The Simons Center
Fort Leavenworth, Kansas

InterAgency Journal

Special Edition:

Weapons of Mass Destruction

The Journal of The Simons Center
Vol. 6, Issue 2, Spring 2015

InterAgency Journal

The *InterAgency Journal* (*IAJ*) is published quarterly by the Command and General Staff College Foundation Press for the Arthur D. Simons Center for Interagency Cooperation. The *InterAgency Journal* is a national security studies journal providing a forum for professional discussion and the exchange of information and ideas on matters pertaining to operational and tactical issues of interagency cooperation, coordination, and collaboration.

Contributions: The Simons Center encourages the submission of original articles based on research from primary sources or which stem from lessons learned via personal experiences. For additional information see "Simons Center Writer's Submission Guidelines" on the Simons Center website at www.TheSimonsCenter.org/publications.

About The Simons Center

The Arthur D. Simons Center for Interagency Cooperation is a major program of the Command and General Staff College Foundation, Inc. The Simons Center is committed to the development of interagency leaders and an interagency body of knowledge that facilitates broader and more effective cooperation and policy implementation.

About the CGSC Foundation

The Command and General Staff College Foundation, Inc., was established on December 28, 2005 as a tax-exempt, non-profit educational foundation that provides resources and support to the U.S. Army Command and General Staff College in the development of tomorrow's military leaders. The CGSC Foundation helps to advance the profession of military art and science by promoting the welfare and enhancing the prestigious educational programs of the CGSC. The CGSC Foundation supports the College's many areas of focus by providing financial and research support for major programs such as the Simons Center, symposia, conferences, and lectures, as well as funding and organizing community outreach activities that help connect the American public to their Army. All Simons Center works are published by the "CGSC Foundation Press."

The CGSC Foundation is an equal opportunity provider.

InterAgency Journal

Vol. 6, Issue 2, Spring 2015
Special Edition

Arthur D. Simons Center
for Interagency Cooperation

P.O. Box 3429
Fort Leavenworth, Kansas 66027
Ph: 913-682-7244
Fax: 913-682-7247
Email: office@TheSimonsCenter.org
Web site: www.TheSimonsCenter.org

PUBLISHER/EDITOR-IN-CHIEF
Raymond D. Barrett, Jr.

MANANGING EDITOR
Elizabeth Hill

COPY EDITOR
Valerie Tystad

DESIGN/PRODUCTION
Mark H. Wiggins
MHW Public Relations
and Communications

PRINTING
Allen Press, Inc.
Lawrence, Kansas

FEATURES

WORTH NOTING

Worth Noting *(cont'd)*

Book Review

Weapons of Mass Destruction and the Interagency

by John Mark Mattox

In principle, the idea of "interagency" in U.S. governance extends back to February 25, 1793, when President George Washington held the first meeting with his full cabinet—Secretary of State Thomas Jefferson, Secretary of the Treasury Alexander Hamilton, Secretary of War Henry Knox, and Attorney General Edmund Randolph.[1] Their interactions stemmed from the constitutional provision that the President "may require the Opinion, in writing, of the principal Officer in each of the executive Departments, upon any subject relating to the Duties of their respective Offices."[2] George Washington desired that his most trusted circle represent divergent geographical and ideological perspectives so as to lend credibility and balance to executive deliberations.[3] In that regard, his inclusion of Thomas Jefferson—a southerner from Virginia and an anti-federalist—and Alexander Hamilton—a northerner from New York and a federalist—provided both the divergence that Washington sought and probably much more. Referring to the oftentimes acrimonious exchanges between Jefferson and Hamilton, Jefferson would later write, "The pain was for Hamilton and myself, but the public experienced no inconvenience."[4] That is as it should be; the interagency is the place to sort out the many inconvenient details of governance that never could be sorted out via public referendum.

This glimpse into Washington's cabinet illustrates several points that collectively capture the essence of the interagency. First, the interagency is the practical means through which the President directs the executive activity of government. Second, the varied functions of government are not necessarily complementary. They involve competing priorities informed by the different emphases of each distinctive bureaucratic mission and the different ideologies that inform the world view of those called upon to deliberate upon and execute decisions and then interpret the specific meanings of those decisions in the ongoing course of implementation.

Even in Washington's world—with four cabinet members, a small interagency, a modest budget, a tiny set of laws to execute, and an operational context in which time moved at a comparatively slow pace—interagency work was hard work. Compare this setting to the world

Dr. John Mark Mattox (Colonel, U.S. Army, Ret.) is a Senior Research Fellow at the National Defense University Center for the Study of Weapons of Mass Destruction and the Director of the National Defense University Countering WMD Graduate Fellowship Program.

of the twenty-first century—with 16 cabinet members; an enormous interagency; a budget featuring numbers so large as to have no real meaning to most people; an ever-burgeoning set of law overlaid with a bewildering array of rules, regulations, and executive orders; and an operational context in which nanoseconds cannot be dismissed as irrelevant—and the contrast speaks for itself. It is in this latter context, however, that the interagency encounters the challenge of weapons of mass destruction (WMD).

Once the issue of what constitutes a "weapon" is resolved, there remains the question of what modalities of weapons should be included in the universe of WMD.

WMD and the Interagency

What is it about WMD that poses such an operational challenge for the interagency? Although the "pie" of possible responses might be sliced in any number of ways, no matter how it is sliced, it contains the following problems:

Definition

"What is a WMD?" is not nearly as straightforward as it may appear, because it presupposes three subsidiary questions: "What is a weapon?" "What does 'destruction' entail?" and "How much 'destruction' must occur before it can be classified as 'massive'?"

Weapons typically function as parts of a larger weapon system. For example, even if a nuclear gravity bomb is called a weapon, its weaponization is not especially meaningful if it does not have a delivery platform—a bomber or a fighter jet. Moreover, not just any bomber or fighter jet will do. The delivery platform must be specially outfitted with equipment that will enable the delivery of the gravity bomb in a very specific manner contextualized by a plethora of mission criteria. Similarly, one can imagine an intercontinental ballistic missile system that is not strictly classified as a "weapon" because it is presently disengaged from its targeting computer or lacks some essential component. Once the issue of what constitutes a "weapon" is resolved, there remains the question of what modalities of weapons should be included in the universe of WMD. Over 50 definitions "with some official standing in the United States and elsewhere"[5] fall into one of the following six categories:

- WMD as nuclear, biological, and chemical weapons (NBC).
- WMD as chemical, biological, radiological, and nuclear weapons (CBRN).
- WMD as CBRN and high-explosive weapons (CBRNE).
- WMD as CBRN weapons capable of causing mass destruction or mass casualties.
- WMD as weapons, including some CBRN weapons but not limited to CBRN, capable of causing mass destruction or mass casualties.
- WMD as weapons of mass effect capable of causing mass destruction or mass casualties or that cause mass disruption.[6]

This latter category at least contemplates the possibility of cyber weapons that could turn Western society—dependent as it is on computer technology—upside down. It also contemplates the possibility—disputed by some but increasingly recognized as plausible—of an electromagnetic pulse attack. Such an attack, produced by a nuclear weapon detonated high in the atmosphere and entailing virtually none of the thermal, blast, or radiological effects traditionally associated with nuclear weapons, would generate a wave of electromagnetic

energy of such magnitude that every electronic device within a one-million-square mile radius could be rendered inoperable. The effect of such an attack could transport the affected area from the twenty-first back to the seventeenth century instantaneously. In addition, the dark side of the emerging world of nanotechnology can create robotic gadgets small enough to flow through the blood stream to sicken or kill their host organisms.

Defining the last two words of the phrase weapons of mass destruction presents another set of challenges. World War II conventional attacks on Tokyo and Manila resulted in destruction as extensive as that visited upon Hiroshima or Nagasaki. However, the former are rarely referred to as WMD attacks. What counts as "destruction" appears to depend, at least in some measure, on whether one is on a weapon's giving or receiving end. For example, a radiological dispersal device that results in the leveling of a single-family dwelling and contaminating the immediately surrounding area may be assessed by the perpetrators as having been only minimally successful; however, to the former occupants, who will never be convinced that the site is sufficiently decontaminated to enable reconstruction, the attack was maximally destructive. In a related vein, the concept of "massiveness" is similarly dependent upon one's perspective. The Center for Disease Control may assess a biological attack with a deadly virus that kills 20 people as fairly minor and eminently manageable; however, for the persons who may have unwittingly interacted with infected persons—not to mention the family and friends of the deceased—the attack is catastrophic and life altering.

This much is clear: Not one of the critical sectors of U.S. infrastructure—not chemical facilities, not commercial facilities, not communications facilities, not manufacturing plants, not dams, not the defense industrial base, not emergency services, not energy production facilities, not financial services centers, not food and agriculture, not government installations, not healthcare and the public health apparatus, not information technology nodes, not nuclear reactors, and not transportation systems[7]—are immune from the risk of a WMD attack. Hence, the proposition that WMD is not an interagency problem is untenable, and the proposition that WMD is an interagency problem is unavoidable.

...the proposition that WMD is not an interagency problem is untenable...

Resourcing

WMD incidents are by their very nature very high-consequence affairs. However, they are also very low-probability affairs. The relationship between consequence and probability of occurrence is exactly inverse: The higher the likely consequence, the lower the likelihood of occurrence; the lower the consequence, the higher the likelihood of occurrence. Hence, the response protocol to lower-consequence scenarios tends to be subsumed under the response protocols for similar, low-consequence scenarios. Higher-consequence scenarios tend to fall in the realm of the unthinkable, and the natural tendency with respect to planning for the unthinkable is not to think about it, and hence, not to plan for it. When coordinating nuclear policy issues for a massive, international military exercise, I once asked the question: "Where in the exercise does the nuclear play occur?" I was frankly informed that such exercise play was totally impractical, as the inclusion of a nuclear event would utterly destroy any possibility of the exercise objectives being accomplished. "Utterly destroy" indeed.

Nevertheless, the fact remains that the threat of WMD is one of infinite competing practical

and political priorities. Given the scorn that attaches to WMD, the political path of least resistance is often to act as though WMD do not exist and then to bet on the viability of opening the emergency appropriation floodgates once a WMD event occurs (pausing periodically to hold committee hearings and conduct investigations to ascertain who was at fault for not having anticipated this low-probability/high-consequence event). It is here that the interagency will receive its "day in court"—only it will be as defendant and not as plaintiff.

In all fairness, most agencies have not totally ignored the problem of WMD. However, even if an agency is successful in assigning a relative priority to this low-probability/high-consequence event, it may still struggle to answer the question of how to spend money to address the problem. The breadth of the WMD challenge is such that "one-size-fits-all" solutions, elegant as they may seem and politically appealing as they may be, rarely work; they typically address only one rather specific aspect of the problem. However, if that solution cannot cover all areas at risk, what does it cover and how does it prioritize those risks? Similarly vexing is the question of where along an operational planning continuum to spend money. Does an agency direct its resourcing effort toward prevention, defense, or consequence management? Does it anticipate a general scenario, the particulars of which it almost certainly will not obtain, or does it wait until an incident arises before it acts? (The proactive leader who summarily dismisses the latter course as "reactive" may find it to be the only available course, such as could be the case with the emergence of a heretofore unknown biological threat.)

The task of defending the nation from the threat of WMD is, in all probability, the single-most challenging human-initiated problem the interagency could ever face.

Division of labor

Still to be answered is the question of who is to resource what with respect to defending against WMD. The solution is not as simple as fixing bureaucratic responsibility with this or that office or even divvying up bureaucratic responsibilities across the interagency. Of course, this must be done, but which agency should be responsible for which aspect of the WMD is not intuitively obvious. The word weapon suggests that WMD is a Department of Defense problem, and it is, but by no means exclusively. Rather, the essence of the interagency—the thread that binds the present to the nascent days of the interagency in George Washington's cabinet room—is the realization that everything is somehow connected to everything else, and at no time has that interconnectivity existed to a greater degree than in the globalized world of the twenty-first century. The problem, then, becomes not only how, where, and when to act, but also how to do so with the realization that whatever actions are taken (intentional or witting) affect the actions of (many) other players in the interagency.

The task of defending the nation from the threat of WMD is, in all probability, the single-most challenging human-initiated problem the interagency could ever face. While incremental progress is evident and welcome, the need for self-critical evaluation endures.

Exploring the Interagency Challenges with WMD

This special edition of the *InterAgency Journal* on WMD and the Interagency is fortunate to have the opportunity to highlight the work of Fellows from the National Defense University (NDU), Countering WMD Graduate

Fellowship Program. This highly competitive graduate program administered by the Center for the Study of Weapons of Mass Destruction at NDU brings together a diverse array of mid-career professionals from the uniformed services and the civil service to study the complexities of the twenty-first century WMD challenge. In this issue, they share valuable insights with respect to the interagency's encounter with WMD.

Chi K. Cheung provides what is likely the definitive account of the interagency effort leading to the demilitarization of Syrian chemical weapons.

Timothy W. Fisher explores the interagency challenge of WMD-related intelligence analysis.

David F. Grieco highlights the underappreciated but nonetheless very real threat of agroterrorism and the need for interagency synergies to counter that threat.

In a related vein, Cindy A. Landgren focuses attention on the imperative to secure the U.S. food supply—very possibly the quintessential interagency task.

Quan Hai T. Lu surveys the critical infrastructure of the U.S. and argues for how a massive cyber-attack—something that many are coming to understand as a new form of WMD—could cripple American society in ways that the average citizen rarely contemplates.

Finally, Matthew J. Moakler raises the question of whether the professional jurisdictional boundaries in the interagency and beyond are properly aligned to counter the threat of biological weapons research that could be accomplished behind the cloak of research for legitimate scientific purposes.

Together, these authors illustrate WMD to be one of the interagency's greatest but possibly least acknowledged (or perhaps even understood) challenges. It is one that will require heroic leadership efforts as U.S. government agencies work to identify common interests and reach an agreement as to who must do what when to protect the nation from what has been aptly described as "the gravest danger"—the use of WMD at the crossroads of radicalism and technology.[8] ***IAJ***

NOTES

1 "Cabinet Members," George Washington's Mount Vernon website, <http://www.mountvernon.org/research-collections/digital-encyclopedia/article/cabinet-members/>, accessed on January 7, 2015.

2 *The Constitution of the United States of America*, Article II, Section 2, Clause 1.

