The transport of prohibited substances (potentially found on corpses) across international boundaries presents moral and legal issues. Also, any chain of custody document for a covert operation is likely to be highly classified and will never see a courtroom. Such evidence could still be made available to policymakers, but they will be in the position of telling the public to "trust us, but we cannot show you the paperwork"—that could help to promulgate the very propaganda, fake news, and conspiracy theories that CBRN forensics aim to combat.[5]

The Way Forward

If CBRN forensics are to be done, they need to be done well or not at all. An effort that is performed at an 80 percent standard might as well not have been

undertaken. Evidence that is tainted, cross-contaminated, spoiled, or mishandled could support erroneous conclusions.

There is no insurmountable reason why military forces, and especially SOF, could not conduct CBRN evidence collection. As a first step, military doctrine should express a requirement for forensic operations. CBRN forensic evidence collection will otherwise remain in the unfunded requirement or "nice to do" category and SOF units will not prioritize CBRN training.

Competent military CBRN specialists and SOF operators could easily be trained in CBRN forensics. Specialty courses offer the necessary skills and already exist within the civilian sector, but the military needs to commit to sending its personnel through this kind of training. Another way to bridge the expertise gap is to embed law enforcement or regulatory personnel within SOF. This likely will raise a host of other concerns, but might still be easier (and more effective) than the alternative of trying to turn SOF operators into CBRN forensic technicians.

Similarly, while existing military gear is indeed largely inadequate to the task of CBRN forensics, adapting existing forensic equipment to a military environment is certainly feasible. This has been done extensively in the realm of counter–improvised explosive device operations and biometrics, and there is no technical barrier to adapting the wide variety of commercial off-the-shelf equipment for SOF operations.

Traditional forensic labs need to be equipped with CBRN capabilities and traditional evidence collection technicians need to learn how to operate in a CBRN environment. There is no fundamental technical obstacle preventing the development of CBRN forensics laboratories that can be moved closer to the samples. Mobile CBRN laboratories already exist, albeit not specifically for forensic analysis. The skills and equipment exist. Training is available. The key issue is putting capabilities together into specialized teams and training and exercising these teams so that they can achieve competence. SOF have the justified reputation for quickly adapting to new missions and integrating new technologies into their operations, so adapting to CBRN forensics should not be too far a stretch, as long as command emphasis is given to it. PRISM

Notes

[1] George Monbiot "A Lesson from Syria: It's Crucial Not to Fuel Far-Right Conspiracy Theories," *The Guardian*, November 17, 2017, available at <https://www.theguardian.com/commentisfree/2017/nov/15/lesson-from-syria-chemical-weapons-conspiracy-theories-alt-right>.

[2] The author has seen training exercises where valuable evidence was literally flushed down the drains by firefighters.

[3] There are pockets of competence, however, including the U.S. Army's Technical Escort unit. Comparable capabilities in other militaries are exceedingly rare. As a disclaimer, the author cannot categorically state that there are or are not specialized units within USSOCOM or the Intelligence Community that are already well-trained for CBRN forensics, given the secretive nature of this line of business. There may be special teams unbeknown to the author because of secrecy and classification. If there are, then the United States is ahead of the curve and has taken the advice of this article already. The author's own experience is that these capabilities barely exist with some of the United States' European allies. CBRN forensics was never mentioned during the author's Chemical Corps training in the early 1990s.

[4] A colleague at the U.S. Secret Service had been a noncommissioned CBRN officer with a Special Forces group. CBRN protective equipment was often at the very bottom of the priority list for missions. Where the load is heavy and every ounce counts, and speed is of the essence, masks, suits, and gloves got left behind. And if you habitually leave it behind, training with it will not be a high priority.

[5] Critics and conspiracy theorists have criticized the apparent lack of chain of custody in the Syrian sarin investigations, although the Organization for the Prohibition of Chemical Weapons clearly did the best that they could under the circumstances.

Photos

Page 84: Stock photo ID:479256460

In 1998, People's Army guards from North Korea march in formation to their appointed posts during a repatriation ceremony in the Panmunjom Joint Security Area. (U.S. Air Force/ James Mossman)

North Korea's CBW Program

How to Contend with Imperfectly Understood Capabilities

By John Parachini

Any major conflict on the Korean Peninsula would put thousands of lives at risk even if it were well short of a nuclear exchange. The conventional forces aligned along the 38th parallel, the border between North and South Korea, are formidable. If a conflict were to erupt short of a nuclear exchange, many fear North Korea might use chemical or biological weapons (CBW). While there is some confidence in the assessments of North Korea's chemical weapons capabilities, comparatively little is known about its biological weapons capabilities. Lack of knowledge about North Korea's biological weapons capabilities is not unique. Aside from the United States, the former Soviet Union, South Africa, and Iraq—countries that have disclosed the nature of their past biological weapons programs—comparatively little is known about other state biological weapons programs.

Biological weapons programs tend to be among the most closely guarded weapons programs in a country's arsenal. By contrast, extensive documentation and histories of nuclear weapons programs exist for virtually all the known weapons states as well as those that abandoned such programs. In recent years, while North Korea (formally the Democratic People's Republic of Korea or DPRK) has gone to great lengths to demonstrate to the world its nuclear and missile programs, the country has hidden whatever CBW it may possess. As the international community grapples with how to reduce tension on the Peninsula, re-assessing what is known about North Korea's CBW program and considering options to minimize their role in the regime's security calculous is an important addition to the complex set of issues that U.S. civilian and military leaders must consider. This article attempts to put in context what little is known about North Korea's capabilities and offer some measures that might be taken to help curtail those capabilities.

Avoiding the "Iraq Moment" in North Korea

There are some parallels with what we knew about Iraq's weapons of mass destruction (WMD) program before 2003. In the Iraq case, the United States knew a good deal about past efforts, but not much about the status of the program at the start of the 2003 military operation. Former Iraq President Saddam Hussein's reluctance to openly disclose the abandonment of his WMD programs for fear of appearing weak to his own

Mr. John V. Parachini is a senior international policy analyst and director of the Cyber and Intelligence Policy Center at the RAND Corporation. This article draws from his testimony before the U.S. Congress in January that was last updated in early March.

people, or historical enemies such as Iran or the United States, confused assessments of Iraq's capabilities. Pretending to have capabilities he did not was hard to imagine.

In the case of North Korea, we know very little about either past or present CBW programs, plans, or intentions. The regime's nuclear and missile programs would appear to provide a credible deterrent against an external military threat. It is certainly possible, however, that the technical sophistication necessary to develop a nuclear capability, has been applied to CBW for the contingency of a non-nuclear fight. Chemical and biological weapons do not require as much industrial infrastructure or unique materials as nuclear weapons programs. The conundrum facing U.S. policymakers and military leaders is that they cannot wait until the "enemy is at the gate," the evidence is incontrovertible, and they are facing disaster before taking action. Conversely, hasty action can lead to a different form of disaster.

While it is important not to let attention to North Korea's nuclear weapons obscure the potential dangers CBW capabilities may pose, it is equally important not to overstate those dangers. Doing so might create an Iraq-like moment where feared capabilities catalyze preemptive military action that turns out to be mistaken. In one of the most heavily armed regions of the world, miscalculating the threat, either by over or underestimating it, can divert precious resources and leadership time in unproductive, or even destructive directions. As the Iraq case illustrates, such a miscalculation can have unanticipated consequences and enduring costs long past the initial operational objective. Prioritizing among the threats posed by different weapons categories poses is essential and, in the case of the highly secretive DPRK, inherently difficult. The nuclear weapons threat is certainly our greatest concern, but in light of the recent heightened tension on the Peninsula, calibrating how CBW and conventional weapons factor into the military standoff is more important than it has been since the end of the Korean War.

Given the horrific effects these weapons capabilities might cause, even a modest capability must be taken seriously. Information sources, some of which are indirect and difficult to validate, have been diverse and inconsistent. Additionally, North Korean skill at denial and deception further complicates any assessment of actual capabilities. Nevertheless, estimating the threat of North Korean CBW capabilities is important for determining the appropriate use of U.S. and allied resources. It is important to hedge against even low-probability threats if they have high consequences. On the Peninsula, where any military confrontation risks escalating to the nuclear precipice, U.S. and international community efforts should aim to reduce the likelihood of CBW usage because of the potential for escalation to cross the nuclear threshold, as well as the mass death CBW would cause by themselves. This danger has become more acute as the United States Nuclear Posture Review states that the United States retains the option of responding to non-nuclear threats with nuclear weapons.[1] Depending upon the context, any of North Korea's non-nuclear military capabilities might trigger a nuclear retaliatory attack.

A Credible Threat That is Easy to Produce

Since North Korea's chemical and biological programs are smaller and easier to embed in legitimate industrial production facilities they will be significantly harder to detect. Unlike nuclear tests, which generate seismic signatures, and missile launches, which can be detected via a variety of technical collection methods, CBW can be produced with some of the same production capabilities used for producing paint, pesticides, and pharmaceuticals.

There is some consensus that North Korea initiated work on chemical weapons in the 1960s

and began producing them in volume in the early 1970s.[2] Most estimates indicate that DPRK's chemical weapon arsenal contains nerve agents, blister agents, blood agents, choking agents, and riot-control agents. Their stockpile of chemical weapons is estimated to range from 2,500 to 5,000 tons.[3] This figure has not changed in more than a decade, which raises questions about its accuracy. Delivery methods are believed to include artillery projectiles, various types of rockets, aircraft, ballistic missiles, drones, and naval weapons systems.[4] The same numbers are repeated in several scholarly articles thereafter without change, again raising the question of accuracy. It is possible that the regime produced and weaponized this quantity of chemical agent at one point and never modernized further. If this is the case the quality of the chemical agent may have degraded. Alternatively, the regime may have continued to modernize its chemical weapons arsenal, in which case these tonnage figures are too low. Early assessments questioned whether the tonnage figures referred to weaponized agent or agent stored in bulk containers.[5] This underscores the number of unknowns even about a weapons capability that most analysts believe exists.

Some analysts believe that North Korea would use its chemical weapons to gain a quick strike advantage in the early stage of a ground conflict or as a retaliatory measure if the regime were on the verge of defeat.[6] They suggest North Korea would use chemical weapons to degrade South Korean and U.S. ground operations and to terrorize the civilian population in South Korea. Depending upon the intensity of the conflict, North Korea might also launch ballistic missiles with chemical payloads against U.S. air bases in the region to suppress U.S. air support to combat operations on the Peninsula. These are two among several plausible scenarios against which U.S. and allied planners must hedge, despite their uncertainty.

The recent murder of Kim Jong-Un's half-brother, Kim Jong Nam, with some form of VX nerve agent in Malaysia's Kuala Lumpur airport offers some insight into the Kim regime's willingness to use chemical weapons.[7] Assassinations can be carried out through a variety of means, and other countries have assassinated people with chemicals and toxins.[8] However, the context of this particular incident suggests the possibility that the means was selected not just for its lethal power: assassinating a regime adversary in such a public place with a chemical warfare agent may have been intended to send a message to the international community about the regime's chemical weapons arsenal and its willingness to use it.

Much to Fear, but Not Much Evidence

Our information sources are inconsistent, often outdated, and generally insufficient. What other factors might explain why we know so little about North Korean biological weapons capabilities? First, as noted, the regime may be able to hide biological weapon development activities more effectively than its nuclear and missile activities because of the significantly smaller required infrastructure and their dual-use nature. Efforts to develop biological weapons can be undertaken in facilities smaller than the industrial facilities required to produce chemical warfare agents, let alone nuclear weapons. Second, the regime may have never pursued a biological weapons capability to the same extent as other capabilities due to the inherent challenges of effective program management. Though DPRK joined the Biological Weapons Convention by accession in 1987, its dubious record of compliance (or non-compliance) with international accords is not reassuring. Third, international experience of state biological weapons programs suggests they take considerable time, resources, and expertise to achieve even rudimentary levels of capability. Fourth, the regime may have dedicated more resources to other components

In 2012, U.S. Secretary of Defense Ashton Carter tours the Military Armistace Commission Building in Panmunjom, South Korea in the demilitarized zone separating North and South Korea. (U.S. Navy/ Chad McNeeley)

of its military that showed potential for quicker and easier progress. Finally, the regime may only have defensive capabilities because it relies upon its nuclear capability for survival and does not view biological weapons as an effective deterrent.

In a 2012 white paper, the South Korean Ministry of National Defense (MND), assessed that North Korea "likely has the capability to produce a variety of biological weapons including anthrax, smallpox, plague, tularemia, and hemorrhagic fever virus," but provided no supportive documentation or evidence.[9] In 2016, the MND slightly altered the language to "sources indicate that North Korea is capable of cultivating and producing various types of biological agents such as anthrax, smallpox, and plague on its own."[10] Frankly, the same could be said for many other countries with industrial infrastructure similar to that of North Korea. The distinction, however, is the context of North Korea's aggressive actions, frequent non-compliance with international agreements, and flagrant disregard for international norms.

The evidence of a DPRK biological program is comparable to that for North Korea's nuclear, missile, and chemical, weapons programs. Defector reporting presents the most worrisome picture of the North Korean biological weapons program, but many of these reports are based on indirect or secondhand

knowledge, repeat what has appeared in the open press, or are evidently inaccurate.[11] During 2003–04 and again in 2009, several defectors claimed that North Korea tested biological agents on political prisoners.[12] Given how the regime has brutalized its people and inflicted violence on opponents, these reports are plausible albeit difficult to verify.

Several independent analysts and assessments by the government of South Korea estimate that North Korea has a dozen biological agents. If true, this is more BW agents than either the United States or the former Soviet Union produced in their BW programs.[13] There are reports that recent defectors have been vaccinated for anthrax, which has led to assertions that the regime has anthrax in its arsenal and is prepared to use it.[14] We cannot rule out the possibility, however, such vaccinations might be a routine practice of North Korea's defensive program. North Korea has argued for years that the United States attacked it with BW during the Korean War and fears the United States might again attack with BW. There is no credible evidence to substantiate North Korea's claim or its current fear.

As evidence of U.S. preparations to conduct a BW attack, North Korea cites the U.S. military's public acknowledgement that in 2015 it advertently sent live anthrax cultures to labs in the United States and to an American military base in South Korea.[15] Shortly after the mishap, Kim Jong-Un visited Pyongyang Bio-technical Institute, a pesticide plant that could be a cover for a BW production facility.[16] Images of the visit did not reveal the military security typical of known or suspected clandestine BW programs throughout history, nor did the images provide compelling evidence that the Institute was a BW facility cleaned up for show. The images did, however, reveal that the regime has obtained equipment that could be used perniciously, raising questions about North Korea's compliance with UN sanctions and underscoring the difficulty of determining the true nature of capabilities that are inherently dual-use.

Recent unclassified U.S. Government threat assessments have shed little if any light on any North Korean biological weapons program; in some instances, these assessments have changed without clear explanation. A threat assessment by the Central Intelligence Agency (CIA) in 1997 indicated that North Korea was "capable of supporting a limited [biological weapons] effort."[17] In 2005, then CIA Director Porter Goss reported that "North Korea has active [chemical weapons] and [biological weapons] programs and probably has chemical and possibly biological weapons ready for use."[18] Since 2014, the U.S. Intelligence Community's unclassified assessments on BW have dropped North Korea from the list of suspect programs. In 2014 Director of National Intelligence (DNI) James Clapper only singled out Syria as having "some elements" of a biological warfare program that had "advanced beyond the research and development stage."[19] One year later, DNI Clapper did not cite any biological weapons programs of concern.[20] Current DNI, Daniel Coats, also failed to mention any biological programs in his first World Wide Threat testimony—an annual requirement—before Congress in May.[21]

What circumstances or conditions might have changed between the earlier and the latest threat assessments? New information might have merited an update to the analytic line. Alternatively, given how the Kim regime shrouds its weapons programs in secrecy, some things might have been misinterpreted that were subsequently clarified. The known program may not be sufficiently significant to highlight. Another possibility is the information the DNI has cannot be revealed in open forums. Thus, while it may be tempting to take comfort in the diminished threat perception of the most recent assessments, there are many factors mitigating against greater confidence. Alas, the international community remains largely, and disconcertingly, in the dark.

CBW and Nuclear Support for Other State and Non-State Programs

North Korea is known to provide military assistance to demonstrate solidarity with its allies.[22] The regime's collaboration with Iran and Syria on their missile programs, with Hamas and Hezbollah on conventional weapons, with Syria on a nuclear reactor, and allegedly with Syria on chemical weapons development, all combine to heighten international concern that North Korea is willing to proliferate unconventional weapons and capabilities.

North Korean support of Syria's nuclear aspirations is the most extensive and disconcerting example of such proliferation that is in clear violation of the international norm. In the wake of the Israeli bombing of the North Korean–designed and built nuclear reactor, Syrians failed to acknowledge its destruction.[23] Their reluctance to publicly acknowledge the existence of the reactor fostered suspicion that it was intended for a clandestine nuclear program. To dispel any question about the nature of the nuclear reactor former CIA Director Michael Hayden in an op-ed from 2011 said that he told the U.S. President that the al-Kibar reactor North Koreans helped build for Syria "was part of a nuclear weapons program."[24] North Korean and Syrian decade-long cooperation on the reactor is indicative of the extent to which the North Korean regime is willing to violate international norms to support its allies and generate revenue.

There are also reports that North Korea has helped Syria with its CW program.[25] Press reporting indicates that a forthcoming report from a UN Panel of Experts will provide greater detail on North Korean assistance to Syria's chemical weapons capabilities that it only alluded to in a single paragraph on Syria in a 2013 report.[26] According to that report, Syria-bound ships from North Korea were interdicted and seized items included defensive chemical warfare equipment, such as protective clothing and chemical antidotes.[27] Press accounts revealed that one of the interdictions involved a Libya-flagged ship that was stopped by Turkish authorities while passing through the Dardanelles.[28] There are reports of similar shipments of equipment seized by Greek and South Korean authorities back in 2009.[29]

Although North Korea is known to have provided conventional weapons to Hamas and Hezbollah, either directly or via Iran, as well as tunneling equipment and training, no evidence has yet surfaced that it transferred nuclear, chemical, or biological capabilities to any non-state actors such as Hamas or Hezbollah.[30] The regime appears at least to have respected the international norm prohibiting transference of unconventional weapons to non-state actors.

Potential Measures to Curtail North Korea's CBW Capabilities

There are no "silver bullet" solutions to the threat that any North Korean CBW capabilities would pose. However, there are measures that may help to limit the desire of the Kim regime to expand its actual or latent CBW programs, to deter and reduce potential effectiveness of those programs against South Korea, and to re-enforce global norms against the production and use of poison, disease, and bacteria as weapons.

Promote Transparency via Reassurance

A recent proposal designed to decrease North Korea's security concerns, be they real or imagined, may also provide an opportunity to increase transparency regarding its chemical and biological weapons activities. The United States has pressed China to influence North Korea without much success. Tension on the Peninsula is rising to such a level that the international community may need to do more than to urge China to uphold its sanctions commitments and to press the North Korean regime to cease its nuclear and missile tests. The prospect of a meeting between the U.S. President

and North Korea's Supreme leader will hopefully reduce tension, but there is always a risk that tension may rise. If tension escalates to the brink of war, one dramatic and unconventional option to consider to avoid militarily intensive conflict may also provide an opportunity to achieve greater transparency on North Korea's CBW capabilities. Alton Frye, a long-time analyst and adviser to senior U.S. officials, recently suggested that China could station 30,000 troops in North Korea to reassure the regime of its survival.[31] This is the equivalent number of troops the United States has stationed in South Korea as a deterrent against DPRK aggression and to reassure the South Korean Government of the United States' commitment to its security. Another function of the Chinese forces could be to verify the regime's compliance with the Biological Weapons Convention and evaluate the security of its chemical weapons capabilities. This proposal assumes away potential complications such as how North Korea, South Korea, or the United States might not want Chinese troops on DPRK soil. Additionally, the Chinese leadership might not want to be seen as an occupying state. Yet, if the alternative that hangs in the balance is a major war that could escalate to a nuclear exchange, all parties in the regime may welcome a confidence building measure that is hard to imagine now. Interested parties should look for opportunities to suggest transparency measures as bi-products of any initiatives that shift relations on the Korean Peninsula.

Help South Korea with CB Defenses

Helping South Korea bolster the chemical and biological defenses of its armed forces and civilian population near the DMZ can strengthen deterrence by denial. If the South Korean armed forces have better chemical weapons protective gear, and train more to operate in a battlespace contaminated by chemical warfare agents, North Korea may be less inclined to use chemical weapons. Given the size of the civilian population this will be difficult to accomplish on a nationwide basis in South Korea, so it should by no means be considered a solution to the threat. However, South Korea might look to Israel as an example of how a state might prepare to mitigate the effects of a possible chemical weapons attack.

While North Korean chemical weapons are a more immediate threat to South Korea, additional bio-defensive measures might serve a similar purpose. There are reports that the South Korean armed forces intend to vaccinate members for anthrax next year. Improving South Korea's disease surveillance capabilities serves a public health benefit by helping to detect any future outbreak of a SARS (severe acute respiratory syndrome) or MERS (Middle Eastern respiratory syndrome)-like epidemic or a biological weapons attack. The United States and South Korea have cooperated on the deployment of the Joint United States–Korea Portal and Integrated Threat Recognition (JUPITR) program, which provides a biosurveillance capability that speeds up the detection of biological threats from days to hours.[32] The deployment of this system or some other biosurveillance system has a potentially important dual-use benefit.

Call for a No-First-Use of CBW Pledge on the Peninsula

South Korea, the United States, other members of the Six-Party Talks, or the UN Security Council should call for a pledge of no-first-use of CBW on the Peninsula. Since South Korea is a member of both the Chemical and Biological Weapons Conventions, and does not have offensive chemical or biological weapons programs, a pledge of no-first-use is a benefit for South Korea without any military downside. Since North Korea has publicly stated that it is a member of the Biological Weapons Convention when challenged about its biological weapons capabilities and asserted that it "does not develop, produce and stockpile chemical weapons

and opposes chemical weapons themselves", there is at least some acknowledgement that these are taboo weapons.[33] Until there is greater transparency on the Kim regime's dual-use facilities, its claims will be suspect. Nonetheless, highlighting concerns about CBW on the Peninsula and how they would complicate a potential conflict may encourage restraint on the part of North Korea. Finally, while North Korea's nuclear and missile programs are its most threatening military capabilities and warrant enduring international pressure for restraint, shifting some of the focus to other military capabilities may provide an opportunity for some arms control dialogue.

North Korea may not be willing to engage in any dialogue about its actual or latent CBW any more than it has with its nuclear and ballistic missile capabilities. However, there is a broader international audience to underscore the taboo on CBW production and use. The taboo on the production and use of chemical weapons has eroded considerably in the Middle East following the Iran–Iraq war in the 1980s, Iraqi use against the Kurds in the 1990s, and Syrian use against regime opponents in the past five years. Introducing the idea of a no-first-use of CBW pledge on the Korean Peninsula may start a process that leads to greater restraint and some transparency. The taboo can extend beyond production and use to also include transfer to third parties.

Conclusion

North Korea's actual and latent CBW capabilities are an underexamined and imperfectly understood factor in the military tinderbox on the Peninsula. In contrast to the ways the Kim regime has highlighted its nuclear and ballistic missile capabilities, it has largely shrouded its chemical and biological capabilities in secrecy. Its chemical weapons capabilities are the higher priority threat as they are easier to produce in volume than biological weapons, and the regime has never embraced the CWC. The regime's biological weapons capabilities are less understood, are less certain to be effective during warfighting, and are probably less developed. Moreover, the regime has at least joined the BWC by accession, although its credibility in adhering to agreements does not inspire confidence. Both weapons capabilities warrant enduring vigilance, as North Korea has proven that it can surprise the international community with rapid advances in its military capabilities. PRISM

Notes

[1] Office of the Secretary of Defense, Nuclear Posture Review, February 2018, 33, available at <https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF>.

[2] International Crisis Group, "North Korea's Chemical and Biological Weapons Programs," *Asia Report*, No. 167, June 18, 2009, available at <https://www.crisisgroup.org/asia/north-east-asia/korean-peninsula/north-korea-s-chemical-and-biological-weapons-programs>.

[3] For an excellent review of issues associated with the sourcing on North Korea's chemical and biological weapons programs see, Elisa D. Harris, "Threat Reduction and North Korea's CBW Programs," *The Nonproliferation Review*, Fall–Winter 2004. See also, Sonia Ben Ouagrham-Gormley, "Potemkin or real? North Korea's biological weapons program," *Bulletin of the Atomic Scientists*, January 11, 2018, available at <https://thebulletin.org/potemkin-or-real-north-korea's-biological-weapons-program10957>.

[4] International Crisis Group, 2009; See also Joseph S. Bermudez, Jr., "North Korea's Chemical Warfare Capabilities," *38 North*, October 10, 2013, available at <http://www.38north.org/2013/10/jbermudez101013>; and Kyle Mizokami, "Everything You Need to Know: North Korea's Chemical Weapons Are No Joke," *National Interest*, August 10, 2017, available at <http://nationalinterest.org/blog/the-buzz/everything-you-need-know-north-koreas-chemical-weapons-are-21849>.

[5] Gordon M. Burke and Charles C. Floweree, *International Handbook on Chemical Weapons Proliferation*, (Westport, CT: Greenwood Press), 1991.

[6] International Crisis Group, "North Korea's Chemical and Biological Weapons Programs," *Asia Report*, No. 167, June 18, 2009, p., 8, available at <https://www.crisisgroup.org/asia/north-east-asia/korean-peninsula/north-korea-s-chemical-and-biological-weapons-programs>. See also, Kyle Mizokami,"Everything You Need to Know: North Korea's

Chemical Weapons Are No Joke," *The National Interest*, August 2017, available at <http://nationalinterest.org/blog/the-buzz/everything-you-need-know-north-koreas-chemical-weapons-are-21849>.

[7] For an account of how the attack was likely conducted, see Doug Bock Clark, "The Untold Story of Kim Jong-nam's Assassination," *GQ*, September 25, 2017, available at <https://www.gq.com/story/kim-jong-nam-accidental-assassination>.

[8] Nick Holdsworth and Robert Mendick, "Prime Suspect in Georgi Markov 'umbrella poison' murder tracked down to Austria," *The Telegraph*, March 23, 2013, available at <http://www.telegraph.co.uk/news/uknews/crime/9949856/Prime-suspect-in-Georgi-Markov-umbrella-poison-murder-tracked-down-to-Austria.html>. For another example see, Griff Witte and Michael Birnbaum, "Putin implicated in fatal poisoning of former KGB officer at London hotel," *Washington Post*, January 21, 2016, available at <https://www.washingtonpost.com/world/putin-implicated-in-fatal-poisoning-of-former-kgb-spy-at-posh-london-hotel/2016/01/21/2c0c5052-bf92-11e5-98c8-7fab78677d51_story.html?utm_term=.addd9ddee625>.

[9] Ministry of National Defense, Republic of Korea, "2012 Defense White Paper," (December 2012), 36, available at <https://www.nti.org/media/pdfs/ROK_2012_White_Paper.pdf>.

[10] Ministry of National Defense, Republic of Korea, "2016 Defense White Paper," 34, available at <http://www.mnd.go.kr/user/mndEN/upload/pblictn/PBLICTNEBOOK_201705180357180050.pdf>.

[11] Elisa D. Harris, "Threat Reduction and North Korea's CBW Programs, *The Nonproliferation Review*, (Fall–Winter 2004), 91.

[12] Bruce Bennett, "The Challenge of North Korean Biological Weapons," testimony presented before the House of Representatives Armed Services Committee on Intelligence, Emerging Threats and Capabilities, October 11, 2013, available at <https://www.rand.org/pubs/testimonies/CT401.html>. See also Bermudez, 2013.

[13] Elisa D. Harris, "Threat Reduction and North Korea's CBW Programs, *The Nonproliferation Review*, (Fall–Winter 2004), 90.

[14] Sofia Lotto Persio, "North Korean Soldier had 'Anthrax Antibodies,' Raising Concerns Over Pyongyang's Biological Weapons Plans," *Newsweek*, December 12, 2017, available at <http://www.newsweek.com/north-korean-soldier-who-defected-may-have-been-vaccinated-against-anthrax-759919>. See also, Patrick Knox, "War and Pestilence: Defected North Koren soldier 'vaccinated' against Anthrax amid fears Kim Jong-un plans to use bio-Weapons to spread lethal infectious disease," *The Sun*, December 26, 2017, available at <https://www.thesun.co.uk/news/5213774/defected-north-korea-soldier-vaccinated-anthrax-kim-jong-un-bio-weapons/>.

[15] Sara Reardon, "US Military Accidently Ships Live Anthrax to Labs, *Nature*, May 28, 2015, available at <https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF>. See also, Patrick Tucker, "This is Why The Army Sent Anthrax to South Korea, Australia, and 11 States, *Defense One,* May 29, 2015, available at <http://www.defenseone.com/technology/2015/05/why-army-sent-anthrax-south-korea/114094/>; Barbara Starr, "Army may have shipped live anthrax to Australia, *CNN*, May 29, 2015, available at < https://www.cnn.com/2015/05/27/politics/live-anthrax-us-military-sent-inadvertently/index.html>.

[16] Melissa Hanham, "Kim Jong Un Tours Pesticide Facility Capable of Producing Biological Weapons: A 38 North Special Report," 38 North, (July 9, 2015), available at <http://www.38north.org/2015/07/mhanham070915>.

[17] Central Intelligence Agency, "Report of Proliferation-Related Acquisition in 1997," last updated June 19, 2013, available at <https://www.cia.gov/library/reports/general-reports-1/report-of-proliferation-related-acquisition-in-1997.html#North-Korea>.

[18] Porter J. Goss, "Global Intelligence Challenges 2005: Meeting Long-Term Challenges with a Long-Term Strategy," (February 16, 2005), available at <https://www.cia.gov/news-information/speeches-testimony/2005/Goss_testimony_02162005.html>.

[19] James R. Clapper, "Statement for the Record: U.S. Intelligence Community Worldwide Threat Assessment," January 29, 2014, available at <https://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf>.

[20] James R. Clapper, "Statement for the Record: US Intelligence Community Worldwide Threat Assessment," February 26, 2015, available at <https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf>.

[21] Daniel R. Coats, "Statement for the Record: US Intelligence Community Worldwide Threat Assessment," May 11, 2017, available at <https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1757-statement-for-the-record-worldwide-threat-assessment-of-the-u-s-intelligence-community-before-the-ssci>.

[22] Bruce E. Bechtol Jr., "North Korea and Syria: Partners in Destruction and Violence," *The Korean Journal of Defense Analysis*, vol. 27, no. 3 (September 2015), 277-92.

[23] David Makovsky, "The Silent Strike: How Israel bombed a Syrian nuclear installation and kept it

secret," *The New Yorker*, September 17, 2012, available at <https://www.newyorker.com/magazine/2012/09/17/the-silent-strike>.

[24] Michael V. Hayden, "Correcting the Record About that Syrian Nuclear Reactor," *The Washington Post*, September 22, 2011, available at <https://www.washingtonpost.com/opinions/correcting-the-record-about-that-syrian-nuclear-reactor/2011/09/22/gIQA1xZtoK_story.html?utm_term=.b6692ab3a4d4>.

[25] Michael Schwirtz, "U.N. Links North Korea to Syria's Chemical Weapons Program," *New York Times*, February 27, 2018, available at <https://www.nytimes.com/2018/02/27/world/asia/north-korea-syria-chemical-weapons-sanctions.html>. See also, Edith M. Lederer, "UN Experts Link North Korea to Syria's Chemical Weapons Programs," *Chicago Tribune*, February 27, 2018, available at <http://www.chicagotribune.com/news/nationworld/ct-north-korea-syria-chemical-weapons-20180227-story.html>.

[26] UN Panel of Experts. *Note by the President of the Security Council*, United Nations Security Council, S/2017/742, September 5, 2017.

[27] UN Panel of Experts. *Note by the President of the Security Council*, United Nations Security Council, S/2012/442, June 14, 2012, p. 28. See also, Bruce E. Bechtol Jr., "North Korea and Syria," 277–92.

[28] Barbara Demick, "North Korea Tried to Ship Gas Masks to Syria, Report Says," *Los Angeles Times*, August 27, 2013, available at <http://articles.latimes.com/2013/aug/27/world/la-fg-wn-north-korea-syria-gas-masks-20130827>.

[29] *Military and Security Developments Involving the Democratic People's Republic of Korea 2012*, (Washington, D.C.: Office of the Secretary of Defense), 23. See also, Bermudez, 2013.

[30] Bruce E. Bechtol Jr., "North Korea and Syria," 277–92. See also, Carl Anthony Wege, "The Hizballah-North Korean Nexus," *Small Wars Journal* (2011),1-8. See also,:Bermudez, 2013.

[31] Alton Frye, "China Should Send 30,000 Troops into North Korea," *Foreign Policy*, November 28, 2017, available at <http://foreignpolicy.com/2017/11/28/china-should-send-30000-troops-into-north-korea-symmetrical-reassurance/>.

[32] Hyun-Kyung Kim, Elizabeth Philipp, and Hattie Chung, "The Known and Unknown: North Korea's Biological Weapons Program," *Harvard Belfer Center for Science and International Affairs* October 2017), available at <https://www.belfercenter.org/sites/default/files/2017-10/North%20Korea%20Biological%20Weapons%20Program.pdf>. See also Kevin McCaney, "JUPITR Integrates All Threats into One Early Warning System," *Defense Systems* (December 8, 2015), available at <https://defensesystems.com/articles/2015/12/08/army-jupitr-chem-bio-base-protection.aspx>.

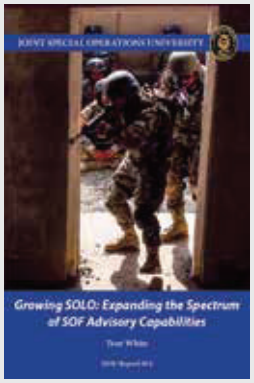
[33] "North Korea Denies Chemical Weapons Link with Syria: State Media," *Reuters*, March 1, 2018, available at <https://www.reuters.com/article/us-northkorea-syria/north-korea-denies-chemical-weapons-link-with-syria-state-media-idUSKCN1GD6IZ>.

JOINT SPECIAL OPERATIONS UNIVERSITY (JSOU) PRESS PUBLICATIONS

These recent JSOU publications are available at https://jsou.libguides.com/jsoupublications.

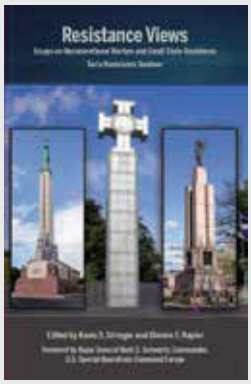
Advancing SOF Cultural Engagement: The Malinowski Model for a Qualitative Approach, by Robert R. Greene Sands and Darby Arakelian

In Advancing SOF Cultural Engagement: The Malinowski Model for a Qualitative Approach, the authors propose a special operations relevant model for engaging populations, illuminating their worldviews and values, appreciating their interests, and translating significant social, cultural, and political information into operational analysis. Their objectives are to introduce the core concepts, the base vocabulary, and the foundational skills in anthropology and sociology necessary for improving the human aspects core competency. While Greene Sands and Arakelian do not expect SOF to become anthropologists, they assert that Malinowski's population-centric research methods are desperately needed to make sense of contemporary human aspects of military operations.



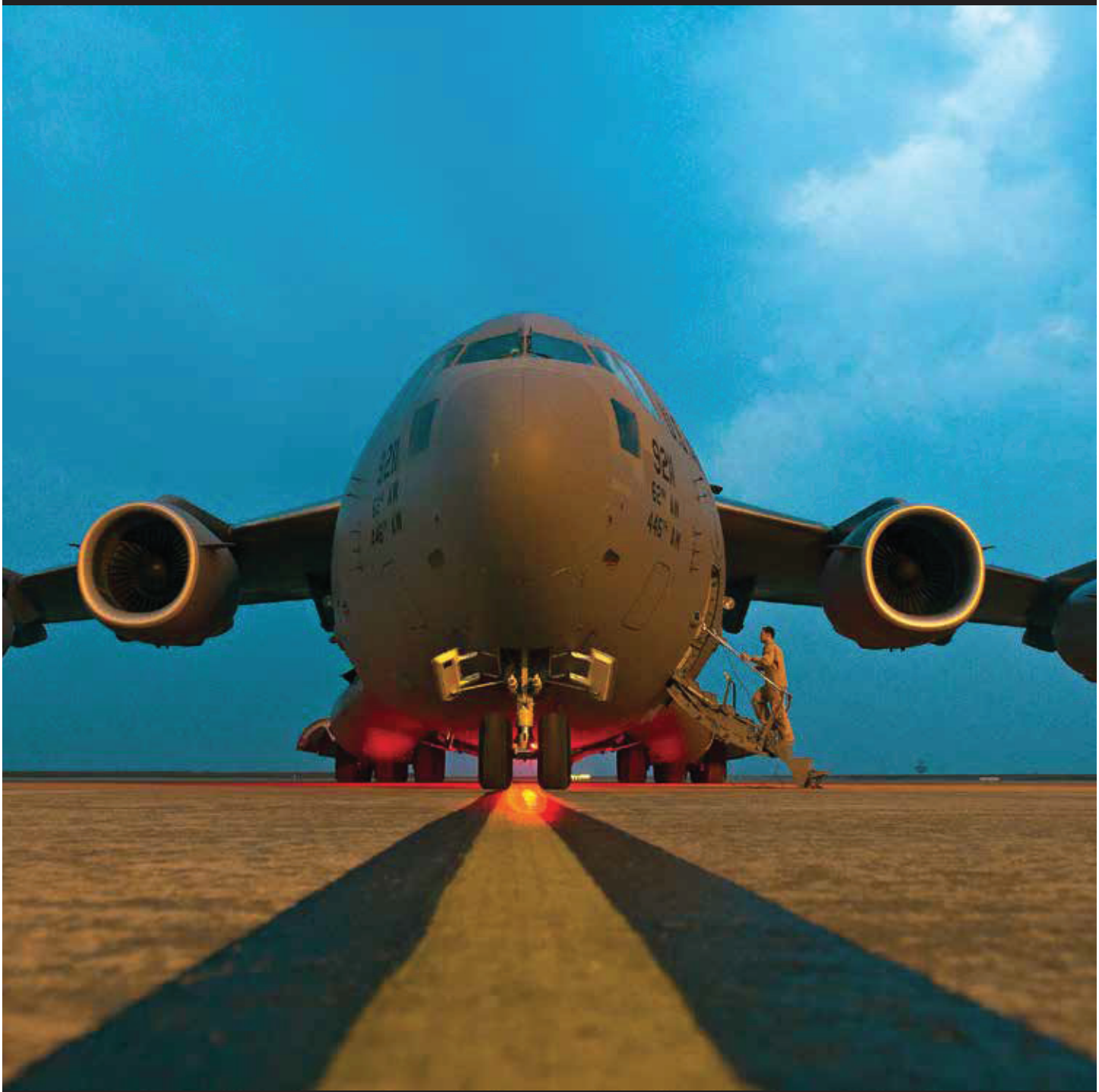
Growing SOLO: Expanding the Spectrum of SOF Advisory Capabilities, by Troy White

The SOF advisory role is a long-term commitment to help enable and aid other nations improve their military forces and security. SOF advisors have traditionally operated at the tactical level to increase partner capabilities 'by, with and through' to generate sufficient rule of law, address local needs, and advance rapport building. Mr. White advocates for a SOF role in advising foreign militaries at the high operational/strategic and ministerial levels. He provides real world examples through four vignettes of SOF advisors in Afghanistan, Iraq, Colombia, and the Philippines. This monograph is a handy resource for commanders and planners needing to establish a rapport with allies and friends at the highest operational/strategic and ministerial levels.