3 "Cabinet Members."

4 Thomas Jefferson, in Andrew A. Lipscomb and Albert Ellery Bergh (eds.), *The Writings of Thomas Jefferson*, Thomas Jefferson Memorial Association, 1905, Vol. 11, pp. 137–138,

5 Seth Carus, "Defining 'Weapons of Mass Destruction'," Occasional Paper 8, National Defense University Press, Washington, January, 2012, p. 6.

6 Ibid.

7 Department of Homeland Security—Critical Infrastructure Sectors, <http://www.dhs.gov/critical-infrastructure-sectors>, accessed on January 7, 2015.

8 George W. Bush, "The National Security Strategy of United States of America," Office of the President, Washington, September 17, 2002.

Cape Ray Diplomacy:
How a U.S. Merchant Vessel Took Center Stage in *Foreign Relations*

by Chi K. Cheung

In August 2013, chemical weapons attacks against civilians in Syria resulted in more than 1,400 deaths, including 426 children.[1,2] As a result of international pressure, the Assad regime agreed to accede to the Chemical Weapons Convention (CWC) and bring the Syrian chemical weapons stockpile under international oversight.

The Organisation for the Prohibition of Chemical Weapons (OPCW), the body charged with providing oversight for the implementation of the CWC, categorized the declared chemicals in the Syrian chemical weapons stockpile into two groups. The Priority 1 group contained the most dangerous agents, including six chemical agents. Two of these substances were the unitary sulfur mustard agent (also referred to as HD) and the binary component for the nerve gas, Sarin, methylphosphonyl difluoride (DF). The international community quickly determined that the remaining Priority 1 chemicals and all Priority 2 chemicals (comprised of chemical weapons precursors with valid industrial uses) should be destroyed at commercial industrial facilities. The options for the destruction of the HD and DF were to destroy them—in Syrian territory, at a host-nation commercial facility or on land or at sea using a transportable neutralization system.

The deteriorating security situation placed too great a risk for safely carrying out the destruction operations in Syria, and finding a nation to host the destruction was politically untenable. This left the plan to destroy the chemical agents at sea in international waters as the only remaining viable option. In late November, the OPCW agreed to the U.S. proposal to host the destruction of Syria's chemicals onboard the U.S. merchant vessel, Cape Ray. The Cape Ray was a first-of-a-kind capability for a mission never before attempted on a vessel at sea. Its story marks both an engineering triumph and a major success in interagency cooperation—in spite of numerous challenges arising from competing agency requirements and strictures.

Chi K. Cheung, (Commander, U.S. Navy, Ret.) served as the Defense Threat Reduction Agency primary on-site representative during the outfitting of the Cape Ray to destroy Syria's chemical weapon stockpile. He received a M.S. Degree in WMD Studies as a National Defense University Countering WMD Graduate Fellow.

The Challenges of Outfitting Cape Ray

The Chairman of the Joint Chiefs of Staff issued the warning order in late November 2013 to activate the strategic sealift vessel, Cape Ray, for the Syrian chemical weapons destruction. The order also directed the ship to be ready to deploy by early January 2014. Major modifications were made to the ship including installing two Field Deployable Hydrolysis Systems (FDHS), developed by the U.S. Army, Edgewood Chemical Biological Center to neutralize the chemical warfare agents, adding additional water desalinization capability, increasing capacity for an additional 96 crewmembers, providing a collective protection system for air filtration, augmenting communications for command and control, and installing a helicopter pad. The design for this massive engineering undertaking required months of planning and preparation prior to the activation order. The ability of the U.S. to make this offer took the efforts of agencies from across the U.S. government including the Departments of Defense (DoD), State, Transportation, Homeland Security, Commerce, and the Environmental Protection Agency.

The Defense Threat Reduction Agency (DTRA) first examined the concept to equip a ship to destroy the chemical agents at sea shortly after Syria acceded to the CWC. The plan matured as the type and quantity of the chemicals became known through the Syrian declarations. In total, the chemical agents weighed 848 metric tons, which called for the substances to be packaged and shipped in 127 separate, twenty-foot, International Organization for Standardization (ISO) containers. The hazardous waste (or effluent) generated in the destruction process required the installation of 382 ISO tanks that were roll-on/roll-off (RO/RO) removable from the ship's deck. Despite the work done by planners to anticipate issues, many assumptions were adjusted during the outfitting related to the chemical throughput and time required for operations.

The Portsmouth shipyard, General Dynamics NASSCO-Earl Industries—where Cape Ray was being activated—held the key to the answers for the two critical assumptions about the U.S. contributions toward the international effort. The first assumption was the amount of chemical agents that the ship could process, and the second was the date the ship would be ready to sail.

The Chairman of the Joint Chiefs of Staff issued the warning order in late November 2013 to activate the strategic sealift vessel, Cape Ray, for the Syrian chemical weapons destruction.

1. Chemical processing capability

The two key variables of the first assumption were the capacity of the sea-based platform selected and the reliance on components readily available in the commercial sector. The Department of Transportation Maritime Administration (MarAd) considered several vessels from its strategic sealift Ready Reserve Fleet for the mission. In the end, MarAd selected Cape Ray as the best-suited platform for the FDHS, primarily because of its large cargo capacity, continuously open deck space, and high overhead height clearances—all the elements necessary to accommodate the needs for a chemical weapons destruction facility. Despite these characteristics, as the outfitting of Cape Ray began, it became apparent that shortfalls in capacity necessitated a change of plans. The most significant discovery came in early December as the ISO tanks arrived onsite. Engineers discovered that due to a host of technical constraints the ship could only carry

269 ISO tanks. This reduction meant that Cape Ray could no longer destroy all six chemicals in the Priority 1 group on a single trip. Only the two most dangerous chemical substances, HD and DF, could now be processed on the ship without the need to offload ISO tanks in the middle of operations. Consequently, planners decided to make disposing of the HD and DF as the centerpiece of the U.S. contribution. This subsequently led to U.S. diplomatic efforts focused on finding international partners to take the four remaining chemical agents.

The U.S. wielded the Cape Ray departure date as a political instrument to apply pressure on the Syrian government to expedite surrender of its chemical stockpile.

In order to meet the required timeline and minimize manufacturing costs, plans called for leasing or buying commercially available prefabricated modules and using ISO tanks and Mafi trailers already in use by the maritime industry. With the exception of the FDHS, all systems installed on the Cape Ray came from the existing inventory found in the commercial sector.

The prefabricated components, including berthing compartments, office modules, reverse osmosis water purifying units, and even the helicopter pad had to be able to withstand harsh maritime conditions and to meet federal regulations, including U.S. Coast Guard certification requirements. As a result, the supply source was limited to a single vendor, located in Midland, Texas—a company that built and rented these types of units for the offshore oil industry.

The next supply challenge was with the availability of Mafi trailers, which were low profile RO/RO flat-bed trailers. The ship's internal tanks could not be used to hold the effluent generated by the FDHS from the processing of the chemicals due to the risk of contamination. The plan thus called for the effluent to be held in the ISO tanks. Once filled to capacity, these tanks exceeded weight limitations of the cargo handling equipment and could not be lifted off the deck. They had to be placed on Mafi trailers and then driven off the ship. Given only 43 days for the outfitting, Cape Ray experienced a shortage of Mafi trailers. Every available Mafi trailer in the U.S. was leased for this project. DTRA chartered an ocean freighter to deliver the remaining Mafi trailers from Germany. When weather delayed the arrival of the ocean freighter, DTRA then chartered two Russian-owned AN-124 air freighters to fly in the remaining Mafi trailers.

2. Sail date

The U.S. wielded the Cape Ray departure date as a political instrument to apply pressure on the Syrian government to expedite surrender of its chemical stockpile. Enormous pressure fell upon planners, engineers, suppliers, and shipyard workers, as well as a host of interagency coordinating staffs, to ready the ship. In total, the ship took 66 days to activate setting sail on January 27, 2014. Notwithstanding the January deadline dictated by the warning order, the delay was rendered unavoidable by, (1) the compressed timeline, (2) the growth in new requirements, and (3) the sheer weight of compounded interagency regulatory requirements.

DTRA planners had to offer a readiness date of the ship to meet the June 30, 2014, destruction deadline established in the U.S./Russia brokered deal. Using this deadline, planners figured early January as the window for when the ship must be available. Shipyard engineers had to work around three major holiday periods: Thanksgiving, Christmas,

and New Year's. Additionally, the shipyard contended with state and federal transportation regulations to move the necessary material. For example, the caustic soda and bleach needed for the destruction operations had to be moved over the U.S. highways to reach the shipyard. State and federal laws limited the weights, hours of operations, and roads used. This scaled back how quickly materials could be moved in each shipment, as well as the routes that could be taken to get to the shipyard. Slowing down the effort further, seven days were lost due to the weather. With a majority of the work happening in exposed areas, welding and crane operations were halted because of the rain, snow, high winds, and extreme cold experienced throughout this period. Furthermore, the media interest and high-level delegations visiting the ship contributed to numerous stoppages. Work ceased out of safety concerns for these large groups, which resulted in the loss of another two workdays.

The original 43 days needed to outfit Cape Ray did not allow for any significant additional requirements. Once operational components (the elements responsible for performing the mission) arrived in Portsmouth, personnel identified shortfalls that prevented them from carrying out the mission. The most far-reaching additional changes came from the OPCW inspectors, medical support team, and communications personnel, adding to the uncertainty of the departure date.

On December 9, 2013, the Office of the Secretary of Defense hosted a delegation from the OPCW Technical Secretariat for the initial consultations on the Facility Agreement, a required component of the destruction plan. The purpose of the consultations was to identify the technical requirements needed to meet the treaty obligations. Out of these consultations came the agreement to provide office spaces, closed-circuit television camera systems, and increased Internet bandwidth to host voice and video communications systems. The new additions for the OPCW required extra time for structural work and acquisition of several components not already on hand. The OPCW delegation returned on January 15, 2014, to hold the Final Engineering Review after final outfitting. This cleared the U.S. hurdle for Cape Ray to be used as a destruction facility.

The original 43 days needed to outfit Cape Ray did not allow for any significant additional requirements.

The final decision on whether to embark military or contracted civilian medical personnel did not come until the end of December. The late decision to move forward with a contracted civilian team was significant because it delayed the identification of one of the most important requirements—the treatment of casualties. The medical team held its first site survey of Cape Ray on December 23, 2013. After touring the spaces allocated for medical treatment, the team found the current accommodations inadequate. The medical team required the capability to stabilize one trauma patient for 24 hours until the patient could be evacuated to a medical trauma center. To facilitate this, the shipyard had to lease a medical module available only from the same vendor in Midland, Texas. The new footprint required removing an entire berthing module, significantly changing the number of people available for the mission.

The high visibility of the mission also created great demands for information sharing. Cape Ray was ultimately outfitted with two military and three commercial satellite communication systems, more than doubling the Internet bandwidth originally planned. As public interest and international attention grew, so did the call for transparency. Nongovernment organizations

and Mediterranean nations voiced concerned over potential environmental impact, and CWC obligations required the U.S. to monitor and report on the status of the destruction process. U.S. military commanders placed additional burdens on the communications infrastructure. Moreover, the crew of 130 took up bandwidth for morale and welfare purposes.

The Cape Ray required a National Defense Waiver (NDW) issued by the U.S. Coast Guard to deviate from her primary mission of strategic sealift.

The unique combination of regulatory requirements generated by this mission created an unprecedented interagency challenge, as the risks involved with carrying out the destruction of chemicals at sea drew concerns from the different organizations responsible for activating the ship and transferring it to military control: (1) military requirements placed additional demands on MarAd to train the crew to a standard beyond those called for on a U.S. flagged public merchant vessel, (2) Unknowns associated with final chemical carriage and hazardous waste made difficult the attainment of required documentation for a National Defense Waiver, and (3) advisory organizations that did not normally take part in the vessel activation process subjected Cape Ray to additional inspections.

MarAd normally maintains Cape Ray in a reduced operating status until called upon for the mission of strategic sealift. Strategic sealift entails moving cargo from one port to another when mobilized for a national crisis. For the strategic sealift mission, MarAd is only required to provide a crew trained to the standards established by the U.S. Coast Guard. However, operating a ship as a chemical agent processing facility is outside of any training a licensed mariner receives. To accommodate the additional training requirements, military commanders dedicated two of the four days during sea trials to this purpose.

The Cape Ray required a National Defense Waiver (NDW) issued by the U.S. Coast Guard to deviate from her primary mission of strategic sealift. The waiver authorized the ship to carry and process the dangerous chemical substances at sea. The challenge for MarAd in obtaining the waiver came from the uncertainty in type and quantity of chemicals that were to be processed, as well as the associated effluent generated. MarAd could not provide this information to the Coast Guard until U.S. policymakers decided upon final chemical carriage for the ship. As a result, the Coast Guard did not sign the NDW until January 17, 2014.

Unlike any vessel activation experienced by MarAd, Cape Ray's activation involved other military agencies levying concerns about seaworthiness and safety of operations. On January 15, 2014, immediately after Cape Ray returned from sea trials, stakeholders held a meeting that included senior executives and flag officers to address these issues. The sea trials answered many of the concerns, but the securing of the cargo to the ship's deck remained a major point of contention drawing in an independent third party, the National Cargo Bureau (NCB). As a result of that inspection, major structural work was needed to correct deficiencies in the cargo lashings on the ship.

Cape Ray Diplomacy

The interagency effort to ready the Cape Ray was not merely about how U.S. military planners and policymakers adjusted to accomplish the challenges of outfitting a merchant vessel; it was also about making the ship the centerpiece of U.S. diplomatic efforts. The unanticipated problems that came up over the two months it took to ready the ship meant that the U.S. had

to broaden its outreach with the international community to keep the destruction of Syria's chemical weapons stockpile a viable option. These diplomatic engagements were followed up by a smart media campaign at senior levels within the Departments of Defense, State, and Transportation, to reinforce the unity of U.S. government efforts. These combined factors ultimately led to a highly successful U.S. diplomatic engagement with the international community.

Developments on the ship frequently drove the discussions at the international table. Denmark, Norway, and Italy made key contributions in the early stages of the initial plan. Later on, Spain, Great Britain, Germany, and Finland gave their support to keep the plan viable.