Resistance Views: Tartu Resistance Seminar Essays on Unconventional Warfare and Small State Resistance, Edited by Kevin D. Stringer and Glennis F. Napier

This volume is based upon the discourse, dialogue, and outcomes of the 2nd Senior Unconventional Warfare (UW) and Resistance Seminar, hosted by the Joint Special Operations University (JSOU); Baltic Defence College (BALTDEFCOL); U.S. Special Operations Command Europe (USSOCEUR); Estonian Special Operations Forces; and the Centre for Applied Studies, Estonian National Defence College. From 4–6 November 2014, a multinational and interagency group of academics and practitioners gathered at the Baltic Defence College in Tartu, Estonia to discuss and debate the study and practice of UW and resistance. This book's aim is to spark intensive discussion on both UW and counter–UW approaches, doctrine, and capabilities.



A U.S. Air Force C-17 prepares to depart Iraq with U.S. Marine Corps Gen. Joseph F. Dunford Jr., Chairman of the Joint Chiefs of Staff, Jan. 8, 2016. During the trip, Dunford met with U.S. and coalition leaders in Germany, Iraq and Turkey to assess the progress of counter–ISIL efforts. (DOD/Dominique Peneiro)

"The Irreducible Minimum"
An Evaluation of Counterterrorism Operations in Iraq

By Richard Shultz

With the end of full-scale combat operations in Iraq in late April 2003, no one at the senior level in Washington or Baghdad expected an organized insurgency to materialize—a "war after the war" was unimaginable. However, mounting violence in August suggested otherwise. Then, in the early fall, several high-profile attacks took place: a member of the Iraqi governing council was assassinated; the United Nations Headquarters and International Committee of the Red Cross offices in Baghdad, and the Italian police facility in Nasiriya were hit by suicide bombs; and a Chinook helicopter was shot down near Fallujah, killing 15 American soldiers.

By the beginning of 2004, the violence had shifted from periodic high-profile episodes to a rapidly increasing number of attacks against U.S. forces and facilities. During early January, the number of significant insurgent activities reported throughout Iraq was more than 200 each week. By the last week of April, these spiked to more than 600 and continued to fluctuate around that number for the rest of 2004. During 2005 the number of weekly incidents, on more than one occasion, climbed to more than 800.[1]

A key actor in the burgeoning insurgency was al-Qaeda in Iraq (AQI), which was comprised of an array of planning and decisionmaking mechanisms, operational detachments, financial units, communications and media centers, intelligence branches, bomb and improvised explosive device production facilities, and arms acquisition systems. AQI's internal workings and organizational structure were considerably different from 20th century counterparts. It was a web of networks.

AQI's center of gravity was not the top leadership but all those who commanded and managed the mid-level functional components of its networks. It was AQI's mid-level leaders and managers who had authority and capacity to maintain and even escalate operations. And there was a plethora of them operating across Iraq.

Task Force–714

During the 1990s, the United States Special Operations Command (USSOCOM) developed a highly proficient counterterrorism (CT) force tailor-made for hostage rescue and discrete, direct-action operations.[2] Arguably, that force became the best of its kind in the world. It also was a highly compartmentalized force with a culture of secrecy and semi-autonomy. But for the infrequent missions it was designed to carry out

Dr. Richard Shultz is the Director, International Security Studies Program with the Fletcher School at Tufts University.

prior to 9/11, those characteristics did not impede its operational capacity.[3]

In planning Operation *Iraqi Freedom* (OIF), consideration was not given to the possibility that in its aftermath a protracted irregular war would follow, and that U.S. counterterrorism forces, which had deployed to Iraq as Task Force–714 (TF–714), would play a major role in fighting the irregular war. Following the fall of Baghdad, General Stanley McChrystal, who took command of the counterterrorism forces in 2003, focused on capturing or killing high-value former Ba´athist leaders—"the deck of cards."[4]

However, while this was taking place, the security situation in Iraq rapidly deteriorated. During the fall of 2003 there were signs—often dismissed by Washington—that pointed to an organized insurgency rapidly taking shape. And as it grew in intensity, the mission of TF–714 changed from taking out a small number of top Ba´athists to going to war against an enemy that was different from any it had previously prepared to confront. Lieutenant General Michael Flynn, TF–714's intelligence chief beginning in the late spring of 2004, characterized AQI as "a strategic surprise" because "the capability and scale of the threat [it posed] was far bigger than any we had ever previously thought about . . . Clearly, the scale of the terrorist networks that existed . . . and the scope of AQI's operations surprised us."[5]

Surprise is a constant in war. But the surprise experienced by TF–714 in Iraq proved to be a major challenge even for an organization comprised of units that excelled at tactical adaptation. Consequently, TF–714's initial response was to do more of what it already did extremely well. "The initial response," explained General McChrystal in a 2014 interview, was that "we will just do more of what we are already very good at and then we would have done our part."[6] What became evident to the task force leadership, however, was that a "more of the same" response was not going to have a meaningful impact on AQI. To be sure, those operations that TF–714 executed were highly successful. The problem was there were not enough of them. They had, at best, only a limited impact on AQI's operational tempo. The Task Force was facing an enemy it had never envisaged and could not degrade through its existing ways of operating.

We needed to view the mission differently and that was whether we were winning or losing in Iraq against al-Qaeda, not just whether we captured or killed its members. Winning is what counts. That's our metric of success.
—General Stanley McChrystal, USA (ret.) [7]

Task Force–714 was operating as a peacetime strategic scalpel, and no matter how excellent, it was losing ground in an unfamiliar wartime environment. A sea change was required, explained McChrystal: "We needed to view the mission differently and that was whether we were winning or losing in Iraq against al-Qaeda, not just whether we captured or killed its members. Winning is what counts. That's our metric of success."[7]

By the fall of 2004 the realization set in that TF–714 had to change from a strategic scalpel to an industrial-strength CT machine. It had to "capture or kill on an industrial scale which was not something it had ever been built to do," explained

Admiral William McRaven, who served as Deputy Task Force Commander under General McChrystal, and later replaced him.[8] To operate at the industrial-strength level meant that "the basic mission fundamentally had to change," which was going to "require us to change the way we were organizationally structured, manned, trained, equipped, and everything else."[9]

Task Force–714 had suffered a strategic surprise for which it was not prepared, but was not paralyzed by it. Rather, it recognized the significance of what it had discovered and that it would have to demonstrate agility and adaptability to overcome an enemy unlike any terrorist organization that had preceded it. AQI was, said McChrystal, "much bigger . . . much more dynamic. It had more speed, momentum, and was benefiting from a very different operating environment than the task force had ever anticipated."[10]

By early 2005 McChrystal concluded the task force had to "adapt to a new, more ominous threat."[11] During the next two years TF–714 did just that, reinventing itself in the midst of the Iraq war. Consider the following acceleration in its capacity to conduct operations against AQI's networks. In August 2004, TF–714 was able to execute 18 raids across Iraq. "As great as those 18 raids were, they couldn't make a dent in the exploding insurgency," McChrystal explained. In August 2006, TF–714 executed 300 raids.[12] And those raids did much more than decapitate the top leadership of AQI. More importantly, the raids began to dismantle AQI's extensive network of mid-level operational commanders and the managers of its operational cells, financial units, communications centers, IED facilities, and arms acquisition enterprises.

In doing so, by late 2009 TF–714 had acutely degraded AQI's capacity to carry out operations. In General McChrystal's words, TF–714 "clawed the guts out of AQI."

Transformation in Wartime

The capacity of TF–714 to transform runs counter to what organizational theory experts identify as barriers inhibiting militaries from learning, innovating, and changing, especially in wartime.[13] But its leadership concluded that they faced an enemy never envisaged that could not be degraded through preexisting ways of operation. Organizational experts argue that for organizations facing complex challenges, problem solving must become a shared responsibility for the whole organization, not just the task of the leadership. It is the duty of the entire organization—a new way of thinking and acting.[14]

TF–714's method of problem solving was too deliberate, hierarchical, and self-contained to counter Iraq's fast-paced and networked insurgency. The Task Force had to transform and partner with several U.S. intelligence agencies to neutralize this unprecedented operational challenge. The mechanism for that transformation was a joint interagency task force (JIATF). The JIATF forged these intelligence agencies and TF–714 into a union, based on interdependence and cooperation that established problem solving methods capable of uncovering AQI's networks. Having adopted the JIATF, TF–714 shed its top-down style of command, substituting decentralized authority and problem solving from below. To outpace AQI, problem solving and decisionmaking could not wait for senior leaders to disseminate commands—that took too long.

TF–714 transformed into an intelligence-led organization. The action arm of the JIATF, the operational units, was coordinated with a robust intelligence capability drawn from the Central Intelligence Agency (CIA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Defense Intelligence Agency (DIA), and National Geospatial-Intelligence Agency (NGA), among others.

To learn and adapt, TF–714 amassed information and knowledge about a new problem set—a complex, clandestine, and networked enemy empowered by information age technology. The Task Force achieved intelligence dominance over AQI. This necessitated the JIATF's adoption of a new operational concept—find, fix, finish, exploit, analyze, and disseminate (F3EAD). This transformed targeting and provided the means to get inside AQI's networks to dominate the operational tempo of the fight.

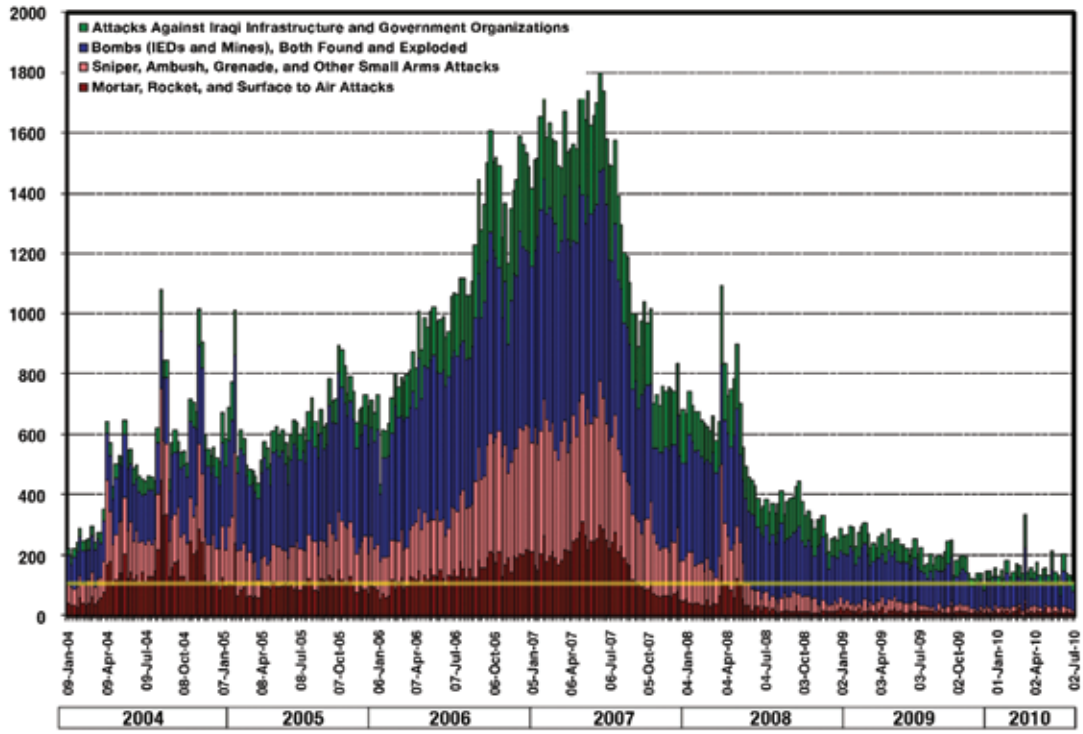
Once inside, the JIATF identified central and peripheral figures, patterns of behavior, and clusters of nodes to degrade parts of AQI's operating system. By doing this fast enough—hitting many targets each night—TF–714 outpaced AQI's capacity to adapt, causing it to collapse in upon itself.

The focus of the remainder of this article is on the impact that transformation had on AQI's operational tempo and the extent to which it allowed TF–714 to eliminate a large number of its mid-level commanders and managers, those who made AQI networks work.[15]

The "Irreducible Minimum"—Winning at the Operational Level

A situation report of U.S. prospects in Iraq from the spring into the early fall of 2006 would have had the following bottom line assessment: *surging violence and a grim prognosis*. To be sure, such a forecast could have been deduced from the escalating "significant acts of violence" reported in the Department of Defense's *Weekly Security Incidents*

Figure 1: Variables of Reconstruction and Security in Post–Saddam Iraq.



Source: Iraq Index: Tracking Variables of Reconstruction & Security in Post-Saddam Iraq (Washington, DC: The Brookings Institution, November 30, 2011).[20]

summary. By September 2006 those totals had risen to more than 1,400—nearly double from the previous summer. And by the summer of 2007, significant acts of violence peaked at nearly 1,800 incidents weekly.[16] Enemy violence was skyrocketing, while almost every prediction of any possibility of U.S. success in Iraq was spiraling downward.[17]

However, by the end of 2009 significant acts of violence had plummeted to fewer than 200 a week. And this trend continued into 2010 as can be seen in the graphic below of weekly enemy attacks against U.S. and coalition partners.[18] Another measure of the decline in the insurgency was the decline in U.S. military fatalities. That number had escalated from 486 in 2003 to 904 in 2007. However, in 2009 the number had dropped to 149, and in 2010 to 60.[19]

The security situation had dramatically changed at the operational level.[21] Factors that contributed to this dramatic change include:

- the adoption of a new counterinsurgency (COIN) strategy;
- the addition of 30,000 troops through the Surge;
- the Awakening Movement, which opened the door for the remarkable growth of police which, in turn, gave the coalition forces the capacity needed to control the physical and human terrain once cleared of insurgent forces; and
- the operations conducted by TF–714 against AQI's clandestine networks.

The introduction of COIN began with the Marine campaign plan initiated in early 2006 in Anbar Province. At that time, many believed Anbar was lost.[22] But by the end of 2006, Anbar was reaching a security tipping point. The COIN-based campaign plan with its interrelated elements of clearing out insurgents through maneuver operations, holding that territory through combat outposts, engaging and aligning with the sheikhs and their tribes, and building local Iraqi police units drawn from those tribes had shifted the ground in Anbar. The conditions were in place to bring about a sea change in 2007.[23] That came in the late spring when the weekly violent incidents for the province dropped from 450 attacks the first week of January to roughly 150 four months later. By July it was less than 100.[24] And when General John Kelly took command of the Marines in Anbar in January 2008, the number was down to 50 attacks a week.[25]

In February 2007, General David Petraeus replaced General William Casey as commander of Multi-National Force–Iraq. He initiated a similar COIN effort enabled by the addition of 30,000 surge forces and the Awakening Movement. The latter was critical to success. As the Marines found in Anbar in 2006, "without the Awakening, the surge would not have stabilized Iraq by the summer of 2008. It was not until the Sons of Iraq stood up that bloodshed fell fast enough; without them, our findings suggest that Iraq's violence would still have been at mid-2006 levels when the surge ended."[26] The focus initially of the Surge was on the greater Baghdad region. As in Anbar, the results were the same as the violence declined precipitously by the end of 2008.[27]

But effective counterinsurgency requires more than the "clear, hold, build" formula found in the classic COIN literature of the 1960s, as well as in its post–9/11 counterpart, Field Manual 3–24 on Counterinsurgency.[28] It also necessitates the capacity to dismantle the clandestine infrastructure or secret underground apparatus of the insurgent organization. It was that subterranean networked mechanism that gave AQI the capacity to initiate, rapidly increase, and sustain insurgent operations across Iraq. The mission of the Task Force was to learn about the inner workings of that largely invisible ecosystem in order to dismantle it.[29]

To what extent was TF–714 able to accomplish this mission and dismantle AQI's networks? As noted earlier, it was able to raise its monthly

operational tempo from 18 raids in August 2004 to 300 in August 2006, and to sustain that rate into 2009. But how effective were those operations? To what extent were they able to "claw the guts out of AQI" so that its networks collapsed?

The linchpin for degrading AQI's operational capacity was to reduce its mid-level commanders and managers, those who made its networks run; what McChrystal described as "the guts of AQI." They were identifiable and potentially vulnerable because they had to move, communicate, and make things happen. But to try to identify, isolate, and focus on one key node or individual within AQI networks at a time "was a fool's mission trying to be so precise. It was beyond what we could know when we initiated operations against a particular network in AQI," McChrystal noted. The alternative was to focus on the attrition of those mid-level elements as they emerged through the F3EAD process. "To hit those targets faster than they could replace them, to make them worry about our ability to constantly pummel them, and to make younger and less experienced those who replaced them."[30]

The goal was attrition. According to Lieutenant General Bennett Sacolick "We intended to conduct raids at a rate that they could not withstand. Through those raids we sought to disrupt, degrade, and dismantle their networks faster than they could re-establish them. Eventually, we concluded, that led to the decline in the capacity of their networks."[31] The results were demonstrable, and "we could see our impact on particular parts of their networks during a given period," explained Admiral McRaven, once TF–714 reached the 300 missions a month tempo.[32]

> *We measured cycles in different operational elements such as bomb making facilities and financing elements. We might seriously degrade a bomb making unit and we could measure its decline in productivity. The same was true for other parts of their operating system. We could also see when a unit was able to re-establish itself, and how long it would take to do so. Then we would begin hitting it extensively again, driving down its capacity.*[33]

From 2006–09 the Task Force maintained an operational tempo of 300 raids a month against AQI's networks in Iraq. During 2008, McRaven continued

> *What we saw in the intelligence being collected during our raids, and from the interrogations of the many members of AQI that we captured on those raids, was that a major decline was taking place in the capacity of different parts of their networks to carry out operations. Our kill/capture raids were considerably driving down their operational capacity. We were able to gauge and evaluate that decline.*[34]

In fact, General McChrystal added, as early as the end of 2006, the commanders of TF–714's raiding teams began sensing the impact of their operations. They told him that AQI was "cracking, it was not at the same level of proficiency and its effectiveness was lessening. We can see it." He noted this was "counter-intuitive because at that time violence was escalating."[35] But those at the operational level saw a weakening. "What they saw and what we heard from many of those who were captured and interrogated was that AQI could not control territory as they had earlier. And that the TF–714 teams were able to attack them in those areas and beat them up badly."[36]

By the late spring of 2007, those same commanders were coming to the conclusion that AQI was in demonstrable decline.[37] One year later, Task Force Deputy Commander, Lieutenant General Eric Fiel believed the indicators were even stronger, signifying that "AQI had been seriously degraded."[38] Those indicators included "What AQI was saying about their situation in their own messaging and communications," which TF–714 was collecting through its extensive signals intelligence capacity. This

reinforced what "we were learning from detainee interrogations about the impact of our targeting."[39]

"Capturing or killing AQI's mid-level managers and commanders was," according to TF–714's leadership, the most important target because they "made the organization function."[40] But "estimating with precision the degree to which the task force was able to degrade those mid-level operational commanders and managers was difficult." This was because there was no "finite target set we could know about," observed McChrystal. That said, TF–714 did "keep a running total of the Emirs, commanders, and managers that were taken off the battlefield. And there was real attrition."[41]

During the 2006–09 timeframe, the count grew considerably as the Task Force was gaining extensive knowledge about various parts of the networks. This included an understanding of who the commanders and managers of various sub-network components were. Admiral McRaven observed that as this period progressed, "we were able to map out different parts of their networks, what they were involved in, who was involved, how they were linked together. With that knowledge, we were able, through raid after raid, to shatter it."[42]

The research underlying this article indicated a strong consensus that by the end of 2009 AQI had been seriously degraded by task force operations, and this was reflected in the decline in its ability to function and carry out missions. Lieutenant General Sacolick, in asserting this was the case, employed the "continuum of effects" framework—disrupt, degrade, dismantle, and defeat. By 2009, TF–714 had disrupted AQI's clandestine apparatus, operational timetable, and freedom of movement, putting the group on the defensive. It also degraded the group's ability to conduct larger operations and a large number of AQI's operational cells, financial units, communications and media centers, bomb and IED production facilities, and arms acquisition networks. Finally, TF–714 dismantled networks to the degree that they could no longer function in the cohesive manner they once had.[43] The task force had developed the capacity to operate inside those networks to break up a considerable number of them.

However, when it came to winning, Lieutenant General Sacolick proposed that in today's irregular wars, a final defeat of the insurgent underground networks is illusive, because the remaining elements of such organizations, once they have been seriously disrupted and degraded, can go into a semi-dormant stage, regroup, and then phoenix-like reappear. Consequently, once AQI was largely degraded, it had to be kept at that stage, while the political reconciliation and reconstruction phases that follow a successful COIN/CT program have time to be established and take root.[44]

General McChrystal added that: "Winning is relative in these kinds of wars. There is no VE Day. We put AQI on its back, having badly beaten it up. But until the political causes of the conflict are addressed, it could reemerge." Consequently, during this post-conflict period which can go on for an extended period of time because political reconciliation and reconstruction do not happen overnight, AQI "had to be kept on its back."[45]

In effect, after three years of industrial-strength CT, Task Force–714 had reached what General Raymond Odierno, then Commander Multi-National Force–Iraq, referred to as the "irreducible minimum." By this, he meant that even when a COIN/CT program is able to greatly weaken a group like AQI, they will still retain a capacity to carry out periodic attacks.[46] At the operational level this is winning. During 2009, the Task Force was "only carrying out two to three raids a night because AQI's operational tempo was way down. And we were beginning to hand those missions off to our Iraqi CT force counterparts."[47] In 2010, those missions contributed to the killing or capturing of 26 insurgent leaders.[48]

That said, the conclusion of those who led TF–714 was that an effective COIN and CT program

can take you only so far. They are necessary parts of the resolution of such wars, but they are never sufficient in and of themselves. This critical conclusion was stressed by the leadership of TF–714. What COIN and CT can achieve is to establish the prerequisites for post–conflict transition, political reconciliation, and reconstruction. For the COIN forces, the goal was to sweep the insurgents from the cities and towns in Iraq and then to hold that ground after it was cleared. In Iraq, the Awakening Movement was an important facilitator for holding ground once the insurgents were cleared. For TF–714 the mission was to disrupt, degrade, and dismantle AQI's networked secret underground; to hit AQI's networks every night, killing or capturing a large number of its mid-level managers and operational commanders, and undermining its operational tempo.

Once territory was held and the insurgent networks degraded to their irreducible minimum, the conditions were set to begin post-conflict transition, political reconciliation, and reconstruction. In Iraq, transition began in August 2010 and culminated in December 2011, with the completion of the U.S. withdrawal of its forces in accord with the 2008 "Agreement between the United States of America and the Republic of Iraq on the Withdrawal of the United States." While withdrawing, the United States would continue to train Iraqi security forces to enhance their capacity and professionalism. Beginning in 2012, there was a generally held assumption that a follow-on U.S. force would stay in Iraq to continue security capacity building, while other interagency elements facilitated post-conflict political reconciliation and reconstruction. A follow-on version of TF–714 would help its Iraqi counterparts maintaining the irreducible minimum to ensure that AQI did not have an opportunity to reconstitute itself and return to the offensive.

Operation *Iraqi Freedom* Transition to Operation New Dawn

In August 2010, the last Brigade Combat Team withdrew from Iraq, and on the 31st of that month, President Obama declared the end to "the American combat mission." Those U.S. forces remaining were to transition to non-combat stability activities as part of Operation *New Dawn* (OND). The remaining 50,000 troops would concentrate on training and advising the Iraqi Security Force (ISF) to improve its capacity to maintain the stability established in Iraq during OIF, while simultaneously withdrawing. To manage the transition, General Lloyd Austin assumed command of United States Forces–Iraq and Ambassador James Jeffery became ambassador.

Operation *New Dawn* had three principal objectives. First, to continue to advise, train, and equip ISF to become capable of maintaining internal stability and security. Second, to assist Iraq's Defense Ministry and other security institutions develop the capacity to oversee and manage operating forces. Each of these activities fit within the non-combat stability mandate of OND. But the third component called for a continuation of TF-714's warfighting operations, carried out in conjunction with its counterpart, the Iraq Special

Airmen prepare to take-off on a C–17 at Ali Air Base, Iraq, signaling the end of Operation *New Dawn* on December 18, 2011. The airmen were part of the last troops to leave Iraq. (U.S. Air Force/Cecilio Ricardo)

Operations Force (ISOF). They were to persistently attack and degrade AQI, keeping it "on its back," preventing any resurgence.[49] During 2010, TF–714 did so very effectively. Nevertheless, despite heavy losses, AQI still managed to maintain a small number of surviving network elements and competent commanders and managers.

Even as OND was being implemented, there was a view among senior U.S. military commanders that Iraq's security forces faced considerable challenges in reaching the point where they could stand on their own. And it would take substantial time to overcome those challenges. Consequently, in Baghdad and Washington senior officers assessed the need for a U.S. military presence after OND ended. In early 2011, General Austin, Chairman of the Joint Chiefs of Staff Admiral Michael Mullen, and Commander of U.S. Central Command General James Mattis concluded that a U.S. force of 20–24,000 would be needed.[50] This was the best military advice of the senior military leadership.

Referred to as the Residual Force, they saw it as essential if Iraqi stability was to be maintained, ISF professionalization continued, and the longer process of post-conflict political reconciliation and reconstruction undertaken. Settling on the size of the Residual Force was the first step in developing an interagency plan for how the U.S. could help facilitate reconciliation and reconstruction. But developing that plan never received attention as the size of the Residual Force became a highly contentious political issue for the Obama administration.

The Austin–Mullen–Mattis number caused "sticker shock" at the White House. As a result, a Principals Committee meeting at the end of April 2011 chaired by National Security Advisor Thomas Donilon sought to outflank the generals, setting a 10,000 ceiling. When Admiral Mullen learned of the maneuver he "prepared a confidential memo to Donilon outlining his position and that of the collective military leadership." The Chairman reduced the number to "16,000 troops." The memo was seen as an attempt to "box the White House in."[51] The result was no Administration decision on the size of the Residual Force at that time, and that indecision continued into the summer months of 2011.[52]

The size of the force was not the only issue that had to be addressed. The White House also stipulated that any force remaining in Iraq after 2011 required a Status of Forces Agreement (SOFA) between Washington and Baghdad that would provide the same immunities for U.S. forces as had been agreed to in the 2008 SOFA. For the Obama Administration a new SOFA authorized by executive agreement would not do. It had to be approved by the Iraqi parliament. Such an agreement was never reached.[53]

Also impeding a decision on the Residual Force was the political turmoil in Iraq, as Prime Minister Nuri al-Maliki had been maneuvering for months to have himself re-appointed following his loss of the March 2010 election. Even though Maliki's party had come in second in the elections to the Iraqiya Party of Ayad Allawi, it was clear to some he had no intention of "stepping down" so Allawi could try to form a government.

In November, Maliki brokered a power-sharing agreement with Allawi and Iraq's two Kurdish vice presidents and resumed the position of Prime Minister. He would use that reappointment in 2011 to consolidate power at the expense of those with whom he had agreed to share power.[54] During that period of political intrigue, Maliki was unwilling to take the risk of making a formal request for a Residual Force to stay in Iraq after 2011. As this dragged on into the summer, the White House started revising the size of the Residual Force downward, while continuing to insist on a SOFA approved by the parliament. In mid-August, the proposed size reached a low of 1,600.[55] This made any accord impossible. Agreeing to a Residual Force

was a contentious political issue in Iraq, and not a risk Maliki was about to take for this level of continuing U.S. support. As a result, President Obama on October 21 informed him that the United States would reduce its forces to zero by the end of 2011, terminating the U.S. military presence.

The Consequences of Withdrawal

During 2011, as the likelihood of a Residual Force faded, Prime Minister Maliki moved to consolidate control of the Iraqi Security Forces by accelerating the removal of senior Sunni officers that he feared could be disloyal to him—a cleanse that began in 2009 with Maliki's removal of Sunni commanders that he believed to be secret supporters of the former Ba'athist regime—and their replacement with loyal Shia officers.[56] The same thing was taking place in the police force. Cleansing accelerated into 2012, as the Prime Minister unremittingly placed his loyalists in senior command posts.

The result of this cronyism was politicization and corruption of the ISF officer corps. The non-sectarian professional army leadership that the United States worked hard to foster, with an officer's corps comprised of competent Shia, Sunni, and Kurds, disappeared. Maliki loyalists were rewarded with high-ranking appointments in combat and intelligence units to ensure that the military posed no internal threat to him. Rather, it could be used by him against all he perceived as political rivals.

Maliki was able to consolidate civilian control of the security institutions, turning them into a sectarian tool he could use for political purposes. He consolidated control over the army and other security institutions through the "Office of the Commander in Chief, which he used to bypass other state institutions theoretically involved in civil-military relations." That office "became the de facto executive body for the whole security sector," and Maliki used it to "established control over the [entire] security sector." This included "controlling appointments to all senior positions in the ISF to create a network of officers loyal to him."[57] Of course, this ran counter to what the United States had sought to achieve—a professionalized Iraqi army in which officers were promoted based on merit.

Maliki's control of the security institutions included the ISOF that had become a highly capable partner of TF–714. But during the transition period, Maliki began to increase his use of those units against political enemies. As politicization and sectarianism crept into ISOF, partnered operations with TF–714 suffered. As it became clear there would be no Residual Force, TF–714 began decamping from its base in Balad and operations ended.

During 2011, Maliki also moved against the Sons of Iraq, the Sunni tribesmen who first emerged in Anbar Province in 2005 and then became the foot soldiers of the Awakening Movement.[58] Their number had risen to more than 90,000 members and the Awakening Movement was credited with having helped reduce the violence first in Anbar and then in the other areas in which they operated during the Surge. The government had planned to reward the Sons of Iraq with jobs in different security institutions when stability was achieved in 2008, but less than 10,000 received assignments. This created a critical mass of unemployed fighters who had been disenfranchised by the government that they had help to survive.

In sum, in 2011 as the U.S. moved down the path to zero, the Maliki government employed the security institutions, which he controlled, to consolidate power. But in doing so, the gains the Iraqi military and police forces had made, thanks to the tens of billions invested by the U.S. to train and equip them, began rapidly reversing. Serious questions began to emerge about the capacity of the Ministry of Defense and Ministry of Interior forces to execute the full range of their duties. Instead, they were devolving into "Maliki's private militia."[59]

AQI Redux and the Origins of Islamic State

By 2009 three years of industrial-strength CT operations by TF–714 had greatly weakened AQI. Then in 2010, 26 of its leaders were either killed or captured. These included Abu Ayyub al-Masri and Abu Abdullah al-Raschid al-Baghdadi, AQI's top leaders. The organization appeared to be at the end of the line, on life support. But the developments chronicled above that took place during Operation New Dawn provided its surviving elements with an opportunity to revive the organization.

First, AQI's Shura Council selected a new leader or emir, Abu Bakr al-Baghdadi. A new operations chief likewise emerged in Hajii Bakr, a former Ba´athist officer, as well as a new war minister, Nu'man Salman Mansur al-Zaydi. This new leadership began calling AQI the Islamic State of Iraq (ISI). To build up the rank and file of the new organization, ISI initiated an "intensive recruitment campaign" directed, in part, at members of the Sons of Iraq who were being "dismissed from their positions in significant numbers" by the Maliki government.[60]

According to an October 2010 account, while "there are no firm figures, security and political officials say hundreds of the well-disciplined fighters—many of whom have gained extensive knowledge about the American military—appear to have joined." Moreover, there may be many other "Awakening fighters still on the Iraqi government payroll . . . covertly aiding the insurgency."[61] According to a former Awakening leader, Nathum al-Jubouri, Sons of Iraq "members have two options: Stay with the government, which would be a threat to their lives, or help al-Qaeda by being a double agent." Many are choosing the latter option, he added, providing a "database for al-Qaeda that can be used to target places that had been out of reach before."[62]

With the death of Osama bin Laden in May 2011, the Obama Administration judged al-Qaeda to be nearing defeat. But that was not the case in Iraq. ISI's ranks swelled in 2011–12, as did their attacks on police and military facilities and checkpoints. Facilitating these developments were the sectarian policies of the Maliki government and the drawdown of U.S. forces, in particular TF–714 and other special operations and intelligence capabilities.

During 2011–12 high casualty terrorist operations burgeoned as ISI launched several suicide car bomb attacks in Baghdad and other major cities. Illustrative of this escalation was the ISI suicide bomber attack on the Umm al-Qura Mosque in Baghdad on August 28, 2011. The terrorist set off the IED inside the mosque, killing 32 and wounding many more.[63] And while the most spectacular, there were a total of "42 apparently coordinated attacks [that] underscored the reality that few places in Iraq are safe."[64]

These operations were the beginning of a resurgence that would culminate in ISI taking control of significant territory in Northern Iraq from 2012–14. And, as a result, Baghdadi promoted himself to Caliph Ibrahim and declared the creation of the Islamic Caliphate on this territory. ISI then became the Islamic State of Iraq and the Levant (ISIL) and seized control of much of Iraq's second largest city, Mosul, and its surrounding province. In six days of fighting, ISIL routed 30,000 ISF soldiers and 30,000 federal police.

Who Lost Iraq?

In the wake of these developments a narrative gained considerable traction that "George W. Bush's 'surge' of American troops in Iraq achieved victory, before Obama fecklessly withdrew U.S. soldiers, transforming success into failure and triggering the rise of ISIS."[65] For critics of the Obama Administration, this outcome was clear. They "blame President Obama's administration for losing [Iraq]," asserting that the administration's failure "to renegotiate a status of forces agreement that would have allowed

some American combat troops to remain in Iraq and secure the hard-fought gains the American soldier had won by 2009" gave AQI the opportunity to reconstitute itself first as ISI and then ISIL.[66]

In effect, President Obama is charged with having snatched defeat from the jaws of victory. Upon entering office, "he inherited a pacified Iraq, where the terrorists had been defeated both militarily and ideologically. Militarily, thanks to Bush's surge, coupled with the Sunni Awakening, al-Qaeda in Iraq was driven from the strongholds it had established in Anbar and other Iraqi provinces. It controlled no major territory, and its top leader—Abu Musab al-Zarqawi—had been killed by U.S. Special Operations Forces. Ideologically, the terrorists had suffered a popular rejection." All of this was squandered by Obama with his decision at the end of 2011 to "withdraw all U.S. forces from Iraq; taking our boot off of the terrorists' neck; allowing them to regroup."[67] The bottom line, according to General Jack Keene: "Bush won the war. Obama lost the peace."[68]

To be sure, there is a kernel of truth in this assessment but there also is considerable overstatement of what had been achieved "on the ground" and where Iraq stood at the end of 2011. Critics of this interpretation of the consequences of the 2011 withdrawal counter that there was no victory in Iraq to squander—U.S. military power had gone as far as it could. Ultimately, it was up to the Iraqis to consolidate those 2006–09 gains. What the Surge and its aftermath achieved, according to supporters of President Obama's policy, was to give the Iraqis an opportunity. But Maliki and the Iraqi leadership had to "seize the moment."[69]

There likewise is a kernel of truth here as well, but also a downplaying of what a Residual Force could have contributed in helping Iraq consolidate the gains made by COIN and CT operations from 2006–09. Those operations had markedly improved the security conditions in Iraq. The Surge and COIN strategy allowed American forces and their Iraqi partners to gain control of Baghdad, Diyala, and other major urban areas where AQI had ensconced itself. And TF–714 had reduced AQI's networks considerably by 2009, keeping them through 2010 at what General Odierno described as the "irreducible minimum."[70]

In an irregular war, there is no decisive battle that culminates in victory for one side over the other. As Rupert Smith writes in *The Utility of Force: The Art of War in the Modern World*: "In contrast to these hard, strategic ends we tend now to conduct operations for 'softer,' more malleable, complex, sub-strategic objectives." Military force is employed "to establish a condition in which the political objective can be achieved by other means in other ways . . . Overall, therefore, if a decisive strategic victory was the hallmark of [traditional] interstate industrial war," for irregular warfare, "establishing a *condition* may be deemed the hallmark of the new paradigm of war."[71] What that means is establishing security and stability which *sets the conditions* in which post–conflict reconciliation can take place.