The initial U.S. proposal to destroy Syria's chemical weapons at sea called for Cape Ray to take all six of the Priority 1 chemicals and destroy them in the FDHS in a single trip before returning to port. To make this plan work, the U.S. needed partner nation support to remove the chemical agents from Syria, a host nation to provide a port to transload the cargo onto the Cape Ray, and the international community, through the OPCW, to accept the hazardous waste generated in the process.

When Syria decided to surrender its chemical weapons stockpile, U.S. planners had to figure out how to remove and destroy the chemical agents without having an American presence in Syria. This became significantly more difficult when left only with the "destruction at sea" option. The challenge then became how to get the chemical agents out of Syria onto the decks of the Cape Ray without entering Syrian territorial waters. The vessel had a grey-hull, giving it a warship appearance. The crew consisted of U.S. civilian contractors, carried government civil servants, and maintained a small U.S. military command and security element. Using the Cape Ray to enter a Syrian port for the removal of the chemical agents was a diplomatic non-starter.

For the option to destroy Syria's chemical agents at sea to be possible, a third party nation would have to carry out the initial task of removing the chemical agents. This meant that planners needed to ensure that the vessels committed to the removal were compatible for the transfer of chemicals onto the Cape Ray. Over the course of the Cape Ray outfitting, DTRA planners exchanged information about potential ships. Oftentimes, the data needed for the Cape Ray did not exist because operational testing had never been done for a mission of this kind. Military-to-military engagements by DoD planners to answer the concerns of partner nations played an important diplomatic role. DTRA planners answered countless requests for information coming from interagency and international partners about the Cape Ray. Consequently, the governments of Denmark and Norway agreed to contribute their respective merchant vessels, Ark Futura and Taiko, for the removal of the chemicals agents from the Syrian port of Latakia. Ark Futura would carry all the chemical agents, HD and DF, destined for the Cape Ray. Taiko would take the Priority 2 chemical agents.

When Syria decided to surrender its chemical weapons stockpile, U.S. planners had to figure out how to remove and destroy the chemical agents without having an American presence in Syria.

After removal of the chemicals from Syria, the next task was to determine how to transload the chemical agents from the Ark Futura onto the Cape Ray. Neither ship was designed to conduct cargo transfers at sea. This meant that they needed access to a port. The Cape Ray ship characteristics and operating parameters limited

the choice of usable locations. The plan required a deep-water port that could accommodate two RO/RO vessels simultaneously. Access to a foreign port by a ship carrying chemical agents also carried great political risks that only the political leadership could shoulder. Negotiating the use of a foreign facility required a whole-of-government approach. In mid-December, a U.S.-led interagency delegation held a series of meetings in Stuttgart, Germany, to seek a donor nation for the use of its port facility. The meetings resulted in the government of Italy announcing on January 16, 2014, that it would offer the containership facility in Gioia Tauro for transloading operations.

Access to a foreign port by a ship carrying chemical agents also carried great political risks... Negotiating the use of a foreign facility required a whole-of-government approach.

Among other nations, Finland's major contribution came through the disposal of the bulk of the effluent generated by the Cape Ray through the OPCW tender process—the final agreement with the international community for how to handle the entire Syrian chemical stockpile. Without it, the Cape Ray would have been unable to dispose of the effluent. The terms of the OPCW tender package treated the effluent as hazardous waste. Thus, it allowed the private sector to dispose of the substances in a commercial facility. Finland won the bid to dispose the DF effluent and one of the four Priority 1 substances that the Cape Ray could no longer handle.

However, the need continued for a holding port in the Mediterranean and other partner nations to accept the remaining four agents that the ship no longer had the capacity to process.

An important international contribution came from Spain permitting the use of the naval base in Rota. The holding port allowed continual logistic access as well as crew relief. Without a holding port, the Cape Ray would have been underway for an indeterminate time, exposed to the harsh maritime environment. Military planners were unsure if the presence of the Cape Ray in Spain posed a political liability even without carrying a single container of chemical agents. Sensitive to the political undertones, military planners did not assume that the use of the naval base would be covered under the terms of the Status of Forces Agreement with Spain. Through the U.S. Embassy in Spain, military attachés worked to confirm with Spain's Ministry of Defense that the ship would be permitted to stay at the naval base prior to the start of destruction operations. On January 21, 2014, the U.S. diplomatic mission in Spain announced that the Cape Ray would be treated like all other U.S. military vessels visiting the country and did not need special diplomatic clearance at this stage of operations.

Great Britain also proved to be a tremendous ally in the effort. The British leadership shouldered great domestic political risk to make the at-sea option possible by accepting the task to destroy the remaining three of the four chemical agents in the Priority 1 group. Uncertain of the British public reaction for bringing these chemical agents into the country, the government made the commitment without seeking public debate. This commitment further reduced the effluent that would be generated by the FDHS process and the number of ISO tanks that had to be carried onboard the Cape Ray. It also removed a great deal of uncertainty for U.S. planners. As a measure of gratitude, the U.S. hosted a delegation from the U.K. Embassy on the Cape Ray at Portsmouth, Virginia.

The U.S. employed multiple channels of diplomacy on the state-to-state level when it negotiated with Italy for access to the

Port of Gioia Tauro to conduct the transload operations. The U.S. also worked with partners by obtaining contributions from Great Britain and Germany for the disposal of additional chemical substances and effluent. At the military-to-military level, U.S. defense officials confirmed with Spain's Ministry of Defense that it would allow Rota to be used as a holding port for the Cape Ray. The ship thus escaped the fate of being held indefinitely at sea to wait for Syria to remove its chemicals. Finally, the Cape Ray's reduced capacity meant the U.S. needed to take an active part in drafting the terms of the OPCW tender package. Here the U.S. employed the CWC treaty to bring the larger international community into funding and disposing of the remaining material and hazardous waste. In sum, the interagency choreography required to accomplish this historic mission was intense.

Controversy followed the Cape Ray even before arriving in theater and despite the fact that it would destroy Syria's chemical agents in international waters. The search for the ideal location to operate the ship limited military planners to the waters in the Mediterranean. Nongovernmental organizations (NGOs) and countries in the Mediterranean raised concerns about the potential environmental impact. The U.S. employed a vigorous communications campaign that called for active engagements with key partner nations in order to stay ahead of the controversy.

To prepare the countries potentially impacted by these operations, the Department of State took the effort to centralize the strategic messaging going out to U.S. missions around the Mediterranean. Meanwhile, U.S. defense officials embarked on a media campaign to take on the issue of the Cape Ray operating the FDHS in the Mediterranean.

Secretary of State John Kerry took measures to provide the missions in the Mediterranean a central U.S. public diplomacy position for the destruction of Syria's chemical weapons stockpile. The State Department issued a series of public affairs talking points regarding the Cape Ray. Given the number of nations making contributions to the effort and the large number of countries potentially impacted by the operating location, the U.S. needed a unified, whole-of-government response. The leadership from the Department of State served to get ahead of the controversy by centralizing the strategic message.

Given the number of nations making contributions...and the large number of countries potentially impacted...the U.S. needed a unified, whole-of-government response.

Taking place concurrently with outfitting and before the start of operations, the DoD launched an aggressive public campaign to demystify the Cape Ray and FDHS process. Over 50 news organizations from around the world received invitations to tour the ship. The media gained unprecedented access to film the FDHS and interview senior government officials as well as crewmembers. The Under Secretary of Defense Frank Kendall and Acting Maritime Administrator Chip Jaenichen seized the opportunity to increase confidence in the operations by making statements before the press. The captain of the Cape Ray and two operators of the FDHS also took the time to answer questions in front of cameras. After the Cape Ray arrived in Rota, Spain, the DoD launched another media campaign that included NGOs, foreign diplomats, and international press members from 15 different countries.

Conclusion

The Cape Ray provided policymakers a means to take Syria's chemical stockpile out of

Assad's hands. Without the at-sea destruction alternative, the options were limited to carrying out the destruction in Syria or finding a host nation, both of which were practically and politically unachievable. Planners working on the Cape Ray had less than two months to come up with a proposal for the at-sea destruction option and had only two months to execute it. Given only the original 43 days for outfitting, engineers and naval architects on the project had to work through regulatory challenges and against a compressed timeline and growing requirements. Despite taking 66 days overall, the Cape Ray was, among other things, a triumph of American interagency cooperation. To be able to so quickly offer U.S. policymakers an option that would not otherwise have existed, the Cape Ray made it possible for the U.S. to take a leadership role on the international scene. The challenges required the U.S. to work multilaterally with partner nations. The effort required a whole-of-government approach with strategic messaging and a media campaign. The engagements happened on multiple fronts of diplomacy, through state-to-state and military-to-military channels, as well as through institutions like the OPCW. In short, the collective effort required to accomplish this historic mission produced an historic success. ***IAJ***

NOTES

1 The views expressed herein are those of the author and do not necessarily reflect the official views of the U.S. government or any of its entities.

2 Office of the Press Secretary, "Government Assessment of the Syrian Government's Use of Chemical Weapons on August 21, 2013," The White House, August 30, 2013, <http://www.whitehouse.gov/the-press-office/2013/08/30/government-assessment-syrian-government-s-use-chemical-weapons-august-21>, accessed on July 13, 2014.

Improving the Intelligence Community's Contribution to Countering Weapons of Mass Destruction

by Timothy W. Fisher

There is, of course, no such thing as a perfect weapon of mass destruction (WMD) threat assessment.[1] Some of the brightest minds in the intelligence community continuously work WMD issues. The intelligence community, consisting of seventeen organizations from six departments and one independent agency, commits millions of dollars searching for information needed by senior leadership to make the best possible decisions concerning WMD threats to the U.S. Interagency planners rely on the intelligence community's efforts to plan for a potential adversary's use of WMD. According to an analysis by the James Martin Center for Nonproliferation Studies (portrayed in Figure 1, pg. 18), the principal U.S. government agencies involved in nuclear policy making include the White House, nine executive departments and agencies, and over 150 offices within them.[2] If this analysis were expanded to include all four WMD modalities (i.e., chemical, biological, radiological, and nuclear), the number of offices involved would be considerably larger. If it were expanded to include the whole of government (i.e., state, local, and tribal organizations) involved in countering WMD, the list would be well over a 1,000 organizations.

The U. S. has spent billions of dollars on programs to prevent, prepare for, respond to, and recover from a potential WMD attack. Nevertheless, with current and projected limitations on the federal budget, spending on WMD defense programs could likely decline. Hence, the U.S. must carefully prioritize its budget in order to counter WMD. Key to this effort is an effective, integrated WMD threat assessment that includes all the potential WMD actors and modalities, portrays adversarial success for each actor and modality, and identifies critical nodes by looking for threat overlap between or among scenarios.

The concerted efforts of the interagency will be required to ensure that the policies, plans, and activities of the whole of government result in an active, layered, defense in depth to protect

U.S. Army Lieutenant Colonel Timothy W. Fisher is the Chemical, Biological, Radiological, and Nuclear Defense Division Chief for the Army Test and Evaluation Command. He has served in the Office of the Secretary of Defense and the FBI Weapons of Mass Destruction Directorate. He received a M.S. Degree in WMD Studies as a National Defense University Countering WMD Graduate Fellow.

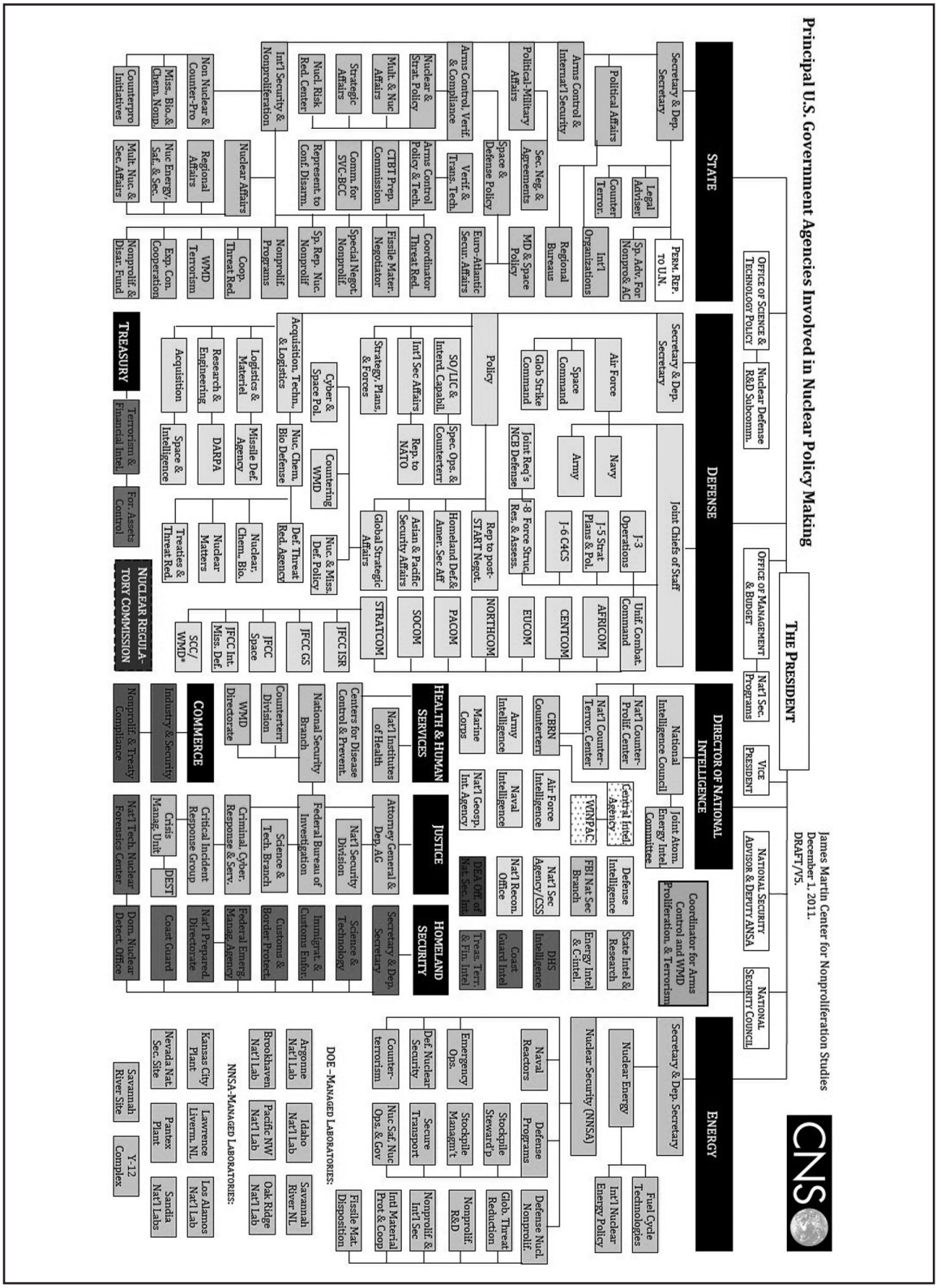


Figure 1. Principal U.S. government agencies involved in nuclear policy

the nation from the threat of WMD. Anything short of high-fidelity integration will result in seams and boundaries between disparate and non-complementary agency plans that could be exploited by a WMD-armed adversary.

Defining WMD

At the root of any successful whole-of-government approach to assessing the WMD threat, there must exist a shared understanding of the term WMD. At present, the definition of the term WMD varies greatly depending on the source.[3] For example, the United Nations defined WMD in 1948 as chemical, biological, radiological, and nuclear weapons or future weapons with similar effects.[4] The Department of Defense defines WMD in terms of the four modalities "chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties..." excluding separable delivery systems.[5] Federal law further expands the definition of WMD by including high explosives.[6] The argument presented in the present study defines WMD as chemical, biological, radiological, and nuclear weapons and includes activities of both state and non-state actors. This delimitation has much to offer, as it includes all traditionally recognized forms of WMD and can be expanded or contracted as technological advancements might indicate without requiring the re-conceptualization of the underlying project.

Defining an "Integrated WMD Threat Assessment"

An "integrated WMD threat assessment" is an intelligence product that incorporates a broad array of information from all available sources into a single picture. It is a compilation of both known and unknown WMD information, showing all the steps necessary for an adversary's employment of WMD against the U.S. or its interests. It cannot end at the point of "known" adversary intelligence, but must continue through successful employment of a WMD. It includes open-source information, classified information, and technical information and fuses this information together to create a comprehensive understanding of the adversary's activities. It includes the people (leadership, technical experts, populations vulnerable to exploitation, and organizations necessary to employ a WMD); infrastructure (medical, industrial, research institutions, communication, transportation, storage, and financial institutions); resources (funding, materials, facilities, precursors, seed stock, process equipment, and delivery systems); and information (internet, academia, libraries, industry, and governmental resources) necessary to create a WMD event. It starts with one actor and shows how that one actor successfully implements a WMD attack. It then adds other actors until all of the actors are included that either have or could produce WMD. The compilation of these pathways will encompass a variety of activities across the globe. This integrated assessment must define what each adversary would target, what modality each is most likely to use against a specific target, and what each might hope to achieve by executing or threatening a WMD attack. Because the assessment portrays success, it does not rely solely on known information. It accounts for looking past the next step and allows those using the assessment to account for an adversary's attempts to surprise the U.S. Collectively, this broad survey of threat information provides an extensive look at the

At the root of any successful whole-of-government approach to assessing the WMD threat, there must exist a shared understanding of the term WMD.

threat that will enable the development of a properly-layered WMD defense. However, this much is clear: The integrated WMD threat assessment thus described is not possible even with the thorough integration of the intelligence community; it requires the integration of the interagency community as well.

Contrary to popular belief, WMD attacks are not easy to perform, and they are not simply random events.

Impediments to Obtaining Accurate WMD Threat Assessments

Contrary to popular belief, WMD attacks are not easy to perform, and they are not simply random events. A WMD attack or even the threat of an attack is the product of an adversary's concerted efforts to achieve specific political objectives. However, because of the near universal condemnation of WMD, it is hardly surprising that states and non-states would go to great lengths to hide their WMD-related efforts. The resulting opacity exponentially increases the magnitude of the challenges associated with producing an accurate WMD threat assessment.

Development of WMD is not the only thing proliferators try to conceal. WMD policies and employment doctrine are also ambiguous. Both doctrine and policy for employing WMD are very closely guarded secrets. Nevertheless, an integrated WMD threat assessment must account for the uncertainties arising from both the knowns and the unknowns of a leader's WMD policy and employment doctrine.

Principles for Formulating an Integrated WMD Threat Assessment

In spite of these not inconsequential challenges, most of the information needed for an integrated WMD threat assessment is already available. The intelligence community has detailed estimates that outline what it believes each WMD adversary is capable of achieving. Because WMD events are low-probability events, adversaries are not likely to attack with WMD or are likely to only attack with toxic industrial chemicals or poisons. This fact constitutes what is called in tactical and operational analyses the "most likely" adversary course of action (COA). Consideration of the "most likely" COA is where most intelligence estimates stop. However, an integrated WMD threat assessment should consider both the "most likely" and the "most dangerous" WMD scenarios—which are not by any means necessarily the same thing. If the integrated WMD threat assessment only shows what is likely to happen, then it will continue to show WMD as very unlikely because that is the most probable scenario. Of course, this is not to suggest that a litany of "the sky is falling" scenarios will serve the national interest. The task is to portray the most dangerous adversary COA without either overinflating or dismissing out of hand the associated WMD risks.

One possible approach would be for interagency players to focus on preventing surprise instead of merely predicting the adversary's most likely activities. Focusing on preventing surprise has the added advantage of accounting for the uncertainty inherent in an adversary's WMD activities, as well as the uncertainty in understanding leadership policy and doctrine for employing WMD. To be useful as a tool for preventing surprise, an integrated WMD threat assessment must look at a broad array of potential actors and WMD modalities.

The easiest method of accounting for incomplete WMD intelligence and unclear understanding of an adversary's WMD policies and doctrine is to template an adversary's success in as many different scenarios as possible. An interagency effort must anticipate

an adversary's success to prevent a surprise WMD event. On this account, one is reminded of the conclusions from the 9-11 Commission. The 9-11 Commission's report stated that one of the biggest mistakes of the intelligence community was a "failure of imagination and a mindset that dismissed possibilities."[7] The model that focuses on both the "most likely" and the "most dangerous" courses of adversary action—a staple for tactical military planning—provides a model for the formation of an integrated WMD threat assessment across the interagency. Often, as interagency organizations build their plans, they spend too much time and lose perspective by fixating on questions of which modality is the most dangerous and which actors are the most capable. What is needed is an integrated WMD threat assessment that accounts for the most likely and most dangerous adversary COAs, regardless of how successful those COAs are assessed to be.

A Practical Approach to Interagency WMD Planning

According to open-source information published by Pro-Con, 21 countries (not counting the U.S.) have known or suspected WMD programs.[8] Figure 2, page 22, is based on the Pro-Con analysis of state WMD programs.

There are 13 known WMD programs in 10 countries, including the eight declared nuclear weapon states and three states that are continuing to destroy their declared chemical weapon stockpiles. The remaining 25 programs in 19 countries are only suspected WMD programs, which illustrates that most countries believed to be pursuing WMD try to keep these programs secret. Thus, not counting U.S. programs, there are 21 countries with 36 known or suspected WMD programs. However, this is only part of the threat.

An integrated WMD threat assessment must account for both state and non-state actors. In 2013, the Director of National Intelligence listed eight terrorist organizations as significant concerns to the U.S. and its interests:

1. Al Qaida in the Arabian Peninsula
2. Al Qaida-inspired home grown violent extremists
3. Core Al Qaida
4. Al Qaida Iraq
5. Al-Shabaab
6. Al-Qa'ida in the Land of the Islamic Maghreb
7. Lashkar-e-Tayibba
8. Hezbollah[10]

There are 13 known WMD programs in 10 countries, including the eight declared nuclear weapon states...

However, the Director of National Intelligence did not list any of these groups as specific WMD concerns—and this in spite of the fact that, in 1998, Osama bin Laden asserted that it was his duty to acquire and employ WMD.[11] It is not definitively known whether the other seven terrorist groups have aggressive WMD programs. Considering the level of effort terrorist groups could go to keep WMD programs secret, it is possible that any of these groups could aspire for, develop, or even employ WMD capabilities without detection by the U.S. and its allies' intelligence organizations. This threat can be expected to continue to increase in the future as chemical and biological technology continues to spread around the globe. This means, all things considered, that all eight terrorist organizations should be accounted for in an integrated WMD

Weapons of Mass Destruction Programs			
	Nuclear	**Biological**	**Chemical**
Known Programs	9	0	4
Known Countries	China France India Israel North Korea Pakistan Russia U.K. U.S.		North Korea (Syria)[1] (U.S.)[2] (Russia)[3]
Suspected Programs	1	8	16
Suspected Countries	Iran	Algeria China Egypt Iran Israel North Korea Russia Syria	Algeria China Egypt India Indonesia Iran Israel Kazakhstan Myanmar Pakistan Saudi Arabia South Africa South Korea Sudan Taiwan Vietnam

[1] Syria's *declared* stockpile has been destroyed. However, reports persist that regime forces continue to employ chlorine gas in contravention of Chemical Weapons Convention obligations.

[2] The U.S. stockpile is currently being eliminated in accordance with obligations under the Chemical Weapons Convention.

[3] The Russian stockpile is currently being eliminated in accordance with obligations under the Chemical Weapons Convention.

Figure 2. Weapons of Mass Destruction Programs[9]

threat assessment.

Based on the definition of WMD presented above, all four of the modalities—chemical, biological, radiological, and nuclear—could be exploited by terrorists. Therefore, the integrated WMD threat assessment must include 24 programs and eight terrorist organizations. Nuclear weapons are a special case. It is acknowledged that most terrorist organizations lack the resources to build a nuclear weapon, and that any nation with a nuclear weapon would be reluctant to share it with terrorists. However, as President Obama has stated, violent extremists with nuclear weapons are among the Nation's greatest threats.[12] Additionally, any intelligence in this area is highly classified. For present purposes, therefore, the intelligence community should assume the most dangerous case and include for all four modalities to illustrate the terrorist WMD threat. Therefore, the new total is 29 WMD actors with 68 potential WMD programs.

The WMD "battlespace" encompasses the entire globe, and WMD proliferators may be expected to seek to develop intricate and obscure proliferation networks in order to avoid detection.

After accounting for the truly global dimension of the WMD battlespace, the next step is to formulate the integrated threat assessment itself. Consider the 29 actors and 68 WMD programs. In order to achieve success, each of these adversaries must accomplish the following six essential tasks for each of the programs:

1. Decide to pursue WMD to achieve desired goals.
2. Develop policy to achieve goals.
3. Select modality or modalities (biological, chemical, radiological, or nuclear).
4. Acquire WMD (purchase, build, or steal).
5. Threaten employment and/or actual employ WMD.
6. Exploit the threat or actual employment of WMD to achieve desired goals.

...all four of the modalities—chemical, biological, radiological, and nuclear—could be exploited by terrorists.

Preparing a complete assessment of the most likely and most dangerous courses of action for each of the 68 WMD programs results in 136 scenarios. Development of 136 detailed scenarios that include all six steps results in a spider web of activities around the entire globe. Again, the primary reason for completing this many permutations is not because any single scenario is likely to occur, but because only by considering the totality of the problem can interagency planners identify critical nodes and develop an integrated plan of multiple layers of defense. Planners can then identify those points where different scenarios overlap, achieving important synergies of effort.

Next, consider the conventional wisdom that "good guys" have to be right 100 percent of the time, but the "bad guys" have to be right only one time to achieve a successful attack. This theory appropriately applies to a single-layered defense. With only one layer in a defensive plan, the "good guys" do have to be correct 100 percent of the time. However, given the scenario in which there are multiple layers of defense, this is not true. For example, if there are 10 layers in the layered defense and each is only 80 percent likely to successfully prevent an adversary's success, the cumulative chance of success for the entire operation plummets to less than one chance in 10 million. If each

layer was improved to 90 percent success, then the adversary's chances of success are reduced to about one chance in 10 billion. This illustrates two important points: (1) the strategy of a layered defense is essential, and (2) in an environment where a single layer of defense is less than 100 percent successful, an integrated approach that employs overlapping interagency defensive layers will strengthen the less than perfect defense layer within a single agency. This approach will allow each layer to perform at its maximum potential.

The U.S. does not need an impenetrable WMD defense. The U.S. needs enough good layers of defense integrated across the interagency communities to reduce the chances of an adversary's success to negligible levels.

The U.S. does not need an impenetrable WMD defense. The U.S. needs enough good layers of defense integrated across the interagency communities to reduce the chances of an adversary's success to negligible levels.[13] The task of the integrated WMD threat assessment, therefore, would be to consider not only the WMD threat writ large, but also the threats that would impinge upon the success of each defensive layer. For example, each time the adversary is able to completely circumvent a single layer, chances of success steadily improve. Similarly, if an adversary determines his chances are only one in a billion, he may adopt a strategy of flooding the field with millions of inexpensive attempts to penetrate the defense. This is similar to the typical lottery held in many states today. The chance that any single person will win the lottery is one chance in a billion. Nevertheless, the credibility of the lottery hinges on the proposition that someone will eventually win the jackpot.

By taking a layered-defense approach that is coordinated across agencies, potential vulnerabilities become less vulnerable due to defensive checks and balances, enabling success where it may have been threatened in the absence of a layered-defense approach. Consider the U.S. investment in radiological detection. Today, funding provides coverage of all of the most likely routes into the country. By taking a layered-defense approach, providing coverage of 100 percent of the border becomes unnecessary. Likewise, efforts to produce the perfect solution in other areas are not necessary. Using the best technology available today at the critical nodes can achieve more success than the never-ending pursuit of a single, perfect, or comprehensive solution. Rather, an integrated WMD threat assessment that truly accounts for both the most likely and most dangerous COAs will favor adding more defensive layers—and adding them more intelligently—from multiple agencies at critical nodes instead of a perfect solution from a single agency or allied nation. Indeed, the approach advocated here is similar to massing combat power at obstacles in order to achieve success. It emphasizes the comprehensive inclusion of all available tools—technical detection, human intelligence collection, all source analysis, law enforcement, non-proliferation regimes, and other methods of massing counter WMD capabilities at the critical nodes—instead of millions (or billions) of dollars on a single perfect detector that might never meet its desired objective.