That condition was reached by the end of 2009. Operation *New Dawn* sought to maintain and enhance it by continuing to advise, train, and equip ISF, as well as other security forces, to become capable of maintaining internal stability and security. At the same time, TF–714 continued to attack and degrade AQI, preventing its resurgence. But what was missing in OND, and what should have been a key part of an interagency-based Residual Force going forward in 2012, was a capacity to foster political mediation and reconciliation in Iraq. It is the key component for settling irregular wars like that which took place in Iraq.

Political reconciliation, within the context of irregular war, is a process designed to foster intergroup understanding, coexistence, and conflict resolution. Political reconciliation seeks to establish

accommodation and to normalize relations among elements of a society that have been in violent conflict with one another. In Iraq, this necessitated an agreement on power sharing among the three major identity groups. To achieve this, an overarching political framework had to be established for negotiating these arrangements at the national level. For that reconciliation to take place, third party mediators have a critical role to play. But as several accounts have reported, post-conflict reconciliation was not facilitated through the formation of a long-term strategic partnership between Washington and Baghdad as part of a post–Operation *New Dawn* Residual Force. The Obama Administration had an important role to play in mediating that political reconciliation process. By not doing so and withdrawing, the security gains that had been achieved through operational level success from 2006–09 by the United States quickly dissipated. PRISM

Notes

[1] This data, which was compiled weekly by the Department of Defense from January 2004 to April 2009 is contained in article by CSIS expert Anthony Cordesman on "The Uncertain Security Situation in Iraq: Trends in Violence, Casualties, and Iraqi Perceptions," (Washington, DC: Center for Strategic and International Studies, 2010), available at < https://www.csis.org/analysis/uncertain-security-situation-iraq>.

[2] William B. Ostlund, "Irregular Warfare: Counterterrorism Forces in Support of Counterinsurgency Operations," *The Land Warfare Papers*, No. 51 (September 2012).

[3] David Tucker and Chris Lamb, United States Special Operations Forces (New York: Columbia University Press, 2007); Linda Robinson, *Masters of Chaos: The Secret History of the Special Forces* (New York: Public Affairs, 2004); Susan L. Marquis, Unconventional Warfare: Re-building U.S. Special Operations Forces (Washington, DC: Brookings Institution Press, 1997); and Thomas Adams, *US Special Operations Forces in Action: The Challenge of Unconventional Warfare* (London: Routledge Press, 1998). For a discussion of the theory underlying such forces, see chapter one of William McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice* (New York: Presidio Press, 1995).

[4] Stanley McChrystal, *My Share of the Task*, (New York: Penguin Books, 2014), 101. The Pentagon had printed packs of playing cards with the grainy photographs and names of the top Ba´athists. During the summer of 2003, TF 714 tracked down the Iraqi dictator's two sons, Uday and Qusay. Then on December 13, in the town of ad-Dawr, near Tikrit, they captured Saddam himself.

[5] Interview with Lieutenant General Michael Flynn, U.S. Army retired, Alexandria, VA, October 2014.

[6] Interview with General Stanley McChrystal, U.S. Army retired, Alexandria, VA, July 2014.

[7] Ibid.

[8] Interview with Admiral William McRaven, U.S. Navy retired, Washington, DC, September 2014.

[9] Ibid.

[10] Interview with General Stanley McChrystal.

[11] Stanley McChrystal, *My Share of the Task*, 92.

[12] "A Conversation with Stanley McChrystal," *Foreign Affairs* (March/April 2013).

[13] Adam Grissom, "The Future of Military Innovation Studies," *The Journal of Strategic Studies* (October 2006); John Nagl, *Learning to Eat Soup with a Knife* (Chicago: University of Chicago Press, 2002); Richard Downie, *Learning From Conflict: The U.S. Military in Vietnam, El Salvador, and the Drug War* (Westport, CT: Praeger, 1998); Kimberly Zisk, *Engaging the Enemy: Organization Theory and Soviet Military Innovation 1955-1991* (Princeton: Princeton University Press, 1993); Michael McNerney, "Military Innovation During War: Paradox or Paradigm," *Defense & Security Analysis* (June, 2005); Theo Farrell, "Figuring Out Fighting Organizations: New Organizational Analysis in Strategic Studies," *The Journal of Strategic Studies* (March 1996).

[14] Creating and sustaining such an organizational approach to problem solving, explain Spender and Grinyer, should be a responsibility "shared by top management and employees." They do so by nurturing a "dialectic between the organization as a whole and its parts." J.C. Spender and P.H. Grinyer, "Organizational Renewal: Top Management's Role in a Loosely Coupled System," *Human Relations*, no. 8 (1995), 913. Also see Nirmal Pal and Daniel Pantaleo, *The Agile Enterprise: Reinventing your Organization for Success in an On-demand World* (New York: Springer, 2005) and Emmanuel Gobillot, *The Connected Leader: Creating Agile Organizations for People, Performance and Profit* (London: Kogan, 2008).

[15] The details of how Task Force–714 carried out this organizational transformation and recreated itself during the Iraq war is beyond the scope of this article. Those developments have been described and analyzed

in considerable detail in Military Innovation in War: It Takes a Learning Organization.

[16] *Measuring Stability and Security in Iraq. Report to Congress in Accordance with the Department of Defense Supplemental Appropriations Act 2008 (Section 9204, Public Law 110-252)* Washington, DC, Department of Defense, June 2010, available at <http://www.defense.gov/pubs/pdfs/June_9204>.

[17] Consider the December 2006 report of the Iraq Study Group, co-chaired by former Secretary of State James Baker and former Indiana Congressman Lee Hamilton. The report painted a grim picture: "The challenges in Iraq are complex,"…"Violence is increasing in scope and lethality … If the situation continues to deteriorate, the consequences could be severe." The Report made 79 recommendations, but the key issue was security and the role of U.S. forces. With respect to that it asserted: "There is no action the American military can take that, by itself, can bring about success in Iraq." See James Baker, Lee Hamilton, and Lawrence S. Eagleburger, The Iraq Study Group Report: The Way Forward—A New Approach (New York: Vintage Books, 2006), 7, 48, and 51.

[18] *Measuring Stability and Security in Iraq*, 27.

[19] Frank Hoffman and Alexander Crowther, "The Surge in Iraq and Afghanistan," in Richard Hooker and Joseph Collins, ed., *Lessons Encountered: Learning from the Long War* (Washington, DC: National Defense University Press, 2015), 124–25.

[20] The most recent Iraq Index is available at <www.brookings.edu/iraq-index/ >

[21] Richard Shultz, *The Marines Take Anbar: The Four-Year Fight Against Al Qaeda* (Annapolis: Naval Institute Press, 2012), chapter 5.

[22] See for example Thomas Ricks, "Situation Called Dire in West Iraq," *Washington Post* (September 11, 2006).

[23] Shultz, *The Marines Take Anbar: The Four-Year Fight Against Al Qaeda*, see chapter 5.

[24] Ibid., see chapter 6.

[25] Ibid., 232.

[26] Stephen Biddle, Jeffrey A. Friedman, and Jacob N. Shapiro, "Testing the Surge: Why Did Violence Decline in Iraq in 2007," *International Security* (Summer 2012), 37.

[27] For assessments of the Surge see Kimberly Kim Kagan, *The Surge: A Military History* (New York: Encounter Books, 2009); Michael Gordon and Bernard Trainor, *The Endgame: The Inside Story of the Struggle for Iraq, from George W. Bush to Barack Obama* (New York: Vintage, 2013); and Peter Mansoor, *Surge: My Journey with General David Petraeus and the Remaking of the Iraq War* (New Haven, CT: Yale University Press, 2013).

[28] David Galula, *Counterinsurgency Warfare: Theory and Practice* (Westport, CT: Praeger Security International, 1964); Sir Robert Thompson, *Defeating Communist Insurgency: The Lessons of Malaya and Vietnam* (New York: Frederick Praeger, 1966); Richard Clutterbuck, *The Long Long War: Counterinsurgency in Malaya and Vietnam* (New York: Frederick A. Praeger, 1966); Frank Kitson, *Low Intensity Operations: Subversion, Insurgency and Peacekeeping* (Harrisburg, PA: Stackpole Books, 1971); John McCuen, *The Art of Counter-Revolutionary War* (Harrisburg, PA: Stackpole Press, 1966); and Sarah Sewall et al., *The U.S. Army/Marine Corps Counterinsurgency FM* (Chicago: University of Chicago Press, 2007).

[29] Follow-up interview with General Stanley McChrystal, U.S. Army retired, Alexandria, VA, May 2015.

[30] Ibid.

[31] Follow-up interview with General Bennet Sacolick, U.S. Army, McLean, VA, June 2015.

[32] Follow-up interview with Admiral William McRaven, U.S. Navy retired, June 2015.

[33] Ibid.

[34] Ibid.

[35] Follow-up interview with General Stanley McChrystal.

[36] Ibid.

[37] Ibid.

[38] Interview with General Joseph Votel, U.S. Army, Tampa, FL, May 2015.

[39] Ibid.

[40] Interview with Lieutenant General Fiel, U.S. Air Force retired, Tampa, FL, May 2015.

[41] Follow-up interview with General Stanley McChrystal.

[42] Follow-up interview with Admiral William McRaven.

[43] Follow-up interview with General Bennet Sacolick.

[44] Ibid.

[45] Follow-up interview with General Stanley McChrystal.

[46] Cited in David Strachan-Morris, "The Irreducible Minimum: Al Qaeda in Iraq and the Effectiveness of Leadership Decapitation," *RUSI Journal* (August/September 2010), 32–36.

[47] Follow-up interview with Admiral William McRaven.

[48] Strachan-Morris, "The Irreducible Minimum…,"32. These included Abu Ayyub al-Masri, AQI's overall leader, and Abu Abdullah al-Raschid al-Baghdadi, the head of the Islamic State of Iraq.

[49] For an elaboration of these three objectives see Richard R. Brennan, Jr., et. al, Ending the U.S. War in Iraq (Santa Monica, CA: RAND Corporation, 2013),

chapter 4.

[50] Gordon and Trainor, *The Endgame: The Inside Story of the Struggle for Iraq, from George W. Bush to Barack Obama*, 657.

[51] Ibid, 658–59.

[52] Robert Gates, *Duty: The Memoirs of a Secretary at War* (New York: Vintage Books, 2014), 554–55.

[53] Gordon and Trainor, *The Endgame: The Inside Story of the Struggle for Iraq, from George W. Bush to Barack Obama*, 666.

[54] Gordon and Trainor, *The Endgame: The Inside Story of the Struggle for Iraq, from George W. Bush to Barack Obama*, chapter 34.

[55] Brennan, Jr., et. al, Ending the U.S. War in Iraq, 103.

[56] Kenneth Pollack, *Iraq Military Situation Report* (Washington, DC: Brookings Institution, 2014)., available at< https://www.brookings.edu/blog/up-front/2014/06/14/iraq-military-situation-report/>.

[57] Florence, "An Unhappy Marriage: Civil-Military Relations in Post-Saddam Iraq," *Carnegie Middle East Center* (January 2016), available at <http://carnegie-mec.org/2016/01/13/unhappy-marriage-civil-military-relations-in-post-saddam-iraq-pub-61955>.

[58] Lelia Fadel, "Iraq's Awakening Stripped of Their Police Ranks," *New York Times* (October 2, 2010).

[59] T.X. Hammes, "Raising and Mentoring Security Forces in Afghanistan and Iraq," in Hooker and Collins, ed., *Lessons Encountered: Learning from the Long War*, 311.

[60] Timothy Williams and Duraid Adnan, "Sunnis in Iraq Allied With U.S. Rejoin Rebels," *New York Times* (October 16, 2010), available at <http://www.nytimes.com/2010/10/17/world/middleeast/17awakening.html?mcubz=0>.

[61] Ibid.

[62] Ibid.

[63] BBC, "Baghdad Mosque Attack," (August 28, 2011), available at <http://www.bbc.com/news/world-middle-east-14704484>.

[64] Michael Schmitt, "Threat Resurges in Deadliest Day of Year for Iraq," *New York Times* (August 15, 2011), available at <http://www.nytimes.com/2011/08/16/world/middleeast/16iraq.html?mcubz=0>.

[65] Dominic Tierney, "Who Really Lost Iraq? Obama Didn't Turn Victory into Defeat. There Was No Victory," *The Atlantic* (January 21, 2016).

[66] James Traub, "The Mess Obama Left Behind in Iraq," *Foreign Policy* (October 7, 2016), available at <http://foreignpolicy.com/2016/10/07/the-mess-obama-left-behind-in-iraq-surge-debate/>.

[67] Marc Thiessen, "Obama's Retreat from War Made Matters Worse," *Newsweek* (May 21, 2016), available at <http://www.newsweek.com/obama-retreat-war-made-matters-worse-461598>.

[68] Ibid.

[69] Michael Crowley, "Who Lost Iraq? Did George W. Bush Create the Islamic State? Did Barack Obama? We Asked the Insiders to Tell Us Who is to Blame," *POLITICO Magazine* (July/August 2015), available at <http://www.politico.com/magazine/story/2015/06/iraq-roundtable-george-w-bush-barack-obama-119221>.

[70] Although not discussed above, it is also important to note that the Shia militias, which had posed a serious security threat to the Iraqi government, had likewise been considerably degraded in 2008.

[71] Rupert Smith, *The Utility of Force: The Art of war in the Modern Age* (New York: Vintage Books, 2007), 272–73.

The Chinese People's Liberation Army Navy is establishing a network of enhanced reefs enabling China to exert control over the South China Sea. (SatelliteImage©2018DigitalGlobe)

Perils of the Gray Zone
Paradigms Lost, Paradoxes Regained

By John Arquilla

In the long years since the 9/11 attacks on America, the wide-ranging "war on terror" has morphed into terror's war on the world. Terrorist incidents have increased seven-fold, with the casualties caused by such attacks more than quintupling.[1] Just as troubling, since the start of the current decade the overall number of wars under way has increased nearly a third—from 31 to 41.[2] There is much overlap between the worst of these conflicts and the number of terrorist incidents, with Iraq, Afghanistan, Syria, and Yemen heading the list in recent years. Paradoxically, the first two of the countries listed have seen extended, very expensive, yet problematic American invasions and occupations. The American military footprint has been light in Syria and Yemen, but these wars have also proved vexing.

If these challenges were not enough, plaguing the lower end of the spectrum of conflict as they do, there are serious threats at the levels of the mid-range and major powers as well. Roguish regional states like Iran and North Korea each pose grave problems. The Islamist regime in Tehran oversees an arc of strategic involvement in wars ranging from Syria to the southern Arabian Peninsula; supports the vibrant, violent Hezbollah organization; and cultivates covert nodes, cells, and networks throughout the world.[3] As for North Korea, Kim Jong Un's vision is focused primarily on continuing his family's totalitarian dynasty. But a key aspect of his strategy includes the development of a robust nuclear deterrent, something seen as highly threatening in capitals ranging from Washington to Beijing.

Mention of Beijing is a reminder of the rise of China, and of its increasingly bumptious policies and actions—from reef enhancement to edgy sea patrols—in the East and South China Seas. The cyber domain is yet another area in which China's behavior can only be described as highly aggressive, given the skill and systematic predations of its corps of hackers—whether they are part of Chinese officialdom or somehow just working at the behest of Beijing. Their ability to make off with vast amounts of intellectual property has resulted in their enjoying a greatly disproportionate share of what then Director, National Security Agency and Commander, U.S. Cyber Command General Keith Alexander called—while he was still in uniform—"the greatest transfer of wealth in history."[4] Needless to say, Russian and/or Russian-backed hackers have enjoyed a healthy share of these spoils as well.

Dr. John Arquilla is Professor and Chair, Department of Defense Analysis at the Naval Postgraduate School.

However, the Russian challenge goes well beyond cybercrime, to include serious acts of political warfare—specifically, of late, attempts to influence democratic elections—across many countries, not least the United States. The Russians have also reasserted their growing power in more muscular though hardly conventional ways as well. Not only in their self-defined "near abroad"—reference should be made here to the bloodless annexation of Crimea and covert combat support to separatist rebels in Donetsk—but also in Moscow's sharp military intervention in the bloody Syrian civil war. Thus, if we are not seeing a recrudescence of the Cold War, without doubt a kind of "cool war" has indeed set in.[5]

Given all the global turmoil, and the seeming inability of American power—even when enhanced by allies—to cope effectively with the wide range of these challenges, it is small wonder that strategists have been casting about in search of fresh paradigms and more innovative concepts of operations. For it is abundantly clear that "overwhelming force"—the foundation of the grand strategic doctrine that bears General Colin Powell's name—will not suffice against hidden networks, or nations that choose covert, unconventional action as their preferred modus operandi.

In an era featuring few stand-up fights, there is a premium on doctrinal innovation. Yet even while the various aggressors of the world seem to have truly grasped the need for and mastered the process of creativity, the United States and its allies have become mired in older habits of mind, manifesting an all-but-nostalgic longing for the return of traditional conventional warfare. The American defense budget is quite revealing of this mindset, with more than 90 percent of expenditures aimed at shoring up or expanding on conventional combat capabilities. Even the most generous views of support for U.S.

Rehearsal of the parade in honor of Victory Day in Donetsk.

Special Operations Command (USSOCOM), for example—including direct and "enabling" funding—have historically reflected little more than 3 percent of the overall budget allocated to it, along with but 4 percent of monies dedicated to overseas contingency operations.[6] In terms of personnel, USSOCOM's estimated 70,000 service members constitute just 5 percent of the total active duty force.

However, there have been voices raised in recent years, pointing to the costly, problematic interventions in Afghanistan and Iraq, the rise in global terrorist networks, and the evidence that mid-level and major powers are flexing their muscles in a mostly unconventional manner—hardly ever distinguishable as familiar traditional warfare. The effort to categorize this challenge has coalesced around a notion of gray zone conflict, a concept defined by strategist Hal Brands as an "activity that is coercive and aggressive in nature, but that is deliberately designed to remain below the threshold of conventional military conflict."[7] A recent report by the International Security Advisory Board—a Federal Advisory Committee established to provide the Department of State independent insight, advice, and innovation—describes the gray zone more narrowly as

> *the use of techniques to achieve a nation's goals and frustrate those of its rivals by employing instruments of power—often asymmetric and ambiguous in character—that are not direct use of acknowledged regular military forces.*[8]

Whatever the differences in definition between these views—and those arising from myriad other gray zone studies—the emphasis on this zone being unconventional comes through loud and clear.