Creation of an integrated WMD threat assessment provides one additional advantage to the U.S. government. It provides a useful yardstick for measuring the effectiveness of the "active, layered, defense in depth" called for in the WMD strategy.[14] It empowers each agency and department to act within its own

resources and authority while simultaneously illuminating scenarios and critical nodes where improvements can be made, which provides the President and Congress with the ability to see how competing programs within the federal government address specific threats. It also helps identify unnecessary duplication of effort. It avoids trying to determine which adversary actor will succeed first with which of the different modalities, which makes the measure of effectiveness how many scenarios and critical nodes are addressed by agencies and departments across the interagency.

An integrated threat assessment shows how each adversary is most likely to succeed in completing its WMD program, selecting a target, employing the weapon, and exploiting the results of the attack or threat. Because the devil is in the details, this model must be as detailed as possible. If states or terrorists have access to certain materials, facilities, or experts, the integrated WMD threat assessment must include the portions in the template that are known, suspected, and unknown. It must include the entire chain of events from considering the pursuit of WMD, through exploitation of a WMD threat or event. It must be done for all 68 WMD programs and 28 actors with WMD aspirations. Note that this has to be done in spite of the fact that U.S. intelligence is limited and it is ultimately impossible to know with certitude what an adversary's next step will be. This level of detail is important because every situation is different. Fleshing out each potential adversary's different paths will allow the interagency to build a global template of potential paths for WMD. This global template will help account for the fact that the data input to the integrated WMD threat assessment may be either incomplete or inaccurate or both. This template will allow the U.S. to plan for situations for which it may not have all the answers and can only postulate additional WMD-event locations. Only by planning for an adversary's success without perfect intelligence can the U.S. build an adequate defense that is layered across the spectrum of potential adversarial actions.

The next issue is how to build a layered and integrated WMD defensive plan that addresses 136 scenarios. On the surface, this may seem like an almost insurmountable task. However, the solution is to use the 136 scenarios to identify critical nodes. Critical nodes are the points where the 136 scenarios cross paths. A critical node could be, for example, crossing the physical boarder of the U.S. with WMD components or weapons, gaining access to the precursors or seed stock necessary for building chemical or biological weapons, or recruiting technical experts from universities with vulnerable student populations. When considering the activities of 29 actors with a potential of 68 programs, critical nodes can be identified as the spots on the integrated WMD threat assessment where multiple scenarios cross the same point. The more threat scenarios that cross the same point, the more important the critical node becomes. Identifying critical nodes provide a prioritized list of the most important locations for implementing the layered defense. Careful analysis of these critical nodes is important because once the intelligence community correctly identifies these nodes, the entire interagency can—and must—use the same integrated threat assessment to build a layered U.S. defensive plan, which will allow planners to create a layered defense that looks

An integrated threat assessment shows how each adversary is most likely to succeed in completing its WMD program, selecting a target, employing the weapon, and exploiting the results of the attack or threat.

at the entire spectrum of threat activities instead of simply funding the next new idea. Only when the entire interagency uses the same integrated threat assessment can it prevent the exploitation of seams.

Of course, there always exists the potential for a "wild card"—that a country with a known WMD program could simply give a WMD capability to a terrorist organization with instructions to employ the weapon against the U.S. or its interests. To prevent this type of surprise, the intelligence community should supplement the 136 scenarios with additional analysis to show how the most likely proliferation countries might give WMD to specific WMD actors and what guidance these proliferators might give to the actors to achieve mutual goals. Because this is likely to occur where goals overlap, the 136 scenarios already created probably cover these potential activities. For example, if country A chose to give WMD to terrorist B, the most likely targets would be within terrorist B's current operational range and would target locations where terrorist B and country A's interests overlap. The main difference with a "wild card" scenario is the speed with which it could present itself. Therefore, scenarios where terrorist's and WMD state's objectives overlap must include an alternative accelerated timeline in order to account for the "wild card" scenario.

At every turn, planners must not fixate on the integrated WMD threat assessment to the point that it generates "group think." Indeed, there is a danger that analysts could create critical nodes by simply applying the same template to multiple organizations. For instance, recent reports of Ebola outbreaks in Africa could potentially be exploited by every actor seeking a biological weapon capability. In reality, only organizations close to an outbreak with appropriate technical expertise and potential access to research facilities are likely to succeed. For these and many other reasons, each integrated WMD threat assessment must look for the most likely and most dangerous COAs for each individual state and non-state actor as the threat pertains to the U.S. This approach avoids the argument of only addressing one agency's favorite threat or modality. By the same token, the approach suggested herein enables each element of the U.S. interagency to tackle the problem within the context of each agency's respective areas of responsibility and resources.

Conclusion

Because the potential impact of an adversary's use of WMD is so great, the issues are so complex, and so many organizations are involved in the effort, there are no simple solutions. The challenge is compounded by the fact that terrorists and nation states pursuing WMD go to great lengths to hide their efforts. Competing budget priorities, compartmented intelligence information, and concern over encroachments upon civil liberties further complicate the problem.

This much is clear: the U.S. needs a more comprehensive integrated WMD threat assessment in order to account for the uncertainty inherent in tracking adversary efforts to acquire, threaten, or employ WMD. In order to prevent surprise, the intelligence community must prepare a common set of threat scenarios for interagency planners to prepare integrated and layered defenses at critical nodes. Critical nodes are identified by looking at an extensive list of threat scenarios and identifying the locations where multiple scenarios overlap. This method will help to empower interagency planners and enable them to develop an "active, layered, defense in depth."[15] Each agency can analyze its investment strategy to identify the investment level that provides the most capability at critical nodes. It will also enable each agency to avoid the negative effects of diminishing returns on investments focused on achieving a perfect solution at any single node. Only by accepting a common integrated threat assessment can the interagency build multiple, layered defenses without

visible seams that WMD-enabled adversaries can exploit.

The creation of a template with 136 different WMD scenarios is not intended to portray the threat as a high-probability event. It is only intended to provide enough scenarios to allow sufficient planning to prevent surprise. However, in the high-stakes enterprise of counter-WMD planning, avoiding surprise is the single most important key to success. ***IAJ***

NOTES

1 The views expressed herein are those of the author and do not necessarily reflect the official views of the U.S. government or any of its entities.

2 James Martin Center for Nonproliferation Studies, "Principal US Government Agencies Combating Nuclear Proliferation," 2009, <http://cns.miis.edu/stories/090213_wmd _coordinator.htm>, accessed on June 24, 2014, used with permission.

3 W. Seth Carus, "Defining 'Weapons of Mass Destruction,'" Center for the Study of Weapons of Mass Destruction, Occasional Paper #8, revised and updated, National Defense University Press, Washington, January 2012.

4 Ibid.

5 Department of Defense, *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*, November 8, 2010, as amended through January 15, 2014, <http://www .dtic.mil/doctrine/dod_dictionary/>, accessed on January 31, 2014.

6 Federal Bureau of Investigation, <http://www.fbi.gov/about-us/investigate /terrorism /wmd/wmd_faqs>, accessed on February 5, 2014.

7 Thomas H Kean (Chair) and Lee W. Hamilton (Vice Chair), "The 9/11 Commission Report," July 22, 2007, p. 336.

8 Based on ProCon.Org, "26 Countries' WMD Programs; A Global History of WMD Use," used with permission, <http://usiraq.procon.org/view.resource.php?resourceID=000678>, accessed on March 23, 2014.

9 Ibid.

10 J. R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," statement for the record, Senate Select Committee on Intelligence, March 12, 2013.

11 Rolf Mowatt-Larsen, "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" 2010, <http://belfercenter.ksg.harvard.edu/publication/19852/al_qaeda_weapons _of_mass_destruction_threat.html>, accessed on February 17, 2014.

12 The White House, National Security Strategy, 2010.

13 This section was inspired by a similar discussion presented by Michael Levi, *On Nuclear Terrorism,* Harvard University Press, Cambridge, MA, May 2009.

14 Department of Defense, "National Military Strategy to Combat Weapons of Mass Destruction," 2006.

15 Ibid.

Closing the Barn Door: Interagency Approaches to Reduce Agroterrorism Threats

by David F. Grieco

Despite billions of dollars spent in the U.S. on national defense, one key area has been historically overlooked.[1] In the twenty-first century, perhaps the greatest national security threat requiring careful interagency coordination is not in a distant land, but in actuality, quite local. It is a weaponization pathway so deadly that it has been described as more powerful than nuclear weapons, yet equally within the reach of first-world nations and terrorists alike.[2] The danger posed is terrorism aimed not directly at populations, troop concentrations, or buildings, but rather at the vast U.S. agricultural system that millions rely upon both domestically and internationally every day. The U.S. has started on the path of interagency cooperation to address and mitigate agroterrorism vulnerabilities. However, the question at hand is whether the interagency approach is sufficient to fortify this vulnerable sector, or whether this collective response will instead to be too little too late.

Risk Areas and Target Factors

At the highest levels, agricultural terrorism, commonly shortened to "agroterrorism," reflects the deliberate use of biological or chemical means to depreciate, stunt, halt, or destroy an agricultural asset or set of assets. Agroterrorism is not defined by a specific size or the associated value of the damage inflicted; a single incident can be limited to a single herd or crop, or have, perhaps unintentionally, a national or even an international impact. While a single event would likely not shut down the U.S., the cumulative effects of multiple such events could instill severe buckling on the system, especially since the agricultural industry is the country's largest employer, including direct and indirect food production employees.[3]

Agroterrorism, in most cases, is fundamentally an attack against livestock and crops. However, an attack need not be targeted at a farm; merely instilling fear and inducing panic in agriculturally-based economic centers, such as nearby processing and transportation facilities, could still constitute an attack and achieve similarly desired results.[4] Regardless of the source or intention behind the

Mr. David F. Grieco is a chemist at the U.S. Army Research, Development and Engineering Command's Edgewood Chemical Biological Center, where he is participating in the development of the Joint Biological Tactical Detection System. He received a M.S. Degree in WMD Studies as a National Defense University Countering WMD Graduate Fellow.

introduction of a pathogen or contaminant, the large number of potential points of introduction means that no **one** government agency will be able to provide a suite of comprehensive countermeasures and systems for defense.

The three great vulnerabilities present in the American agricultural system are the lack of security measures, livestock susceptibility to foreign animal diseases (FAD), and the frequent, condensed transportation of livestock.[5] An area of particular concern is the protection of livestock, which becomes particularly difficult when considering open pastures, especially those found in the Southwest, where no physical security exists to separate animals from potential perpetrators.[6] Crop susceptibilities add another dimension for consideration in that the pathways for infection increase to seven different categories including fungi, bacteria, viruses, viroids, nematodes, protozoa, and parasitic plants.[7] An interagency effort known as the Strategic Partnership Program Agroterrorism (SPPA) takes cognizant of the fact that human intervention at multiple points across the supply chain, especially at processing and storage facilities, can pose an additional concern if access to these areas is not closely controlled.[8] Moreover, through contamination of seed stock, a would-be agroterrorist could indirectly infiltrate a farm's most precious commodities without ever stepping foot on the farm, bypassing physical security features even if they have been installed.

Regardless of the method of introduction of a pathogen, and whether it is directed against livestock or crops, an even larger and more fundamental issue exists. Determining what exactly comprises America's agroterrorism threats becomes significantly more complex as the result of insufficient interagency coordination. The Department of Agriculture (USDA)/Department of Homeland Security's Animal and Plant Health Inspection Service (APHIS) and the Center for Disease Control (CDC) have different, only partially overlapping lists of threat agents.[9] The lack of coordination among different agencies greatly complicates the cross-referencing task when assessing agricultural risks and threats at the ground level of local farmers.[10]

Another significant interagency challenge pertains to the question of how a response to an agroterrorism event would be funded. The U.S. government does not currently have lines of funding appropriated to pay for the necessary response mechanisms.[11] Even within the existing umbrella for biological defense, including the aptly named Biological Warfare Defense Program that is managed by the Defense Advanced Research Projects Agency (DARPA) under the Department of Defense (DoD), the maintenance of consistent funding levels for such response activities is uncertain.

Agroterrorism, in most cases, is fundamentally an attack against livestock and crops. However, an attack need not be targeted at a farm...

In a contingency operation for rapid response payments, funding would likely be reprogrammed from the Biological Warfare Defense Program portfolio due to its similar scope. Despite being an appropriated program within the Congressional budget process, there is not a level of consistency or reliability; funding has decreased dramatically from an explosion in funding at $164 million in fiscal year (FY) 09 to $30.4 million and $19.2 million in FY12 and FY13 respectively.[12] The single greatest reduction observed was $41.3 million in FY10, demonstrating that the budget could vary as much as 75 percent within one year.[13] As a result, funding would need to be rapidly scrambled from otherwise non-appropriated

funds to make appropriate disaster payments, which could be difficult to assemble in the chaotic aftermath following an incident.

Depending on the manner in which an agroterrorism event is imagined or constructed for hypothetical scenarios, the actual risk present in the American agricultural system varies significantly. Through analysis of historical vignettes, the CDC has expressed confidence that an agroterrorism risk does, in fact, exist, but that it is almost solely limited to livestock. The CDC also acknowledges that crops also face a risk, but assessed that this risk is significantly less probable than an attack against animals; thus, prioritization has left plant pathogens largely unaddressed.[14] Fortunately, this is not a view held universally across the U.S. government, as others have also identified that presently an entire season's worth of crops could be ruined through either pathogens or toxins.[15] Undetected until too late, a simple biological pathogen could devastate a great portion of crops with deadly rapidity. Unless these vulnerabilities, including contamination of feed and animal susceptibility to FADs, are addressed, the U.S. will remain vulnerable to future agricultural emergencies that cannot be easily controlled.

President George W. Bush signed into law a series of efforts to cap the growing biological threat. Known colloquially as the "Public Health Security and Bioterrorism Preparedness and Response Act of 2002"...

Interagency Coordination and Response

In light of the risk posed by agroterrorism, the U.S. government has begun to prepare countermeasures and defenses. Efforts to address agroterrorism increased significantly following the creation of the Department of Homeland Security (DHS) in 2002. At first, agricultural defense funding was heavily aligned toward APHIS, then a part of USDA. Prior to APHIS's realignment under the DHS, annual funding for APHIS constituted upwards of 74 percent of USDA's budget, highlighting the heavy emphasis on the service for detection, prevention, and containment.[16] In addition to surveillance and inspection efforts conducted by APHIS, USDA also turned to the U.S. Army in its attempts to address agroterrorism. USDA's connection to the Army is not as clear as it may appear to the casual observer, as the purpose of the partnership is not to provide medical treatments or products for soldiers following an agroterrorism event, but instead to use existing Army laboratory facilities to achieve a potential synergistic effect between USDA and U.S. Army research goals. Specifically, the USDA has turned to the Biosafety Level-3 (BSL-3) facilities located at Fort Detrick in Frederick, MD, to continue research on select agents of interest, focusing on efforts related to counterterrorism and preparedness operations.[17]

Among the largest—if still not completely adequate—aspects of the government response to agroterrorism are the laws that have been implemented to create a preventive screen to hopefully close avenues through which agroterrorism attacks can occur. In the aftermath of the September 2001 Amerithrax incidents, President George W. Bush signed into law a series of efforts to cap the growing biological threat. Known colloquially as the "Public Health Security and Bioterrorism Preparedness and Response Act of 2002," the law established important protocols for increasing defenses against wide-encompassing areas of the homeland. While this law consists of five sections, only two of them apply to themes relevant to agroterrorism per se; the others

address pathogen containment and water safety.

To hedge against the possibility of pathogens from abroad entering the U.S. through a shipment, the law includes a provision that authorizes the withholding of suspect foods for 20 to 30 days prior to importation.[18] A supplemental effort, implemented to prevent pathogen introduction and assist in inspections at a source of control, has been the introduction of APHIS personnel into more than 27 countries to conduct screening prior to entry at American ports.[19] Two significant limitations are associated with this withholding. First, there must be credible evidence to support the case for the withholding. Second, this is a limited tool intended for preventing foodborne disasters. In order to successfully intercept questionable foods, there must be strong evidence from the intelligence community, and more importantly, timely transmission of this information to the Food and Drug Administration (FDA), which would carry out the withholding.

Even with this legislation firmly in place, loopholes exist through which pathogens can still be introduced into foods. Despite the scope of the legislation, which accords higher precedence to pharmaceuticals than food, there is a mandatory registration process for both foreign and domestic food processing centers, establishing a baseline for food surveillance efforts.[20] The flaw in this approach is that it still presents vulnerability, as farms are not registered in a similar manner. The target in this respect is to combat foreign pathogen threats, which presumes that overseas farms and processing plants would be the intended targets of agroterrorists. This does lend some credence if one believes that international destinations are the primary targets of terrorist interest, but the argument does not hold up sufficiently. Without insider knowledge, it would be nearly impossible for terrorists abroad planning to commit an act of agricultural terrorism to pinpoint which shipments are destined for the U.S. unless they are already packaged and marked as such. The paradox thus created is that products that are clearly labeled and packaged would be prone to screening by APHIS and thus the danger likely mitigated, while those unpackaged materials available for adulteration would not necessarily be destined for shipment to the U.S. If one accepts this argument, the legislation holds more validity, but the risk then shifts to the efficiency of the command chain within APHIS and the intelligence community. However, there is no evidence that there is close coordination between these two communities, creating many opportunities through which agroterrorism threats may slip by.

...the law includes a provision that authorizes the withholding of suspect foods for 20 to 30 days prior to importation.

Beyond pre-importation withholding, the typical timeframe for acceptance upon arrival at an American port is only eight hours; information regarding suspect shipments as determined by the FDA must additionally flow through state and local levels before reaching APHIS personnel, truly limiting the timeframe of opportunity in which to react to an agroterrorist attack.[21] The efficiency needed to achieve significant results within this model becomes nearly impossible to achieve realistically, thus calling into question the likelihood of the government successfully preventing any dangerous shipments. In this example, the well-intentioned effort to respect state jurisdictions falls short, and the muddling through interagency efforts complicates the effort beyond a workable level. Either the U.S. has not received a shipment in which the provisions of the "Bioterrorism and Preparedness Act" have faced a true test, or shipments have not been a target of agroterrorists. Regardless of the case,

the legislation has provided essentially a null impact on the agrodefense front.

Complementary and supportive to the "Bioterrorism and Preparedness Act," a series of Homeland Security Presidential Directives, or HSPDs, were initiated to provide further directives and guidance to the DHS as it was hurriedly created following the 9/11 attacks. The first of these HSPDs with direct application to agricultural defenses is "HSPD 5: Management of Domestic Incidents," issued on February 28, 2003, which mandated the creation of the National Incident Management System (NIMS) as a unified response system following any type of terrorist attack. It designates DHS as the leading activity to oversee and supersede control as incidents progress from a state/local to the national level.[22] The management structure within NIMS theoretically flows in a manner to facilitate a logical and regulated response to crisis incidents, both agriculturally-related and not. Under NIMS, state/local authorities are responsible for response until one of four situations occurs: federal assistance is requested, state/local authorities are overwhelmed in the response effort, an incident has progressed to an interagency/multiagency level, or DHS has been tasked by the President to provide a response.[23] NIMS and a second system, the Incident Command System (ICS), work in tandem to provide a standardized method in the hierarchy and response patterns following a terrorist attack or other disaster; these tools have been implemented within DHS, but also in other agency functions including USDA, APHIS, and the Federal Emergency Management Agency (FEMA).[24]

...Homeland Security Presidential Directives, or HSPDs, were initiated to provide further directives and guidance to the DHS as it was hurriedly created following the 9/11 attacks.

At the surface level, this may appear to be a brilliant demonstration of interagency adoption of policy using common resources; in actuality, the use is mandated across all federal agencies and departments for incident management.[25] In light of this, the actual functionality under the new system is debatable and appears to resemble that of a partially employed system not at full functionality. An incident on the magnitude of September 11, 2001, in a biological terrorism setting would likely challenge the system beyond levels at which it has been previously tested and could overwhelm the system altogether. Although NIMS does caveat its management structure and approach by stressing compatibility to achieve interoperability—which possibly alludes to a responsive system that adapts to different situations—the true gravity of the situation exposes greater issues.[26] Under a universal system in which training should be standardized to provide cohesiveness among the various responding groups, the above approach instead leaves many areas open to interpretation.

For example, although NIMS and ICS are meant to be standardized, response to an agroterrorism incident uses a modified ICS command structure.[27] Those unaware of the variation would be ill-equipped to fully understand the operational approach used in this situation. Similarly, the manpower allocated for agroterrorism response is also greatly expanded beyond normal NIMS operations, calling upon first responders to create and maintain security zones to minimize the access of non-essential personnel to high-risk areas, similar to practices used in chemical decontamination protocols.[28] With large groups and different types of first responders present, those that have not been formally instructed on this structure variation

are highly likely to fall between understanding gaps, with the result being a disjointed response effort.

Following the release of HSPD-5, a second directive, released in 2003, addressed aspects of agriculture protection. "HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection" is meant to identify both perceived risks to the economy and the security of the U.S. as assessed by DHS, interagency partners, and local officials.[29] HSPD-7 attempts to bring the best of different departments together in order to combat different areas of concern, including agriculture; but much like HSPD-9 that would follow, a general lack of understanding of the skill sets available undermines the intent of HSPD-7. The intended result of obtaining experts is instead met with an unequal set of professionals, none of whom have previously worked on the agroterrorism defense mission in this manner. Instead of collaborating with each other, local entities, and private industry to identify best practices as identified in the HSPD, a shallow series of mandatory after-action reports are the only deliverables that have been produced to date.[30] Proper engagement through consultation with experts to understand available capabilities by the President rather than broad grouping based on different department's presumed specialties would work to greatly enhance the end products provided from such interagency efforts. As it is related to HSPD-7, tasking is divided up between DHS, USDA, and the Department of Health and Human Services (HHS), with USDA taking the lead on agriculture and food efforts, and HHS leading the remaining efforts.[31] DHS's role in the effort, presumably that of an overarching lead, is not explicitly stated. Therefore, the likely result of the effort is the stove-piping of time and research efforts rather than a unified approach.

One report that appears to have captured the intent of HSPD-7 is a multi-year series of assessments that occurred between 2005 and 2008 known as the Strategic Partnership Program Agroterrorism (SPPA). As identified in HSPD-7, DHS, USDA, FDA, and a number of local industry volunteers visited agricultural and food service sites across the country to assess agricultural risks and vulnerabilities.[32] The approach used appears to have been inconsistent, and there was a lack of continuity in the manner of sites selected for assessment. The underlying assessment tool for all the evaluations contained in the report was a newly-developed analysis instrument known as Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability, and Shock (CARVER+Shock).[33] The primary issue with SPPA, if it is indeed the envisioned deliverable from HSPD-7, is that extreme variability was identified within the different areas evaluated. Assuming that those who conducted the assessments were agricultural specialists, many of the recommendations exceed the knowledge presumable of generalists unfamiliar with the threats posed, and hence, not trained to develop appropriate agroterrorism countermeasures at their respective facilities. Attempting to cover an entire "farm-to-table" continuum for evaluation, the SPPA report covers eight risk areas within the supply chain: producers (plants), producers (animal), processors/manufacturers, restaurant/food service, retail, warehouse and logistics, and agriculture inputs and services.[34]

An incident on the magnitude of September 11, 2001, in a biological terrorism setting would likely challenge the system beyond levels at which it has been previously tested and could overwhelm the system altogether.

The overarching report structure emphasizes that substantial flaws existed in all eight of these areas and that tampering or introduction of a pathogen could be implemented at multiple points within each process area.

The third of the agriculturally-related HSPD documents, "HSPD 9: Defense of United States Agriculture and Food," released in 2004, attempts to bring agriculture defenses to the forefront. By rescinding Presidential Decision Directive-63 (PDD-63) and identifying agriculture as a "critical node," the 1998 Presidential HSPD-9 emphasized understanding agriculture risks and mandated new state-of-the-art biocontainment facilities.[35] HSPD-9 is an acknowledgement of the need to increase efforts to directly confront and address issues of terrorist attacks via interagency collaboration. In this effort, the Environmental Protection Agency (EPA), HHS, USDA, and the Secretary of the Interior are jointly engaged to mitigate existing vulnerabilities in order to protect the American food system.[36] Like earlier efforts under the "Bioterrorism and Preparedness Act," follow-through and integration of the right elements are required to make such interagency functions a useful value-added; in the absence of this element, they remain a loosely assembled compilation of unlike parts, and the end result is fragmented or, worse, left unaddressed.

The likely result is that agroterrorism defense will not receive the attention it appropriately deserves until after a critical asset has been struck.

Efforts through the National Veterinary Stockpile (NVS) to combat livestock risks through vaccines and the associated National Plant Disease Recovery System (NPRDS) to use more disease-resistant seed varieties for crops that are also contained within HSPD-9 appear well intentioned.[37] Yet without stewardship and an agency directly responsible for their management, they have largely fallen by the wayside within the USDA architecture as miscellaneous programs that are nearly nonexistent in the current budget. The intent would be that different groups of first responders would be able to function cohesively. This goal, however, requires that first responders have the same fundamental understanding of a response organization and the associated hierarchy. In light of the HSPD-5/7/9 series, farms still trail far behind with regard to biological defense. Analysis of available funding documentation reveals that there has been a much greater emphasis on civilian, non-agricultural aspects of biological defense, including the Strategic National Stockpile (SNS), State and Local Preparedness and Response Capability, and the National Hospital Preparedness Program (HPP).[38]

The Future of Combating Agroterrorism

A survey of the available literature suggests that the recommendations provided by the National Research Council of the National Academies have created the baseline upon which all agroterrorism defense efforts have sprouted. In their assessment, three policy recommendations were provided to the federal government: surveillance on a national level for biological agent incidents, establishment of doctrine for response to agroterrorism events, and emphasis on public and community education to assist in surveillance efforts to deter an attack.[39] Supplementing community education are further advocacy efforts to improve the existing training of first responders to improve their ability to assist in the identification of potential animal disease events or improve their response time in the instance

of an event.[40]

In spite of these hopeful signs, and given the country's great reliance on its farms and associated food infrastructure, it is especially puzzling that the overall progress in creating agricultural defenses has remained largely stagnant despite many efforts that have been initiated across the interagency. Of all of the efforts initiated, the SPPA efforts have spawned perhaps the most comprehensive and tangible progress toward meeting and addressing the agricultural terrorism threat. Even so, databases for best practices are spread across DHS's Homeland Security Information Network, USDA's FoodSHIELD, and the Federal Bureau of Investigation's Infragard database, among others.[41] Each advocates its respective database as a "one-stop-shop" for information, but with three independent databases, this statement is far from accurate.

What has been started within the U.S., both government-initiated and non-government initiated, to combat agroterrorism is unevenly distributed at best or dangerously chaotic at worst. That which becomes overly complex unfortunately becomes avoided and disregarded—the exact opposite of what the interagency should be doing with respect to agroterrorism. An underlying idea of "out of sight, out of mind" possibly contributes to this effort, with many leadership decisions vested in organizations far removed from agricultural communities.[42] The likely result is that agroterrorism defense will not receive the attention it appropriately deserves until after a critical asset has been struck. Until the current approach of interagency coordination for addressing agricultural threats is righted, the U.S. is poised on a very dangerous path, as the existing flaws appear ripe for exploitation. Only through substantial reworking and retooling can the system be remedied to provide adequate defenses before it is too late. ***IAJ***

NOTES

1 The views expressed herein are those of the author and do not necessarily reflect the official views of the U.S. government or any of its entities.

2 Simon M. Whitby, *Biological Warfare Against Crops*, Palgrave, New York, 2002, pp. 175–176.

3 Jason B. Moats, *Agroterrorism: A Guide for First Responders*, Texas A&M University Press, College Station, 2007, pp. 6–7; R. Norton, "Food Security Issues: A Potential Comprehensive Plan," *Poultry Science Association*, Vol. 82, 2003, p. 959, <http://ps.fass.org/content /82/6/958.long>, accessed on January 13, 2015.

4 Moats, p. 1; Peter Chalk, *Hitting America's Soft Underbelly: The Potential Threat of Deliberate Biological Attacks Against the U.S. Agricultural and Food Industry*, RAND Corporation, Santa Monica, 2004, p. xii, <http://www.rand.org/content/dam/rand/pubs /monographs/2004/RAND_MG135.pdf>, accessed on January 13, 2015.