This prompts two questions: "why do we need the gray zone concept?" and "has the focus on today's so-called gray zone resulted in a dangerous diversion of attention away from the accumulated body of knowledge about unconventional aspects of conflict developed over the past two hundred years?" The problems posed by irregular warfare in the 19th century, from Carl von Clausewitz's notions of *kleiner Krieg* in the Napoleonic era to C.E. Callwell's "small wars" during the heyday of colonialism, were deeply studied by these two, and many others.[9] As to the anti-colonial guerrilla wars of the 20th century, these were closely examined by insurgents and counterinsurgents alike. Mao Zedong, Che Guevara, and Vo Nguyen Giap were undoubtedly the best guerrilla memoirists, respectively, of Chinese, Cuban, and Vietnamese insurgent movements. The counterinsurgent perspective on the past century has perhaps been best exposited in remarkable works by David Galula, Otto Heilbrunn, and Lewis Gann.[10] These are but a few of the highest peaks in a whole mountain range of studies of irregular warfare. In light of this existing literature, why is the gray zone concept needed?

As to the second question, about diversion of attention away from accumulated knowledge of the subject of conflict "other than traditional conventional warfare," it seems that here too there is much cause for concern. Brands puts the matter succinctly, noting that "exaggerating the newness of the [gray zone] phenomenon risks muddling rather than sharpening our comprehension."[11]

Paradigms Lost

Beyond impairing our understanding of the current landscape of conflict, failure to recall and rely upon relevant security paradigms of the past—in favor of simply ginning up a new term for longstanding practices—has led to a sharp loss of earlier knowledge and insight, consequences of which have surely played a significant role in the unsatisfying course of events described in the opening section of this article. It is with deep concern about the severe price paid by forgetting the substance and power of earlier security paradigms—an inattentiveness that plays

right into our enemies' hands—that I provide the following reminders.

Perhaps the most important insight to recall and reflect on speaks to the very rise of an age of irregular warfare. This was predicted by political scientist Kenneth Waltz more than sixty years ago, when he observed that "mutual fear of big weapons may produce, instead of peace, a spate of smaller wars."[12] Journalist Robert Taber affirmed this view a decade later in his classic *War of the Flea*, which foretold the future dominance of insurgency and terror on the conflict spectrum. As Taber viewed the matter, a traditional military simply had "too much to defend, too small, ubiquitous and agile an enemy to come to grips with."[13] This insight resonated with bright jihadis, especially Abu Mus'ab al-Suri, the deepest strategic thinker that al-Qaeda produced. He used Taber's work in his teachings during the 1990s, when al-Qaeda ran a "university of terror" in Afghanistan.[14] Waltz and Taber had hardly been heeded in the United States, and much too conventional means were applied in Vietnam. A predictable debacle ensued, yet American thought still turned back to conventional war with development of an AirLand Battle doctrine after the communist overrun of South Vietnam in 1975. And it would take more than 30 years—after 9/11 and in the middle of the insurgency in Iraq—before a new counterinsurgency manual was published.[15]

With regard to the notion of a blurriness between peace and war—a key aspect of the justification for the gray zone concept—it is hardly new. Forty years ago Eliot Cohen was writing insightfully about "the blurring of war and peace . . . the struggle to mobilize the populace . . ." and a "new era of warfare [differing] sharply from that which preceded it."[16] As to notions of covert action as means by which to effect regime change and pursue other political objectives, this portion of the gray zone was illuminated, studied, and critiqued long ago. Given that the United States was an eager participant in this realm, it is hard to see why a new construct for this form of action is necessary. Indeed, a look back at the heyday of covert action, and its often problematic results—in Iran, Guatemala, Cuba, Chile, Angola, and Nicaragua, to name just a few places where Americans plied this craft—might curb the future appetite for this dark mode of statecraft.[17] Conversely, given the high failure rate of covert actions, excessive fear of others using them might be eased.

In addition to covert action—a phenomenon closely associated with the world of intelligence and counterintelligence—the defined gray zone implicitly relates also to aspects of warfighting that extend well-beyond the aforementioned guerrilla operations. These modes of conflict are generally reflected by instances in which a nation chooses to counter or confront a potential adversary by investing in off-design technologies and highly innovative concepts of operations, rather than by imitating the structure and doctrine of the opposing forces. The best current example of such an approach can be found in Beijing's strategy in the East and South China Seas. Instead of relying on aircraft carriers—though the Chinese People's Liberation Army Navy now has two of them—Beijing is establishing a network of enhanced reefs, one with potential to exert control over these narrow seas with supersonic anti-ship missiles, brilliant mines, and attack aircraft based on or otherwise using them. By these varied means, Beijing is taking a highly asymmetric approach to dealing with American carrier-based power projection capabilities.

This notion of asymmetric warfare, pioneered more than 40 years ago by Andrew J.R. Mack, is one of those well-developed paradigms in danger of being lost as soldiers and statesmen flock to the gray zone. For Mack, the asymmetry was not only to be found in the concept of field operations but also in the combatants' relative motivations. Key studies that have built upon his thinking, and advanced fresh ideas, have addressed both the

operational and the motivational dimensions.[18] In the world today, these factors are much on display at all levels. Clearly, the Taliban see their campaign in Afghanistan as a total war for control of the state, while the U.S.-led coalition operates with a limited conflict in mind, seeking to "hold the line" with the minimum level of human and material resources expended. At the level of the major powers, Russia has a high level of commitment to holding the Crimea, and to supporting ethnic Russians in Donetsk, while NATO is clearly less determined to see any redress of the situation in favor of Ukraine. As to the United States and Britain, signatories to the 1994 Budapest Memorandum on Security Assurances, which guaranteed Ukraine's territorial integrity, both major powers seem to be suffering from selective or strategic amnesia.[19]

As to terrorism, it seems that the gray zone concept is limited in its ability to help us grasp the strategic implications of the shift in this phenomenon from its origins as a form of symbolic violence with some form of extortion in mind to a mode of conflict in its own right. On this point, though, it is clear that much earlier thinking on terrorism as an emerging form of warfare remains highly relevant. Indeed, the Baron von der Heydte—a German paratroop commander during World War II and an international legal scholar after—was among the first to see, in the wake of the Six-Day War in 1967, that terrorism was becoming a form of "war out of the dark" in which "the decision is sought, and ultimately achieved, in a very large number of small, individual operations."[20] To say the least, the Baron was prescient. As was Claire Sterling, who observed back in the 1980s that terrorism was growing via networked forms of organization—and would continue to do so.[21] The challenge in the great post–9/11 war among nations and terrorist networks is to understand the characteristics, including the strengths and vulnerabilities, of networks. The gray zone concept does little to achieve this. Sterling's ideas do, and can form the basis for a counter-network paradigm. Just as the Baron von der Heydte's formulations provide a foundation for viewing the nature of the current era of conflict.

Thus it seems clear that there are times when, in the words of Winston Churchill, "the farther back you can look, the farther ahead you will see." This is such an era, an age of irregular warfare, terror, covert action, and other asymmetric modes of conflict. To confront and master these challenges, older, deeper, more developed concepts are likely to serve better than just freshly-minted terms. For example, Lewis Gann observed not only how often guerrillas have been defeated, but also the key elements upon which victory or defeat pivot in these wars. Beyond well-known factors like denying havens and inhibiting external support, Gann emphasized the largely psychological nature of guerrilla wars, railed against having counterinsurgent forces with "big administrative tails," and suggested cost-effective ways to improve the ability to gain information critical to finding the hidden.[22] Recent scholarship has powerfully affirmed Gann's views—especially about the frequency with which and conditions under which guerrillas can be and have been defeated.[23]

Otto Heilbrunn should also be mentioned. Almost 50 years ago, he provided an outstanding analysis of the conditions favoring victory by the counterinsurgents over irregulars and, conversely, conditions associated with the likelihood of seeing an insurgent victory. Briefly, Heilbrunn identified three types of insurgencies: terrorist wars (e.g. Palestine); small-unit guerrilla wars (e.g. Malaya, Kenya, Greece, and Algeria); and large-unit insurgencies (e.g. Tito, Mao, and Giap). He went on to argue that terrorist wars generally lead to stalemates—a point he made so long ago, yet which resonates quite powerfully today. Small-unit guerrila wars have been won, more often than not, by the counterinsurgents; whereas guerrillas have won all large-unit conflicts.[24] Heilbrunn's typology

of irregular wars and his analysis of them remain highly relevant, yet his work—and that of others who grappled with these challenges—will all too likely be forgotten or lost in the gray zone. Another example of the risk run by relabeling a longstanding phenomenon.

Paradoxes Regained

As important as it is to take a retrospective view and search out still-valuable paradigms before they become totally lost or simply ignored out of existence, one must also remain attentive to the possibility of reemerging paradoxes. Perhaps the most nettlesome of the paradoxes is revealed by contemplation of the costly, all-too-often counterproductive results of American military interventions and foreign policy initiatives in the years since 9/11. This period, which began a decade after the dissolution of the Soviet Union, should by all traditional measures of power have seen American vital interests well-served and policy goals promptly achieved. Yet results have proved to be very far from satisfactory, with a seemingly endless sea of troubles looming straight ahead. To be sure, part of the problem lies in the rise of irregular modes of conflict—but such challenges have been met and mastered in the past. Curiously, what may be adding to the difficulty in parsing them today is the very concept of the gray zone.

By creating the notion of a space that lies between war and peace, rather than simply recognizing the rise of irregular warfare to a leading position on the spectrum of conflict, American strategists have hobbled themselves, like horses whose tethered legs allow little movement. The failure to see that the gray zone is actually *in and an essential part of* the realm of war conveys huge advantages to insurgents, terrorist networks, and roguish nations. Understanding why this failure of perception has occurred reveals another paradox: how the Marxist worldview—that failed socially, politically, and economically—and a radical offshoot of Islam—that is overwhelmingly rejected by Muslims—have both come to life owing to the fuzzy thinking about conflict in the United States that has diffused among its allies and friends.

The problem with gray zone thinking is that it confounds the very paradigms that have generally guided the behavior of the world's more progressive, or at least more advanced, nation-states. One foundational body of thought is classical liberalism—not to be confused with today's meaning of the word "liberal"—that grew from the economic thinking of Adam Smith and David Ricardo. Both favored free markets instead of the controls imposed by mercantilist policies. And both saw the rational individual as the prime unit of analysis in commercial affairs. The heirs to their thinking became devoted to the "Manchester Creed," a belief system based on the notion of an enduring harmony of interests. War in this paradigm is a clear aberration. Thus classical liberalism has a hard time with the notion of a gray zone between a harmony of interests and open conflict. Perhaps the best example of the great difficulty this world view has had with creeping aggression of the gray-zone sort is provided by the befuddlement of England, France, and even the League of Nations in the face of Nazi actions and annexations during the 1930s. Edward Hallett Carr, the great historian and analyst of this period, was the first to critique the liberal paradigm as inadequate, noting of this time that it was "no longer possible to believe that every state, by pursuing the greatest good of the whole world, is pursuing the greatest good of its own citizens, and *vice versa*." He concluded that "[t]he inner meaning of the modern international crisis is the collapse of the whole structure of utopianism based on the concept of the harmony of interests."[25]

Despite the travails of World War II and the Cold War, in the half-century between Hitler's invasion of Poland in 1939 and the fall of the Berlin Wall in 1989 sustained efforts arose to rehabilitate notions of the harmony of interests. "Neoliberal"

thought, which emphasizes the importance of global institutions and agreements, operates under the assumption of harmony. As Robert Jervis has noted, neoliberals believe that the onset of armed conflict is just evidence that "international politics represents tragedy rather than evil."[26] Even the polar opposite of liberal thought, flinty Realism with its emphasis on power calculations in matters of war and peace, makes clear that there are "rules of the game" even at this level that are not lightly disregarded. The father of the realist school of thought, Hans Morgenthau, went so far as to argue "there is the misconception . . . that international politics is so thoroughly evil that it is no use looking for ethical limitations of the aspirations for power." Instead, he noted, it was more proper to focus on "the increasing awareness on the part of most statesmen of certain ethical limitations restricting the use of war as an instrument of international politics."[27]

The structural realists who have come after Morgenthau have seen war as a disturbance—what leading realist John Mearsheimer, echoing Jervis, describes as tragedy—of an equilibrium to be restored by balancing behavior.[28] In sum, classic liberalism and realism, along with their neoliberal and structural realist descendants, remain key, guiding paradigms that tend to see sharp, clearly delineated dividing lines between states of peace and war. The gray zone concept poses a challenge they are not particularly well-suited to address which may help to explain, in part, the difficulty liberal- and realist-oriented policymakers have had in coping with the crises of the post–9/11 era.

By way of contrast, the seemingly defunct Marxist paradigm actually provides a more useful way to think about the low-level conflicts that populate the gray zone and bedevil our time. Like classic liberalism, Marxism draws its basic tenets from economic analysis. But a key difference is that, whereas liberal thought was based on a belief in the harmony of interests, Marxism sees the world, in the phrasing of Jeffry Frieden and David Lake, as "necessarily conflictual."[29] And it is quite clear that Marxists did not simply see this conflict as limited to the economic realm. For V.I. Lenin a perpetual war was to be fought, often of subversion and various forms of low-level violence. The aim was to meet what he described as "the preliminary condition for every people's revolution . . . the smashing, the *destruction* of the ready-made State machine."[30] His successor Josef Stalin reaffirmed this point in his 1924 monograph, "The Foundations of Leninism," in which he argued "the law of violent proletarian revolution . . . is an inevitable law." The coming of peace, he thought, could happen only "in the remote future, if the proletariat is victorious."[31]

The gray zone construct, as noted earlier in the mention of formal definitions in current use, includes irregular and guerrilla war, as well as acts of terrorism. The Marxist paradigm makes no effort to employ such fine distinctions. Instead, all these phenomena are forms of *war*. Mao Zedong argues this point unambiguously in his writings, affirming that "guerrilla operations must not be considered as an independent form of war. They are but one step in the total war." He returns to this theme repeatedly, linking irregular warfare to overall goals, and finally concluding that "the strategy of guerrillas is inseparable from war strategy as a whole."[32] Vietnam's Vo Nguyen Giap, who was influenced to a significant degree by Mao's thinking, adhered to this notion in his and Ho Chi Minh's long, successful fight against the French and, later, the Americans.

For all the continuing value of Marxist strategic thought today—Russia and China, two heirs of Marx, are showing real mastery of our so-called gray zone—there is another conceptual paradox that has been regained: Islamism. And not just the odd, fringe beliefs so widely and overwhelmingly rejected by the world's Muslims. Rather, the paradox is to be found in the rebirth of the early notion of the obligation to wage perpetual warfare against "unbelievers."

This idea animated the first great sweep of Arab conquests in the 7th century and thereafter, shored up resistance to repeated "crusades," and sparked continuing conflict that was waged for many centuries in the Mediterranean, and at times beyond, by the corsairs of Barbary—who eventually ended up fighting U.S. Marines early in the 19th century. Of this true "long war" mentality Sir John Bagot Glubb, a soldier who did much service with Arab forces, wrote tellingly about how their forebears

> *swept irresistibly forward without organization, without pay, without plans, and without orders. They constitute a perpetual warning to technically advanced nations who rely for their defence on scientific progress rather than the human spirit.*[33]

Could there be any more cautionary, telling explanation of the true antecedents of the zeal and tenacity modern Muslim extremists have shown since the great war between nations and terrorist networks erupted in the wake of the 9/11 attacks on America? I don't think so. Just like the heirs of Marx, today's Islamist fighters see war as a quite unitary construct. A phenomenon that, from very early days, saw the jihadis skillfully blending conventional and irregular modes of conflict. As G.E. von Grunebaum, a leading scholar of Islam from the 7th to the 13th centuries, observed, "guerrilla warfare, apart from several larger expeditions, *continued without interruption*."[34] Those who oppose the present-day jihadis may try to slice and dice conflict in different ways, based on their habits of mind and institutional biases against treating something other than conventional war as "war." But they do so at their increasing peril.

Conclusion

This article has sharply critiqued the very notion of the "gray zone." It is an intellectual construct that confuses rather than clarifies the spectrum of conflict, and plays into the hands of smart, motivated aggressors who see war in simpler ways. That is, today's aggressors are most willing to accept insurgency, terror, subversion and covert action as war—right alongside increasingly rare occurrences of conventional conflict. The irony of the situation is that the victors in the Cold War, the champions of democracy, modernization and the "new world order," hamstring themselves by dithering over new definitions for old concepts that an earlier generation of their own strategists had thought about deeply and insightfully. Meanwhile, the heirs of Marx and of classical militant Islam—two paradigms long seen as defunct and widely rejected—come to 21st century conflict better prepared, in terms of mindset, for the waging of protracted war in all its many dimensions.

If we must have a fresh definition for war in this era—and I am still far from convinced that we should—let it be "hybrid warfare," the term for present and future conflict that then-Defense Secretary Robert Gates first used in 2009. He was no doubt inspired by "hybrid thinking" going on in the Marine Corps, and the thoughtful 2007 policy study by Frank Hoffman, *Conflict in the 21st Century: The Rise of the Hybrid Wars*. In it, he posed the prospect that "we can expect to face competitors who employ all forms of war and tactics, perhaps simultaneously."[35] At least this term recognizes the irregular as a full-blooded form of conflict, right alongside conventional war. Thus it gives those on the defensive—and make no mistake, the United States and its allies and friends are on the defensive—good reason to sharpen their wits in the face of aggressive actions by major powers and regional states, rogues, and terrorist and insurgent networks. There is a world war under way, waged in hot, cold, and cool modes. The aggressors see no gray zone "between war and peace." They see all as war. So must we. PRISM

Notes

[1] The Uppsala Conflict Data Program (UCDP), Peace Research Institute Oslo (PRIO), and the Global Terrorism Database (GTD) maintained at the University of Maryland all concur broadly with this assertion. In 2001, there were roughly 2,000 terrorist incidents that caused an estimated 14,000 deaths and injuries. By 2015 that number had risen to 15,000 attacks and more than 80,000 total casualties. The upward trend continues.

[2] UCDP and PRIO figures for conflicts exceeding 1,000 battle deaths in a given year.

[3] Perhaps the broadest depiction of Iran's global capabilities was offered in a hearing before the House Committee on Foreign Affairs, Subcommittee on Terrorism, Nonproliferation, and Trade on March 20, 2013. See especially I*ran's Global Force Projection Network: IRQC Quds Force and Lebanese Hezbollah* (statement of Will Fulton, American Enterprise Institute Critical Threats Project Iran Analyst and IRGC Project Lead).

[4] Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History'," *Foreign Policy Magazine*, July 9, 2012.

[5] I borrow and slightly expand the meaning of the term from Frederik Pohl's classic dystopian novel, *The Cool War* (New York: Del Rey Books, 1981), in which many of the world's leading nations engage in protracted, covert conflicts against each other.

[6] For details, see Marcus Weisgerber, "Peeling the Onion Back on the Pentagon's Special Operations Budget," *Defense One*, January 27, 2015.

[7] Hal Brands, "Paradoxes of the Gray Zone," (Philadelphia: Foreign Policy Research Institute, February 2016). Another thoughtful exposition of the concept can be found in Michael Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: U.S. Army War College Press, 2015).

[8] International Security Advisory Board, Hon. Gary Hart Chairman, *Report on Gray Zone Conflict* (Washington, DC: Government Printing Office, 2017), 1.

[9] Clausewitz's *On War* scarcely touched on the irregular—e.g. see Book Six, Chapter 26, "The People in Arms." But he lectured extensively at the Prussian War College on the guerrilla wars against Napoleon conducted in Spain and in the Austrian Tyrol. Christopher Daase and James Davis edited and translated these lectures in the fine *Clausewitz on Small War* (Oxford: Oxford University Press, 2015). C.E. Callwell's seminal work was *Small Wars: Their Principles and Practice* (London: University of Nebraska Press, [1896]1996). One of the best general surveys of irregular wars in this era can be found in Walter Laqueur, *Guerrilla: A Historical and Critical Study* (Boston: Little, Brown & Co., 1976).

[10] See Mao Zedong, *On Guerrilla Warfare*, Samuel B. Griffith translation (New York: Frederick A. Praeger, 1962), Ernesto "Che" Guevara, *Reminiscences of the Cuban Revolutionary War*, V. Ortiz translation (New York: Grove Press, 1963), Vo Nguyen Giap, *Big Victory, Great Task* (New York: Frederick A. Praeger, 1968), David Galula, *Counterinsurgency Warfare* (New York: Praeger Security International, 1964), Otto Heilbrunn, *Partisan Warfare* (New York: Frederick A. Praeger, 1962), and Lewis Gann, *Guerrillas in History* (Stanford: Hoover Institution Press, 1970).

[11] Brands, "Paradoxes of the Gray Zone,"4.

[12] Kenneth N. Waltz, *Man, the State, and War: A Theoretical Analysis* (New York: Columbia University Press, 1954), p. 236.

[13] Robert Taber, *The War of the Flea* (New York: The Citadel Press, 1965), 29.

[14] Regarding al-Suri's keen interest in Taber's work, see Brynjar Lia's biography of him, *Architect of Global Jihad* (Oxford: Oxford University Press, 2009).

[15] See *U.S. Army Field Manual 3-24 and Marine Corps Warfighting Publication 3-33.5*, jointly published as The U.S. Army and Marine Corps Counterinsurgency Field Manual (Chicago: University of Chicago Press, 2007).

[16] Eliot A. Cohen, *Commandos and Politicians* (Cambridge: Harvard University Center for International Affairs, 1978), 45.

[17] Gregory F. Treverton, *Covert Action: The Limits of Intervention in the Postwar World* (New York: Basic Books, Inc., 1987) provides an excellent survey of the American practice of covert action from the early 1950s to the late 1980s.

[18] See Andrew J.R. Mack, "Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflicts," *World Politics*, Vol. 27, No. 2 (January 1975), 175–200. Important studies that have built upon this theme include: T.V. Paul, *Asymmetric Conflicts: War Initiation by Weaker Powers* (Cambridge: Cambridge University Press, 1994), which explores both successes and failures of asymmetric approaches; and Ivan Arreguín-Toft, *How the Weak Win Wars: A Theory of Asymmetric Conflict* (Cambridge: Cambridge University Press, 2005), which argues that conventional strategies for opposing irregular opponents do rather poorly.

[19] Ironically, Russia also signed the Memorandum—that extends the guaranty to Belarus and Kazakhstan as well—in return for their and Ukraine's agreement to give up the nuclear weapons they inherited upon the dissolution of the Soviet Union.

[20] Friedrich August Freiherr von der Heydte, *Modern Irregular Warfare in Defense Policy and as a Military*

Phenomenon, translated by George Gregory (New York: New Benjamin Franklin House, [1972]1986), 3.

[21] See Claire Sterling, *The Terror Network: The Secret War of International Terrorism* (New York: Holt, Rinehart and Winston, 1981).

[22] Gann, *Guerrillas in History*, 89–90. With regard to information-gathering, Gann advanced the clever idea of reversing the terrorist tactic of using threatening "night letters" aimed at intimidating the populace. Instead, he outlined a means by which the people caught in the middle of a guerrilla war could be encouraged to inform anonymously on the insurgents while retaining secure means for later proof of the valued information they provided.

[23] Ben Connable and Martin C. Libicki, *How Insurgencies End* (Santa Monica: RAND, 2010), note of the 89 cases from the modern era they examine that the counter-insurgents won slightly more than half of the clearly decided conflicts.

[24] Otto Heilbrunn, "When the Counter-Insurgents Cannot Win," *Royal United Services Institution Journal*, Vol. 114, No. 653, (1969), 55–58.

[25] E.H. Carr, *The Twenty Years' Crisis, 1919–1939* (London: Macmillan, 1939), 62.

[26] Robert Jervis, "Realism, Neoliberalism, and Cooperation," in Colin Elman and Miriam Fendius Elman, eds., *Progress in International Relations Theory* (London: MIT Press, 2003), 289.

[27] Hans Morgenthau, *Politics Among Nations* (New York: Alfred A. Knopf, 1948), 174–80. Morgenthau goes on at some length to condemn the killing of innocents in peacetime and noncombatants in wartime.

[28] See John Mearsheimer, *The Tragedy of Great Power Politics* (New York: W.W. Norton, 2001); and Kenneth N. Waltz, Theory of International Politics (New York: McGraw-Hill, 1979).

[29] See Jeffry Frieden and David Lake, *International Political Economy* (New York: St. Martin's Press, 1987), 9.

[30] V.I. Lenin, *Selected Works* (Moscow: Progress Publishing, [1904] Second Edition 1965), 37. Emphasis in the original.

[31] Cited in David McLellan, ed., *Marxism: Essential Writings* (Oxford: Oxford University Press, 1988), 303.

[32] Mao Zedong, *On Guerrilla Warfare*, 41, 95.

[33] General Sir John Bagot Glubb, *The Great Arab Conquests* (London: Hodder and Stoughton, 1963), 359.

[34] G.E. von Grunebaum, Classical Islam (New York: Barnes & Noble, 1997), 97. Emphasis added. See further affirmation of this view in Robin Wright, S*acred Rage: The Wrath of Militant Islam* (New York: Touchstone, 2001).

[35] Cited in Paul Brister, William H. Natter III, and Robert R. Tomes, eds., *Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict* (New York: Council for Emerging National Security Affairs, 2011), 13.

Photos

Page 118: Image reproduced unaltered with permission from DigitalGlobe.

Page 120: Wikimedia/Andrew Butko. Licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License. Photo produced unaltered.

The WMD Center's annual symposium traditionally attracts more than 300 officials and experts from the countering–WMD and strategic deterrence communities. The symposium this year will take place from June 20–21 at NDU and will focus on the evolving role of WMD within the geopolitical strategies, defense policies, and military plans of potential U.S. adversaries. The first day will emphasize the strategic calculus and WMD capabilities of adversaries, while the second day will consider responses to the challenges they pose. The symposium's overall classification is SECRET/REL FVEY, and participation will be open to citizens of the Five Eyes countries possessing the requisite security clearance. Register for this event at <http://beta.saic.com/ndu2018/>.

An Interview with Congressman James R. Langevin

How have the threats facing the United States evolved in the 16 years you have been in Congress?

When I first came into Congress, we were still in that transition phase of going from a relatively calm and stable, bipolar world with the United States and the Soviet Union as chief adversaries. We were just entering the multi-polar world in which we live and the world became much more paradoxically unstable and the threats became more involved and grew. I came in around 2000—before 9/11—and none of us could have anticipated how the world would change so dramatically, on that date in particular, and later morph into other threats and challenges.

Now we have threats of international terrorism. A resurgent Russia is a challenge to the United States and to the international community. There is the growing challenge of China and their cyber activities, as well as the challenges China poses to U.S. interests in the Asia Pacific region. And you have the nations of Iran and North Korea—particularly the nuclear threat coming from North Korea. And then of course, one of my primary focuses is the challenge of cybersecurity. I often say that cybersecurity is the national and economic security issue of the 21st century. All those things have emerged and morphed since I first came to Congress and I do not see this challenge as diminishing any time soon.

The U.S. House of Representatives Armed Services Committee (HASC) Subcommittee on Emerging Threats and Capabilities (ETC)—please explain its mandate and priorities.

Much of the work in the ETC focuses on trying to confront our immediate challenges but also staying one step ahead of our adversaries, and the challenges that we face on a number of levels. Our subcommittee

This interview was conducted by Ms. Patricia Clough in October 2017 and updated early this year.

has jurisdiction over U.S. Special Operations Command (USSOCOM); U.S. Cyber Command (USCYBERCOM) and some aspect over the National Security Agency (NSA); and all Department of Defense (DOD) research and development programs. This includes the Defense Advanced Research Projects Agency (DARPA) and the work of the Office of Naval Research, as well as counterterrorism, counterproliferation, and information warfare-type programs. All of those elements confront not just immediate threats but also look down the road as to how we meet the emerging threats and challenges to our security. The ETC is perhaps the most interesting and challenging of the subcommittees, which is why I have stayed on it from the very beginning.

When I first got on the HASC it was the Research and Development (R&D) Subcommittee and I also was on the [separate] terrorism panel. We were limited by [House] rules on the number of subcommittees that we could have, so the HASC could not add another subcommittee. So what had existed prior to my arrival and had continued on for the first term of my time was the terrorism panel, which was relatively new and did not have the same power as a subcommittee. After 9/11 the HASC combined the R&D subcommittee and the terrorism panel to become-the Emerging Threats and Capabilities Subcommittee.

You mentioned USSOCOM—our Special Operations Forces primarily have been focused on counterterrorism but they recently assumed responsibility for countering non-strategic weapons of mass destruction. What new capabilities do our Special Operations Forces need, if any?

USSOCOM is still adapting to those additional responsibilities, but they are well-resourced in terms of people, training, and capabilities for their [new] counterproliferation mission. I am confident they will continue to do the job we expect.

What are your major concerns regarding the proliferation of WMD and the potential intersection with cyber and terrorist attacks?

There is a range of concern. Certainly nuclear proliferation is a chief challenge that we face, with North Korea as our primary adversary—the enemy that we need to be more concerned about and confront. Because as more fissile material is created you run the risk of that material getting into the wrong hands. The difficult part in creating a nuclear weapon is not developing the design—unfortunately, that information is readily available on the internet. The difficult part is getting your hands on fissile material. So anytime there is more fissile material out there in the world, you run the risk of it getting into the wrong hands.

This is something that has always worried me—if a nation-state sells fissile material to an individual or terrorist group, they may use it to make a nuclear device or to make a dirty bomb using radiological material. This worries me the most. Some radiological material is commonly available. Cesium, for example, is found in medical testing equipment and is the consistency of salt. If [a small amount of] cesium was dispersed through a traditional explosive device it could deny access to a significant amount of area for an extended period of time. Not only is there a physical threat, there is also psychological concern. North Korea is an enemy of the United States—what they might do with their fissile material concerns me.

As for the other emerging threats—chemical and biological threats worry me, as do cyber threats. What years ago could only have been achieved through use of kinetic weapons can now be achieved through a use of a few key strokes. A cyberattack on our electric grid could wipe out large portions of the grid for not just days or weeks, but potentially months.

When I first came into the [emerging threat] field, I chaired the subcommittee within the House

Committee on Homeland Security that has jurisdiction over cyber issues. My work there carries over to the ETC subcommittee. Sophisticated cyber actors, such as China, Russia, North Korea, and Iran threaten the United States as do individuals, terrorist organizations, and criminal enterprises. Nation-states give proxies the tools to carry out cyber operations to avoid having the nation-state's fingerprints on the operations. This keeps me up at night. Nation-states might have the worst weapons, but they lack the will to use them. How long will it be before the worst weapons get into the hands of someone or some entity that has the will to use them?

State and non-state adversaries have successfully adapted to the cyber age; what can the United States and our partners do to sustain our technological superiority?

Here is where we really need a whole-of-government approach. The [U.S. Department of State (DOS)] Global Engagement Center (GEC) was created by the previous Administration to coordinate counterterrorism messaging [to foreign audiences]. I have been very disappointed in the current Administration's limited use of the Center, for which the Department of Defense (DOD) plays a supporting role. The lack of stability and consistency in senior leadership positions within the DOS—and particularly in their oversight of the GEC—does nothing to instill confidence in this very important effort. It is imperative the United States uses the Center's robust capabilities and responsibilities to counter the messaging from our enemies—both terrorist organizations such as Islamic State of Iraq and the Levant or al-Qaeda in their recruitment efforts, and nation-states who use disinformation to sow discord in an attempt to weaken democratic institutions in western societies. It is noteworthy that the DOS has finally accepted $40 million in transfer funds from the DOD to assist in this effort. But we cannot, and should not, do this alone. We need to work with our international partners on counter-messaging. Terrorism and brazen threats to democracy are not just problems for the United States, they are international problems, and we need to be working on this together.

What would that collaboration look like?

We must ensure that we are using all of our capabilities to identify terrorist organizations that are trying to use their messaging capabilities to recruit and operationalize, whether it is domestically or overseas. The Federal Bureau of Investigations and Department of Homeland Security have the internal mission, which is not our role here in the ETC Subcommittee. But certainly overseas is something the ETC ought to be focusing on—is the United States using its capabilities in a robust way, making sure that we are working with our international partners to fight or countermessage?

What our Special Operations Forces might need for the fight—should the United States focus on acquisitions (software or equipment), technological know-how, or training?

USSOCOM already has vast acquisitions authority and rapid prototyping. Although, rapid prototyping is something we really ought to continue to support so that we get the best technologies in the hands of the warfighters. We have done some good work on that—separating out the research and development work from the acquisitions piece so that things function more appropriately. Still, there is more room for progress.

Rapid acquisitions versus over-the-horizon capabilities—how should the United States prioritize these needs?

That is where research and development comes into play in our subcommittee. How do we overcome the "valley of death?" Getting the technologies out of the lab and into the hands of the warfighter is always a challenge. As is overcoming cultural barriers. The

Pentagon loves their legacy capabilities and technology. We [the ETC, HASC, and Congress] sometimes need to prod the Pentagon along to ensure that they are adapting and utilizing these new capabilities. This is partly what oversight is about—constant hearings, and updates—pushing this wherever possible. As is understanding the lay of the land, understanding our adversaries' capabilities and investments—if they are trying to counter our advantage—or trying to invest in new technology areas that we may have ignored.

One of the things that comes to mind is our electronic warfare and how the United States' EW capabilities have somewhat atrophied. The Pentagon recognizes this and has revitalized its efforts to understand the nature of our EW challenges and what the United States needs to do on the defensive and offensive levels. Additionally, the Pentagon is making those changes and those investments known.

Are additional reforms needed within the Defense Department?

It is important to note that the past two National Defense Authorization Acts have contained key reforms that will require time for implementation. Separating research and development programs from acquisitions was key. We also elevated U.S. Cyber Command to a unified combatant command. There is still a question as to whether USCYBERCOM and the NSA should be split. At this point, I am not prepared to say USCYBERCOM should be split. How and when to end the dual-hat arrangement is a question we will have to grapple with down the road.

The Age of Lone Wolf Terrorism

By Mark. S. Hamm and Ramón Spaaij
Columbia University Press, 2017
336 pp., $ 35.00
ISBN: 978-0-23154-377-4

Reviewed By James Mis

The Age of Lone Wolf Terrorism by Mark S. Hamm and Ramon Spaaij provides the national security professional with an exceptional overview and appreciation of this growing problem facing the United States and its partners. Detailed in their compilation of the 123 incidents of lone wolf terrorism from 1940–2016, the authors examine the incidents against 20 variables to help identify trends in backgrounds, modus operandi, and motivations. Hamm and Spaaij, a professor of criminology and a sociologist respectfully, then devise a radicalization model that provides an evidence-based explanation for select case studies of lone wolf terror incidents.

The authors' findings are hindered by their broad definition of lone wolf *terrorism* that is misaligned with their constricted definition of a lone wolf *terrorist*. Hamm and Spaaij generalize, defining lone wolf terrorism as "terrorist actions carried out by lone individuals, as opposed to those carried out on the part of terrorist organizations or state bodies." The authors associate terrorism with political violence—making the lone wolf terrorist a "political creature"—based on "strong ideological or religious conviction," but this characterization allows the authors to include a wider population, including assassins, such as Sirhan Sirhan and James Earl Ray, abortion clinic bombers, and anti-civil rights fanatics. Yet, their hard-and-fast criteria of being a singleton discounts others such as Syed Rizwan Farook and his wife, Tashfeen Malik, in San Bernardino, California in 2015, or the Tsarnaev brothers in Boston, Massachusetts in 2013, although the authors point out valuable commonalities to the lone wolf in terms of motives and other variables. The friction in definition may add clutter in its broadness, while excluding valuable data and case studies that would assist in clarity.

While the reader can judge the overall uniqueness and applicability of the Hamm and Spaaij' model, it does meet the authors' intent to illustrate "push-pull factors," and serve as a suitable analytical tool in the absence of others. The model starts with a personal or political grievance that launches an "affinity with on-line [like-minded] sympathizers or external groups." It then moves onto being further influenced by enablers such as people—what Hamm and Spaaij call "model heroes"—or information on tactics or techniques for terrorist acts. The cycle continues with a broadcast of the lone wolf terrorist's intent, followed by trigger events that serve as the catalyst for the actual terrorist action. The cycle is then refreshed by a copycat or copycats with similar personal or political grievances.

However thorough their research or sophisticated their model, Hamm and Spaaij fall short in support of their argument that incidents of lone wolf terrorism are preventable since "violent radicalization is a social process involving behavior that can be observed, comprehended and modeled." Radicalization is a social process, but it is the individual—the lone wolf—who goes through the process. Humans are complicated, individually processing and reacting differently to such inputs as world events and social media posts, while existing within the complexity of the human domain. It is within the context of this complex system that trends based on a compilation of past events do not always lead to a predictable outcome.

Colonel James Mis, USA (ret.) is a faculty member in the College of Special Operations at the Joint Special Operations University.

The authors do, however, provide useful insight into the pools of individuals who may be susceptible to the influences of known enablers that serve as catalysts toward acts of lone wolf terrorism. For the national security and law enforcement professional, predictability is therefore facilitated by a narrowing of focus on a more select group; although some might describe this as "profiling"—a term and technique that may not be appealing in today's social environment, no matter its proven value.

For those readers who are in search of solutions to lone wolf terrorism, the authors' recommendations may disappoint. The authors state that one of their goals is to illustrate how the law enforcement and the intelligence communities can deal with this challenge. However, Hamm and Spaaij approach this by critiquing what they call the United States' three-pronged approach for combatting lone wolf terrorism," namely, the U.S. Department of State's digital diplomacy, joint U.S. Department of Homeland Security and Federal Bureau of Investigation efforts to forge ties with Muslim community leaders, and the FBI's sting program—arguably the United States' leading approach. Critiquing a current approach is a critical first-step in developing a more effective strategy, yet the authors over editorialize and offer little in the way of viable alternatives.