5 Johnnie L. Gilpen, Jr. et al., "Agriculture Emergencies: A Primer for First Responders," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, Vol. 7, No. 2, 2009, p. 188, <www.ncbi.nlm.nih.gov/pmc/articles/PMC2995339/>, accessed on January 13, 2015.

6 Frank R. Spellman, *Food Supply Protection and Homeland Security*, Government Institutes, Lanham, 2008, p. 122.

7 Whitby, pp. 24–25.

8 U.S. Food and Drug Administration, "Strategic Partnership Program Agroterrorism (SPPA) Initiative: Final Summary Report, September 2005–September 2008," Silver Spring, MD, 2008, pp. 6–7, <http://www.fda.gov/downloads/Food/FoodDefense/UCM181069.pdf>, accessed on January 13, 2015; Terrence Wilson et al., "Agroterrorism, Biological Crimes, and Biowarfare Targeting Animal Agriculture: The Clinical, Pathologic, Diagnostic, and Epidemiologic Features of Some Important Animal Diseases," *Clinics in Laboratory Science*, Vol. 21, No. 3, 2001, p. 550, <http://agresearch.umd.edu/CANRP/files/6th%20Annual%20Agricultural%20outlook%20and%20Policy%20Conference/Agricultural%20and%20Food%20Security%20Issues.pdf>, accessed on January 13, 2015.

9 Spellman, pp. 104–105.

10 National Research Council of the National Academies, *Countering Agricultural Bioterrorism*, The National Academies Press, Washington, 2012, p. 1.

11 Linda B. Katz (ed.), *Agroterrorism: Another Domino?* Novinka Books, New York, 2008, p. 10.

12 Tara Kirk Sell et al., "Biodefense Funding: Changes from President's Budget to Congressional Appropriations," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, Vol. 10, No. 3, pp. 322–323, <http://online.liebertpub.com/doi/pdf /10.1089/bsp.2012.0042>, accessed on January 13, 2015.

13 Ibid., p. 323.

14 Spellman, pp. 102–103.

15 U.S. Food and Drug Administration, 2008, p. 5.

16 Katz, p. 23.

17 Katz, p. 38.

18 U.S. Food and Drug Administration, "Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Public Law 107-188)," Washington, 2002, pp. 3–4, <http://www.fda.gov/regulatoryinformation/legislation/ucm148797.htm>, accessed on January 13, 2015.

19 Jim Monke, "Agroterrorism: Threats and Preparedness," Congressional Research Service Report RL32521, 2007, p. 48, <http://www.fas.org/sgp/crs/terror/RL32521.pdf>, accessed on January 13, 2015.

20 U.S. Food and Drug Administration, 2002, p. 6.

21 U.S. Food and Drug Administration, 2002, pp. 10–12.

22 Moats, p. 33; The White House, Office of the Press Secretary, Homeland Security Presidential Directive (HSPD)-5, "Management of Domestic Incidents," Washington, 2003, pp. 1–2, <http://training.fema.gov/EMIWeb/IS/ICSResource/assets/HSPD-5.pdf>, accessed on January 13, 2015.

23 The White House, Office of the Press Secretary, HSPD-5, pp. 2–3.

24 Gilpen et al., p. 190.

25 The White House, Office of the Press Secretary, HSPD-5, p. 4.

26 Ibid., p. 3.

27 Moats, p. 31.

28 Ibid., pp. 69–74.

29 The White House, Office of the Press Secretary, Homeland Security Presidential Directive (HSPD) 7, "Critical Infrastructure Identification, Prioritization, and Protection," Washington, 2003, pp. 1739–1740, <http://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1739.pdf>, accessed on January 13, 2015.

30 Ibid., pp. 1741–1743.

31 Ibid., p. 1741.

32 U.S. Food and Drug Administration, 2008, p. 1.

33 Ibid.

34 Ibid., p. 3.

35 The White House, Office of the Press Secretary, Homeland Security Presidential Directive (HSPD) 9, "Defense of United States Agriculture and Food," Washington, 2004, pp. 175–177, <http://www.gpo.gov/fdsys/pkg/PPP-2004-book1/pdf/PPP-2004-book1-doc-pg173.pdf>, accessed on January 13, 2015; Chalk, pp. 1–2.

36 The White House, Office of the Press Secretary, HSPD-9, "Defense of United States Agriculture and Food," pp. 173–174.

37 Ibid., pp. 175–176.

38 Sell et al., pp. 322–323.

39 National Research Council of the National Academies, p. 9; Monke, p. 47.

40 Gilpen et al., p. 193.

41 U.S. Food and Drug Administration, 2008, pp. 14–15.

42 Susan R. Owens, "Waging War on the Economy," *Nature*, Vol. 3, No. 2, 2002, p. 111, <www.ncbi.nlm.nih.gov/pmc/articles/PMC1083981/pdf/kvf043.pdf >, accessed on January 13, 2015.

Securing the U.S. Food Supply:

The Quintessential Interagency Task

by Cindy A. Landgren

The general public puts little thought into the vast, interconnected infrastructure that constitutes the fabric of life in the U.S.[1] Nevertheless, large segments of that infrastructure are susceptible to failure—potentially even catastrophic failure—through both accidental and intentional means. Sometimes it is hard to tell the means by which failure has occurred, especially if the possibility of malicious intent does not receive thoughtful consideration. This is especially true of those things which, although absolutely fundamental to the sustainment of life—the air we breathe, the water we drink, and the food we eat—are mostly taken completely for granted by the average person. Moreover, the U.S. public enjoys a surplus of food availability and almost infinite variety. Nevertheless, the average citizen possesses almost no appreciation of the intricate processes required to bring food safely to the shelves. Hence, the idea that malicious persons could use food as a vehicle for intentional harm is something most people rarely if ever think about, let alone plan to prevent.

In fact, the most definitively documented case of introducing a biological agent in the food supply was one in which the possibility of "biological terrorism" was not even considered initially. In the fall of 1984, a cluster of gastrointestinal illness occurred in the eastern Oregon town of The Dalles.[2] A total of 751 people became ill over a two-week period. During the investigation, the investigators ruled out the possibility of intentional contamination based on the following:

- No one claimed responsibility.
- No motive was apparent.
- No pattern of unusual behavior was apparent to law enforcement.
- No one could find a disgruntled employee in the establishments to which the illness seemed to be traceable.

U.S. Army Lieutenant Colonel Cindy A. Landgren (Ph.D., DVM) serves at the Defense Threat Reduction Agency, where she manages medical and countermeasure science and technology for the DoD Chemical and Biological Defense Program. She is a Countering WMD Graduate Fellow at National Defense University.

- There were repeated attacks of illness.
- Indiscriminate illness involved employees and patrons.
- No event like this had been reported before.
- Hypotheses other than deliberate adulteration of the food supply were more likely.
- The source simply was not obvious either to casual observers or even to trained investigators.

It was not until much later that the motive of attempting to influence the outcome of a local election by disabling the electorate was ascertained. Although the objectives of the attack were not achieved, the perpetrators were successful in that they caused a significant number of illnesses over a short period of time in a town of 10,000 served by only one hospital.

Reflection upon this incident in The Dalles, which serves as the textbook reference case for the adulteration of the food supply chain in America, invites some interesting, pressing, and sobering questions that properly claim the attention of the interagency:

- Is the possibility of intentional contamination properly considered during outbreak investigations?
- Does the motive need to be known to ascertain the fact that adulteration has occurred?
- Does someone need to claim responsibility?
- Just because something has not happened before, does that mean it never will?
- Is "red-teaming" a part of processes that consider different types of scenarios?
- Are resources being applied to preventive measures that could reasonably be expected to have precluded the event from occurring in the first instance?
- Is due consideration given to exclusion criteria that definitively would rule out natural contamination and enable the identification of either accidental or intentional causes?

These tactical-level questions invite a yet more sobering, but no less pertinent, reflection:

Is the U.S. prepared for an intentional attack with wide effect—perhaps even an attack of WMD-like proportion—on the food supply?

It may be compellingly argued that one of the fundamental functions of government is to ensure the safety of basic human essentials, such as the food supply, for all its citizens. However, such a burden is not one that can be borne by any single organization of government alone. Rather, it is the quintessential interagency task.

...the average citizen possesses almost no appreciation of the intricate processes required to bring food safely to the shelves.

The U.S. Food Supply as a WMD Terrorist Target

The system by which food reaches U.S. tables is complicated and provides a wide variety of choices for the American consumer. Food grown in the U.S. may be sold directly to the consumer through local farm stands or may travel long distances for processing, packaging, and marketing. The U.S. food supply includes a wide variety of foods that are imported from around the world, from fresh produce to highly processed packaged products. As the consumer walks through a supermarket of choice, the local farmer's market, or sits down at a favorite restaurant, all of the food being consumed has been touched by a human in some significant

way, and every human encounter with that food introduces the possibility of intentional adulteration.

History provides numerous examples of small-scale attacks on the food supply, such as lacing baked goods with arsenic to kill SS soldiers in a WWII prisoner of war camp...

The food chain is far more diverse than most routinely imagine. Well over 100,000 farms in the U.S. sell directly to consumers.[3] However, the majority of the products on grocery shelves are actually an amalgam of multiple ingredients processed in some way to transform the product into something that will be further prepared in the home or restaurant, such as a cake mix. Still other products are in final form and are ready to eat, such as baked goods or yogurt cups. Similarly, foodstuffs may be imported to the U.S. as ingredient-type products or in consumer-ready form. Regardless of the form in which the consumer ultimately encounters a food product, processes have occurred to get the food into the hands of the consumer, and at each stage of each process, the possibility for adulteration exists. As the interagency works to anticipate terrorist threats to the food supply, four questions present themselves:

1. What threats do current safeguards fail to consider or even imagine?
2. How adequate are current interagency capabilities?
3. How adequate is current food safety policy?
4. How might current management protocols actually heighten risks to the safety of the food chain?

Imagining the "Unimaginable"

History provides numerous examples of small-scale attacks on the food supply, such as lacing baked goods with arsenic to kill SS soldiers in a WWII prisoner of war camp[4], the contaminating of store-bought muffins with *Shigella dysenteriae* type 2 by a disgruntled laboratory worker in a hospital causing 12 casualties, or the lacing of a group meal with *Ascaris suum* eggs (a swine roundworm) by four university students.[5] Nevertheless, it does not tax the imagination to consider that malicious activities like these could be expanded into much larger incidents with far more significant consequences. Technical failures in a process likewise can have large impacts on a centrally-produced ingredient. For example, in 1994, transportation of ice cream mix in a tanker that was not adequately sanitized after carrying liquid, unpasteurized eggs affected an estimated 224,000 people in 41 states.[6] The ensuing investigation revealed that the ice cream company had recently awarded a new contract for the transportation of the ice cream mix. The written procedures for cleaning the trucks were not followed, and routine inspection of the tankers was not completed. The level of contamination in the final ice cream product had only six bacterial organisms in a half-cup serving, but that was sufficient to cause illness. While this single point of failure was essentially an accident due to carelessness, deliberate adulteration of the ice cream would have had similarly widespread affects, and a malicious but imaginative bioterrorist could identify just such an opportunity.

Conventional wisdom assumes the most effective vehicle of biological attack to be an aerosol. However substantial modeling and research have made abundantly clear the difficulty in delivering the particle size and agent that would serve as an effective weapon. Hence, the assumption that a successful biological

attack would likely be delivered by an aerosol, coupled with scientific evidence establishing the difficulties with aerosolization, have led some to conclude that a biological attack appropriating the food supply as a transmission vehicle is so unlikely as not to merit serious consideration. However, that is not sufficient reason to dismiss out of hand the possibility of attack by other means. For example, the oral route for ingesting food-borne contamination is much easier to accomplish and most likely to be disguised as unintentional food contamination. Radiological adulteration of food may also be another surprising but viable venue for terrorists.[7]

To the larger point: actual and hypothetical instances such as these combine to suggest that a different way of thinking about WMD attacks on the food supply is warranted across the interagency–one that strikes a balance between defending against threats that are known and those that are "unthinkable."

Synergizing Interagency Capabilities

Different bureaucratic emphases within the interagency sometimes lead to non-complementary approaches to securing the food supply from terrorist attack. Consider, for example, the distinction between "food safety" and "food defense." Food safety has been a part of the food supply system at least since the advent of the industrialization of food production. The majority of food laws resulted because of incidents that caused harm, such as chemical adulteration. Food defense, on the other hand, embodies a more recent concept that requires a somewhat different set of capabilities and skills. Since 9/11, the emphasis on food defense is lauded in public forums but is proving much harder to execute than one might suppose. The Department of Homeland Security's (DHS) Center of Excellence, the National Center for Food Protection and Defense[8] defines "food safety" as food system reliability, reducing the exposure to natural hazards, errors, or failures in the food system. It defines "food defense" as "resiliency of the food system—reducing the impact of system attacks or catastrophic effects." Other interagency members, such as the Food and Drug Administration (FDA), situate their definitional emphases somewhat differently.[9] However, all of this portends a larger problem: While definitions like these may be meaningful and important to specialists in one agency, the distinctions they seek to capture may not be particularly resonant in the context of another agency's work. As a practical matter, competing definitions can present conceptual gaps and seams ripe for exploitation by WMD terrorists. To counter this, the interagency needs commonly accessible conceptual tools to prevent and detect intentional adulteration of the food supply. Key food defense tools are being implemented, such as coordinated data collection and analysis, food defense plans, and the training of food defense professionals. Nevertheless, significant gaps and seams continue to exist in the system.

Since 9/11, the emphasis on food defense is lauded in public forums but is proving much harder to execute...