Spending two chapters on the subject, the authors are critical of the FBI sting program, calling it the "practice of creating crimes to solve crimes." Clearly the authors are not alone in their criticism, with others labelling the program as "entrapment." However, no judge has thrown out a case for this reason, while the program provides the proactive prevention expected by law-abiding citizens. The authors instead recommend a softer approach of intervention, stating, "There comes a point in each sting when FBI agents might have called on a family member, a psychologist, or a member of the clergy to provide counseling in a secure setting, instead of encouraging a person to kill innocent Americans with a bomb." To most readers the idea of FBI agents or any law enforcement entity serving as social workers undertaking interventions seems ridiculous.

There *are* other options in preventing lone wolf terrorism. Proactive law enforcement that utilizes the community as additional sensors is one option, ensuring that the focus is not on a specific religious or ethnic group community to avoid driving a wedge between the community and law enforcement. Increased and consistent intelligence-sharing among and between local, state, and federal agencies has also proven effective in prevention, with very recent lapses such as the mass shooting in Las Vegas, Nevada last year having catastrophic consequences. Monitoring of social media or the utilization of the community-based network will also be beneficial at the point when the lone wolf broadcasts intent, an opportunity that the authors themselves label as "the key to preventing lone wolf terrorism." Though many will disagree with the authors' recommendations and editorializing, non-traditional, alternative views and approaches are always beneficial, especially within an academic or theoretical setting meant to generate educational discourse in pursuit of better methodologies. There is no disputing that the law enforcement and intelligence communities have the most experience in effectively preventing such attacks, despite the tragic incidents that do and will occur.

Hamm and Spaaij meticulously demonstrate how the threat of lone wolf terrorism is ever-constant, manifesting itself in numerous forms of individuals with differing motives and backgrounds. The book's database, case studies, and modeling—despite the authors' political, or at least philosophical, slant—are valuable references and tools for the critical thinker's understanding of this problem set, while challenging some of today's approaches to defeating it. *The Age of Lone Wolf Terrorism* serves as a reminder for constant study, vigilance, and innovation.

Dirty War: Rhodesia and Chemical Biological Warfare 1975–1980

By Glenn Cross
Helion and Company, 2017
290 pp., $ 28.93
ISBN: 978-1-91151-212-7

Reviewed By Seth Carus

Glenn Cross's *Dirty War: Rhodesia and Chemical Biological Warfare 1975–1980* is a welcome addition to the small, but growing scholarly literature on the history of chemical and biological warfare. In 1965, the minority white community in the British territory of Rhodesia (officially Southern Rhodesia) rejected demands that it transfer political power to the majority black population. By the mid-1970s, white Rhodesians found it increasingly difficult to counter the growing power of native African nationalists fighting the government. As with many insurgencies, the guerrillas lacked the resources to defeat government security forces in direct combat, but Rhodesian forces were stretched too thin to suppress the insurgents, especially once they had established base camps in neighboring countries. Amidst the conflict, Rhodesian military and intelligence services employed what would now be considered chemical and biological agents against the guerillas with unknown results.

The Rhodesians adopted a decidedly low technology approach to waging chemical warfare. They made no attempt to acquire or produce any of the agents—e.g. VX, sarin, mustard gas, or phosgene—commonly associated with military chemical warfare programs. Instead, they employed commercially available poisons, primarily parathion (an insecticide) and thallium (used to kill rodents). Rhodesian intelligence officials, relying on the technical support of a small team based at the University of Rhodesia's medical school, used the infamous Selous Scouts to disseminate material. Another technique was to contaminate clothing with parathion infiltrated through nefarious channels to guerrillas. Contact with the poison treated clothing would kill or incapacitate the wearer.

The Rhodesians also killed a considerable number of guerillas through poisoned water sources and food, although exactly how many are unknowable. Cross seems most comfortable with an estimate of 1,500–2,500 people. This figure does not account for an unknown number of civilians who came into contact with the poisoned material, evidenced by the dramatic rise in poisoning cases reported by Rhodesian medical authorities.

Cross also discusses Rhodesian use of biological weapons. His account is somewhat confusing since it appears that there were two different biological weapons programs. The first, operated by Rhodesian regulars in the early 1970s, contaminated water supplies used by guerrillas with the pathogen responsible for cholera. Whether these efforts had any effect is impossible to discern. What public health officials call the 7th cholera pandemic reached Africa in 1970, so it is possible that claimed cholera outbreaks in guerrilla camps resulted from the natural spread of the disease.

The second program, which was a component of the 1970s chemical program, was much less ambitious. Cross believes that the Rhodesians only made significant use of botulinum toxin, noting claims (of uncertain reliability) that it caused substantial casualties among the guerrillas. His arguments about the limited scope of the second biological warfare program reflect doubt that the government deliberately created Rhodesia's 1978–79 anthrax outbreak, the largest in modern

Dr. Seth Carus recently completed a Distinguished Research Fellowship with the Center for the Study of Weapons of Mass Destruction at National Defense University.

history. The outbreak, which killed hundreds of thousands of cattle belonging to the black community, also caused considerable illness in the black population. Statistics, undoubtedly undercounting the true extent of the outbreak, indicate that nearly 11,000 people were affected, including an estimated 200 who died.

According to some accounts, including from sources who Cross considers less than reliable, the outbreak resulted from the intentional introduction of anthrax into native areas, ostensibly to infect cattle and deprive insurgents of a source of food. However, as Cross indicates it is possible to construct plausible natural explanations for the outbreak and its extent so that it is impossible to prove that it was intentional.

This highlights the complexities of CBW attribution—it probably will never be possible to determine responsibility for the anthrax outbreak or provide a complete picture of Rhodesia's CBW efforts and the consequences of those efforts. Outsiders—even foreign intelligence organizations—were unaware of Rhodesian chemical and biological warfare activities until more than a decade after the conflict came to an end. What few surviving documents exist Cross supplemented with interviews and declassified U.S. Government documents.

The problems Cross encountered are part of the story and highlight the contemporary importance of the efforts by the UN, human rights organizations, and the Organisation for the Prohibition of Chemical Weapons to systemically document CBW use. Almost four decades later, Cross' definitive account of an obscure set of events little known outside the specialist community offers important insight into CBW use by states in combating insurgencies. PRISM

The Darkest Sides of Politics, II: State Terrorism, "Weapons of Mass Destruction," Religious Extremism, and Organized Crime

By Jeffrey M. Bale
Routledge, 2016
492 pp., $33.77
ISBN-13: 978-1-13878-563-2

Reviewed By Brendan G. Melley

In this companion to his first volume on *Postwar Fascism, Covert Operations, and Terrorism*, Jeffrey Bale explores the influence of some of the world's most pressing security concerns through a review of global case studies on weapons of mass destruction (WMD), violent extremism, and organized crime. Bale is thorough in his selection and treatment of the cases, using primary sources whenever available and delivering an "intentionally robust" text to provide an alternative to what he describes in the volume's preface as often unqualified opinions taking the guise of academic works. Based on decades of research in violent extremism, Bale reviews select works and either updates their findings, or acknowledges their currency. *State Terrorism, "Weapons of Mass Destruction," Religious Extremism, and Organized Crime* is dense with explanations and structured expositions, but the volume offers a good model for how to convey conclusions that are framed by evidence.

Mr. Brendan G. Melley is a Senior Research Fellow with the Center for the Study of Weapons of Mass Destruction at National Defense University. His previous government experience includes work for the National Security Council, President's Foreign Intelligence Advisory Board, and the Defense Intelligence Agency.

In chapter 2, "South Africa's Project Coast: 'Death Squads,' Covert State-sponsored Poisonings, and the Dangers of CBW Proliferation," Bale traces the origins of the country's chemical and biological warfare (CBW) programs to the 1960–70s, as a purported response to Communist influences in the region. In this article that was originally published in 2006 and not altered, Bale explores Project Coast—a CBW program that the South African government formally initiated in 1981. Bale demonstrates that if South Africa had created the program officially in response to the fear that the Popular Movement for the Liberation of Angola (MPLA) and Cuban forces were equipped for chemical agent use against South African Defense Forces (SADF), it might have been expected to focus on defensive training and protective gear. This was not the case, however, which leads him to suggest that the regime did not take seriously the external CBW threat.

Bale states that Project Coast's offensive focus was likely influenced by neighboring Rhodesia's use of clandestine and covert operations to disrupt and kill internal enemies. Bale traces possible connections and, although he finds that South Africa did not appear to make frequent use of the wide variety of chemical and biological agents it was researching and novel weapons it was developing to support tactical military operations broadly, these efforts did find a ready home in the country's decades-old assassination program against internal enemies. He finds that "there can be little doubt that several of these toxic materials, items, or devices were subsequently used to murder or poison opponents of the apartheid regime."

In the volume's preface, Bale notes that fortunately, the worst fears regarding CBW proliferation from Project Coast have not materialized. He acknowledges this risk in his conclusion to Chapter 2 noting that, although Project Coast was gradually phased out in the early 1990s (and later scrutinized by the Truth and Reconciliation Commission), it is unknown if all of the documents and toxic materials were destroyed, or if key figures in the program had developed dangerous associations with despotic regimes or extremists.

Bale's extensive research raises a consideration that he does not specifically address—how some of Project Coast's personnel believed that lethal chemical weapons could be used against internal enemies of the state because that was not explicitly forbidden by the 1925 Geneva Protocol. A good topic for future study might be the parallels to more recent situations where states may have also held that justification, such as Syria's use of chemical weapons against its own population, and even North Korea dictator Kim Jong Un's use of nerve agent to assassinate his half-brother in Malaysia last year.

In Chapter 4, "Apocalyptic Millenarian Groups: Assessing the Threat of Biological Terrorism," Bale defines and explains the features of the numerous types of apocalyptic groups and cults, and highlights motivations behind their pursuit of biological weapons. Based on his related, unpublished research from the 2000s for an unnamed U.S. Government organization, Bale rationalizes various historic factors to identify specific features of indicators (ideological, organizational, rhetorical, financial, demographic, and behavioral) to help characterize the threat. He notes apocalyptic groups that simultaneously exhibit several of the above indicators' features should be of concern to law enforcement and intelligence communities, and that these would apply not just to biological terrorism, but also to mass-casualty producing conventional weapons or other types of WMD, if available.

In Chapter 5 Bale expresses his personal convictions on the unrelenting dangers of jihadist Islam and the inability of many Western analysts to understand the ideologies and objectives of global jihadist networks. Bale chooses to focus on al-Qaeda "central," as opposed to the spin-off groups and "amateur jihadists" that may take their guidance and motivation, if not training, from al-Qaeda. However, "Jihadist

Ideology and Strategy and the Possible Employment of WMD," was originally published in 2009 as part of an edited volume by Gary Ackerman and Jeremy Tamsett on *Jihadists and Weapons of Mass Destruction* and misses the rise (and recent decline) of Islamic State of Iraq and the Levant. Nonetheless, Bale's observations on the ideological factors, historic rationality, and long-term objectives of jihadism are still relevant and worth considering.

Bale decries "mirror imaging" Western concepts of rationality and security policies to help understand the jihadist threat; he states that "authentically Islamic conceptions" do not recognize sovereign states and have as their foundation the goal of the subordination of the whole world to Islam. Bale uses primary sources to characterize these "uncompromising" views of jihadist figures, which he acknowledges have been tempered by practical considerations, international norms, and power structures. Yet, he asserts, it is "naïve" to not appreciate the long term objective to Islamize the world, found in numerous statements and writings, and that their "rationality" cannot be captured by Western standards.

Bale explains that terrorists do pursue violence to achieve calculated objectives. On the subject of jihadist pursuit of chemical, biological, radiological, or nuclear (CBRN) weapons, he writes that by focusing on their stated intentions, it is still not clear how they might eventually decide to employ such weapons (e.g., for deterrence, tactical use, or against strategic targets). Bale also argues against the false assumption that CBRN weapons use is only intended to cause mass casualties and massive physical damage. For him, the real reason is the psychological influence on both enemies and supporters. Bale is adamant that Western analysts must conclude, from publically available research, that states cannot ever hope to compromise or reach an accommodation with groups such as al-Qaeda central whose aim is the destruction of America.

In this companion volume, Bale delivers on his promise to "promote more conceptual clarity" to confront popular misconceptions of terrorism and extremist violence that are oft held by experts. Bale uses empirical evidence to undermine these misconceptions and, although he may not win friends, critiques would have to confront his research head-on to try to convert him to their side. PRISM

The Politics of Weapons Inspections: Assessing WMD Monitoring and Verification Regimes

By Nathan E. Busch and Joseph F. Pilat
Stanford University Press, 2017
400 pp., $ 29.95
ISBN: 9-781-50360-160-4

Reviewed By Margaret Sloane And Justin Anderson

Nathan E. Busch and Joseph F. Pilat in their book *The Politics of Weapons Inspections: Assessing WMD Monitoring and Verification Regimes* draw attention to the important role that politics can play within weapons of mass destruction (WMD) verification, but the title promises more than the authors deliver. The authors analyze three cases of disarmament using inspections (South Africa, Iraq, and Libya); examine how the verification of global nuclear disarmament might or might not work; and apply the book's lessons to what they term difficult cases, which may be subject to future inspections

Dr. Margaret Sloane and Dr. Justin Anderson are Senior Research Fellows with the Center for the Study of Weapons of Mass Destruction at National Defense University.

(North Korea, Iran, and Syria). The studies provide a useful survey and side-by-side comparison of the successes, pitfalls, and likely future challenges of efforts to verify individual state compliance with WMD agreements. The authors on occasion fail to place the case studies within a broader geopolitical context, leaving important gaps in their analysis, which makes for an uneven read. As an example, the authors point to shortfalls in multilateral verification regimes without fully assessing how these regimes are limited and sometimes hamstrung by the external and internal politics of sovereign states.

In the post–World War II era, the threats posed by WMD led states to negotiate multilateral agreements that sought to limit or prevent the development and proliferation of these weapons, including the Nuclear Nonproliferation Treaty (NPT), Biological Weapons Convention (BWC), and Chemical Weapons Convention (CWC). The terms of these agreements varied, but the NPT and CWC both included provisions for verifying compliance. An important tool for verification is on-site inspections, which feature experts who visit sites and through observation, collection of samples, and other activities gather evidence to be used to assess compliance. The experts report their assessment to the political authority responsible for overseeing the agreement. This authority (or authorities) makes the ultimate decision about whether the inspected party is in compliance with the agreement and if not, whether its failure to comply was through honest error, negligence, or willful noncompliance. Verification and monitoring agreements result from states' negotiations to address a security threat and state governments make the final judgment about compliance or noncompliance.

Despite the origins of these agreements, the authors seem to expect the International Atomic Energy Agency (IAEA) and Organization for the Prohibition of Chemical Weapons (OPCW) to be larger than the sum of their parts and independent from them as well. Their verification processes, however, are deliberately embedded—by the states that negotiated the agreements and who provide the funding, authority, and means of enforcement for verification regimes—within a *political* framework and therefore they are constrained by the calculations and actions of independent, sovereign political actors. Both organizations reflect their members' wishes and have little agency to act independently, although individual leaders and inspectors can certainly have an impact. But these political dynamics are not addressed within the book's case studies, as the authors fluctuate between explaining the limits of inspections, verification, and monitoring and calling for actions by the IAEA and OPCW that may exceed the wishes of the member states.

While they recognize the limitations of means of conducting verification and monitoring, including possibly greater difficulty inherent in verifying chemical and biological weapons-related activities in comparison to nuclear, Busch and Pilat nevertheless argue that the IAEA and OPCW are "not sufficiently utilizing all of the tools at their disposal." They repeatedly criticize the IAEA and the OPCW for not going further in investigating suspect states by exercising options such as special or challenge inspections. The two organizations, they write, are pulling their punches with regard to these types of non-routine inspections, which are designed to catch potential violators. This criticism, however, overlooks important aspects of how these organizations operate, particularly given the book's focus on politics.

While both the IAEA and OPCW are international organizations supported by civil servants, they exist and operate within political environments and report to and are sustained by their member states. Their actions are conditioned by, and in some cases constrained by, political imperatives. The criticism also overlooks an important difference between the organizations' legal mandates. In

the case of the IAEA, the Secretariat can request a special inspection, which the country in question can accept or refuse. (In fact, the IAEA called for a special inspection in North Korea in 1993. After North Korea refused to accept it, the IAEA Board of Governors concluded that the country was in non-compliance with its Safeguards Agreement.) In the OPCW's case a member state must call for a challenge inspection; *not the organization itself*. This call can be blocked by a three-quarters majority of the states seated on the organization's Executive Council. If the inspection is not stopped, the subject country can still refuse to accept it. Given these onerous constraints, it is no surprise that thus far no member state of the OPCW has requested a challenge inspection. While the OPCW's member states and the IAEA's Secretariat may need to further utilize special or challenge inspections, recommending how they should do so within their political context and legal mandates would have been more useful and realistic.

The authors present an adequate summary of the Iraq case, which one of us has researched extensively and participated in as a member of the Iraq Survey Group, without delving too deeply into the politics and details of inspections and what transpired in the multi-year process of verification and monitoring. Perhaps this is too much to require of a single case study, but the omission of details (to include the politics and geopolitics that shaped, and ultimately significantly constrained, multilateral weapon inspections in Iraq) makes the discussion less rich and informative than it might have been. It is not possible to understand the complexities and limitations faced by international inspection teams in Iraq without a discussion, which is largely absent in this case study, of the divergent and often conflicting political agendas of different members of the UN Security Council. The lessons learned discussion for this case overlooks the importance of intelligence sharing and the work of inspectors, leaving the reader with an incomplete view of what is needed to successfully accomplish verification and monitoring.

The book is on stronger ground when the authors shift to a discussion of some of the scientific and technical challenges to developing and implementing verification regimes. The fifth chapter about how verifying global nuclear disarmament could work is thought-provoking and adds depth and reality to a lofty goal whose fulfillment would rest on verifiable compliance. It is an interesting exercise that highlights the limits of verification and its reliance on political will and trust. Without both factors verification may be limited to a point of uselessness. As the authors acknowledge at the end of the chapter, "Ultimately, verification requirements and their prescribed effectiveness will be decided politically. . ." This underlines a hard fact that deserves more attention in the wake of the new Treaty on the Prohibition of Nuclear Weapons, open for signature at the time of this writing: future deep cuts of nuclear arsenals and promulgation of a verification regime, not currently part of the treaty, will require fundamental political changes to both the international system and the internal politics of several current nuclear weapon states. PRISM

SUBSCRIPTIONS

Keep up to date with global and national security affairs, including sources, effects, and responses to international insecurity, global policy and development, nation-building and reconstruction, counterinsurgency, and lessons learned. To request your journal for complex operations, contact the *PRISM* editorial staff at <prism@ndu.edu>. Please include your preferred mailing address and desired number of copies in your message.

INSS

INSTITUTE FOR NATIONAL
STRATEGIC STUDIES