Filling Policy Gaps

The food safety policies and regulations have had only minor revisions between 1906 and 2011. Other than name changes in the organizations with responsibilities for different aspects of the food supply, little has changed. Homeland Security Presidential Directive/ HSPD-9[10] was established in 2004 to protect agriculture and food systems from terrorist attacks by developing early warning capabilities, mitigating vulnerabilities at critical production nodes, enhancing screening procedures for

Agency	Responsibility
Food and Drug Administration (FDA)	Food (but not meat) Dietary Supplements Bottled water Seafood Wild game (exotic meat) Eggs in the shell
U.S. Department of Agriculture (USDA)	Grading of raw fruits and vegetables Meat and poultry Eggs, processing and grading Certifying organic production
National Oceanic and Atmospheric Administration	Grading fish and seafood
Environmental Protection Agency	Drinking water Pesticide residues
Customs and Border Protection	Front-line enforcement and referral
Department of Justice	Law enforcement
Federal Trade Commission	Advertising
Alcohol and Tobacco Tax and Trade Bureau	Alcohol

Table 1: Comparison of Selected Agency Responsibilities for Food Safety and Quality[12]

imported and domestic products, and enhancing response and recovery procedures. However, given the enormous scope of defense challenges immediately confronting the DHS, it is easy to imagine that food defense could be easily lost in the maelstrom. The FDA Food Supply Modernization Act (FSMA) of 2011[11], intended as a response to gaps in, among other things, food defense regulations, provides expanded authority for the FDA to mandate recalls and revoke food facility registrations. However, sections have not been implemented due to resource constraints and public comment. Of particular concern are the gaps remaining in the regulatory framework that could pose continued vulnerability to WMD attack on the food supply. For example, under the FSMA, direct marketing was excluded from the food safety provisions. This means that a farmer may sell directly to the consumer, restaurants, or cooperative agreements without oversight. The direct market exclusion is not predicated on business size, and this can be a substantial vulnerability to intentional adulteration. Terrorists do not necessarily have to kill a lot of people to achieve their objectives: Contaminating a shipment of produce that will be distributed in a cooperative may be enough. This is not to suggest that everything needs to be regulated, but rather, that loopholes in the regulations remain and must be closed. Identifying those loopholes will take a concerted whole-of-government approach.

On the other side of the coin is the overlap of regulations to which the FSMA contributes. As previously described, at least 15 federal government agencies have food safety responsibilities (Table 1).

The Government Accountability Office (GAO) has conducted several audits addressing this issue.[13] The findings include major overlaps

Product	FDA	USDA
Red Meat Products	Non-specified red meats (e.g. bison, rabbit, game animals, zoo animals, elk, wapiti, moose)	Cattle, swine, goats, horses, mules, other equine
Poultry	Non-specific birds (wild turkeys, wild ducks, wild geese, emus, ratites)	Domesticated birds (chicken, turkey, ducks, geese, guineas)
Other poultry products	Products containing <2% poultry (wet)	Products containing >2% poultry (wet)
Other meat products	Products containing <3% red meat (wet) and closed-face meat sandwiches	Products containing >3% (wet) and open-faced meat sandwiches
Eggs	Shell eggs, products containing egg products, and other egg processing not covered by USDA (e.g. restaurants, cake mix plants, bakeries) Enforcement of shell egg labels/ labeling	Pasteurized processed egg products, egg processing plants (washing, sorting, breaking, and pasteurizing)
Soup	All soup not covered by USDA	Soup containing >3% red meat or >2% poultry (e.g. chicken noodle)
Other products	Cheese, onion, mushroom, pizza, spaghetti sauces (<3% red meat), spaghetti sauce with mushrooms and 2% meat, pork and beans, sliced egg sandwiches (closed-face), frozen fish dinner, rabbit stew, shrimp-flavored instant noodles, venison jerky, buffalo burgers, alligator nuggets	Pepperoni pizza, meat lovers stuffed-crust pizza, meat sauces (>3% red meat), spaghetti sauce with meatballs, open-faced roast beef sandwich, hot dogs, beef pot pie, chicken sandwich (open-faced)
Exceptions to the above	All foods involved in an outbreak aboard an interstate vessel, plane, train, bus	

Table 2. FDA/USDA Jurisdiction Overlap for Commercial Food Products[15]

in domestic and importation food safety regulations. Many facilities are regulated and inspected by two or more agencies for the same or similar products. For example, jurisdiction for shell eggs is under the FDA, but egg processing is under the USDA. A facility that puts eggs in cartons for the consumer and cracks eggs for liquid use, e.g., as a bakery ingredient, has dual regulatory requirements and inspections. Table 2 highlights overlaps in the industry sector-specific Food and Agriculture Protection Plan.[14] The overlap itself may, in principle, serve to reduce vulnerability to WMD terrorist attack. However, this division of labor consumes resources that almost certainly could be applied more efficiently to the overall task of securing the food supply.

Interagency Management Challenges

The Obama Administration has acknowledged the need to protect critical infrastructure from a broad spectrum of threats. Indeed, the expanse of working groups, plans, conferences, and assessments intended to

provide recommendations for collaboration to protect critical infrastructure is large. As a result, several grand directives have assigned the responsibility for infrastructure protection under single agencies. The Presidential Policy Directive on National Preparedness (PPD-8)[16] directed the development of a national preparedness goal and system. The Secretary of Homeland Security was assigned the responsibility of coordinating the domestic all-hazards preparedness efforts across federal agencies with consultation of state, local, tribal, nongovernmental, private-sector partners, and the general public. The DHS Secretary's responsibilities for critical infrastructure were further defined, but not reduced, with the publication of Critical Infrastructure and Resilience (PPD-21) in 2013.[17] In addition to the coordination of national preparedness, the Secretary is tasked to provide strategic guidance and promote unity of effort. Critical infrastructure is divided into 16 sectors, and DHS is solely responsible for 8 of them. The Food and Agriculture sector is the coordinated responsibility of USDA and the Department of Health and Human Services (DHHS).[18] The National Infrastructure Protection Plan (NIPP) of 2013 is an update to the previous plan of 2009 and acknowledges that "the Nation's critical infrastructure is largely owned and operated by the private sector."[19] While this acknowledgement is important, it makes the job of the DHS Secretary to coordinate and implement the NIPP unimaginably difficult. Moreover, the promulgation of the NIPP does nothing to simplify challenges caused by the fact that the food industry is regulated by 15 federal agencies. Although both the USDA and FDA each developed supporting plans, there is no indication of coordination of the individual plans.

History provides numerous examples of small-scale attacks on the food supply, such as lacing baked goods with arsenic to kill SS soldiers in a WWII prisoner of war camp...

The idea of a single food safety agency has been discussed by analysts[20] and the GAO.[21] The National Academy of Sciences[22] concluded that a single federal food safety agency with a clear mandate, dedicated budget, and full oversight of the entire food supply would eliminate the need for each agency to develop data-collection and risk-analysis expertise. Barring the complete reorganization of the federal food safety construct, an alternate approach is to change the traditional thinking and move to a "One Health" paradigm.[23] This paradigm uses collaboration across multiple disciplines and jurisdictions to look at health problems holistically.

By analogy, a "One Food" paradigm for food defense would include intelligence, risk analysis, regulators, and food scientists. However, the paradigm would not be without implementation challenges. These would include the ability of public health agencies to adapt to globalization, negotiating regulatory differences between federal and other regional agencies, inhibiting interdisciplinary research and collaboration due to stovepipe training and funding, and requiring training for medical, veterinary, and public health professionals in "One Food" concepts. Nevertheless, with proper resolve, all of these challenges can be overcome and should not be used as reasons to not pursue change, even if it must occur incrementally. The improvements in management of a complex system cannot be held hostage by traditional thinking and the concern about the loss of responsibility and funding. "One Food" is one way to make strategic improvements. Another way may be to start over with a whole new organization. Failure to update management models can be observed to one degree or

another in all institutions. However, failure to acknowledge the pressing realities of globalization can radically affect the security of any system in ways impossible to anticipate without conscious, consistent effort.

As pertaining to the task of securing the nation's food supply, the interagency appears to be paused on a plateau. In 2009, President Obama directed the formation of the Food Safety Working Group.[24] In the only progress report of the group, intentional food adulteration is discussed in only two paragraphs, which describe studies conducted or planned to improve food defense. Based on the publically available record, it is not clear whether any substantive activities have occurred since 2011. Whatever the case, it would appear that recognition of the problems that gave rise to the Food Safety Working Group in the first instance have not been accorded such a priority as would provide the impetus for ongoing action that eventually translates into executable policy.

Conclusion

As the interagency moves forward, some of the questions that require further study to develop the knowledge and structure required to mitigate current gaps include but are not limited to the following:

- Has the food supply been adequately "red-teamed" and, if so, were the vulnerabilities considered in risk-mitigation strategies?
- Will the revised food defense regulations prevent a WMD terrorist attack on the food supply?
- Can the new system be operationally and tactically tested?
- What incentives would be more effective for the private sector to maintain food defense?
- Can the loopholes in the new regulations be exploited or abused?
- Are all the stakeholders participating in adaptive deep defense?
- Is the answer to multiple regulatory agencies and overlap of jurisdiction a single food defense agency ("One Food")?
- Will the DHS alone be able to do all that is being asked to protect the nation's food supply?

Countering weapons of mass destruction cannot be confined to the traditional thinking of delivery systems. WMD agents can be delivered in non-traditional ways that few people presently pause to consider—including via the food supply. Limited resources do not allow action calculated to prevent every possible scenario. The assessment of comparatively low risk of a previously unimagined wide-spread attack on the U.S. food supply largely fails to take account of the high consequences that just such an attack could entail. Hence, resources are directed to manage higher-risk possibilities. However, the problem with this approach, particularly for the biological contamination of the food supply, is that the current detection and investigation culture is not capable of distinguishing an intentional incident from an unintentional one. The same biological agents can be used to contaminate a food source and outbreaks are too common to alert suspicion. Terrorists are adaptive and smart. They are averse to failure and will patiently determine a method to achieve their objectives. ***IAJ***

NOTES

1 The views expressed herein are those of the author and do not necessarily reflect the official views of the U.S. government or any of its entities.

2 Thomas J. Torok et al., "A Large Community Outbreak of *Salmonellosis* Caused by Intentional Contamination of Restaurant Salad Bars," *The Journal of the American Medical Association*, Vol. 278, No. 5, 1997, pp. 389–395.

3 U.S. Department of Agriculture, "2012 Census of Agricultural Highlights," August 2014, <www.agcensus.usda.gov>, accessed on January 12, 2015.

4 Ali S. Khan et al., "Precautions against Biological and Chemical Terrorism Directed at Food and Water Supplies," *Public Health Reports*, Vol. 116, No. 1, January–February 2001, pp. 3–14.

5 Ibid.

6 Thomas W. Hennessy et al., "A National Outbreak of *Salmonella Enteritidis* Infections from Ice Cream," *New England Journal of Medicine*, Vol. 334, 1996, pp. 1261–1266.

7 Shannon M. Allen and Peter Leitner, "Attacking Agriculture with Radiological Material—A Possibility?" *World Affairs*, Vol. 168, No. 3, Winter 2006, pp. 99–112.

8 National Center for Food Protection and Defense, <https:// www.ncfpd.umn.edu/about/what-is-food-defense/>, accessed on January 12, 2015.

9 Food and Drug Administration, <http://www.fda.gov/Food/GuidanceRegulation /FSMA/ucm247559.htm#FD>, accessed on January 12, 2015.

10 The White House, Office of the Press Secretary, "Homeland Security Presidential Directive(HSPD)-9, "Defense of United States Agriculture and Food," January 30, 2004, <http://fas.org/irp/offdocs/nspd/hspd-9.html>, accessed on January 12, 2015.

11 Public Law 111-353, "FDA Food Safety Modernization Act," January 4, 2011.

12 Renee Johnson, "The Federal Food Safety System: A Primer," Congressional Research Service, January 17, 2014, <https://www.fas.org/sgp/crs/misc/RS22600.pdf>, accessed on January 12, 2015.

13 Government Accountability Office, 11-289, report to Congressional Committees, "Federal Food Safety Oversight," March 2001; Government Accountability Office, 11-652, report to Congressional Committees, "Homeland Security," August 2011; Government Accountability Office, 12-589, report to Congressional Committees, "Food Safety," July 2012.

14 Department of Homeland Security, "Agriculture and Food: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan," May 2007.

15 Ibid.

16 The White House, Presidential Policy Directive (PPD)-8, "National Preparedness," March 30, 2011, <http://www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf>, accessed on January 12, 2015.

17 The White House, Presidential Policy Directive (PPD)-21, "Critical Infrastructure Security and Resilience," February 12, 2013, <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>, accessed on January 12, 2015.

18 Department of Homeland Security, "National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience," <http://www.dhs.gov/national-infrastructure-protection-plan>, accessed on January 12, 2015.

19 Ibid.

20 Ron Knutson and Luis A. Ribera, "Provisions and Economic Implications of FDA's Food Safety Modernization Act," Agriculture and Food Policy Center Issue Paper 11-1, Texas A&M University, January 2011, <https://www.afpc.tamu.edu/pubs/1/554/IP%2011-01.pdf>, accessed on January 12, 2015.

21 Government Accountability Office, 11-289, "Federal Food Safety Oversight."

22 National Research Council, "Enhancing Food Safety: The Role of the Food and Drug Administration," 2010, <http://www.nap.edu/catalog.php?record_id=12892>, accessed on January 12, 2015.

23 National Research Council, "Improving Food Safety Through a One Health Approach: Workshop Summary," 2012, <http://www.nap.edu/catalog.php?record_id=13423>, accessed on March 30, 2015.

24 The White House, "Federal Food Safety Working Group Progress Report," December 2011, <http://www.whitehouse.gov/sites/default/files/fswg_report_final.pdf>, accessed on January 12, 2015.

Cyber Attacks

The New WMD Challenge to the Interagency

by Quan Hai T. Lu

The Ubiquitous Cyber Threat

The President of the United States recently said that "cyber threat is one of the most serious economic and national security challenges we face as a nation."[1,2] Advances in transistor design and integrated circuits have accelerated technologies exponentially. U.S. civil society's reliance on these modern digital systems has, itself, made the U.S. vulnerable to cyber attacks. Cyber attacks are becoming more sophisticated, making detection and attribution difficult. Simultaneously, the "Internet of Things" (IoT) is growing exponentially in the U.S., making every citizen vulnerable to a cyber-attack. Computing and networking systems are vulnerable because integrated circuits and processors are complex—making subversive counterfeit microchips easily replaced and nearly impossible to detect; internet anonymity is pervasive; the building blocks of software are open-sourced or developed by third parties; widespread commercial-off-the-shelf (COTS) software and hardware are manufactured with low or no concerns for security; foundries for microchip manufacturing are located overseas; lines of codes for software now number in the tens of millions and are growing; integrated circuits have over two billion transistors and are also growing; testing and verifying all systems for vulnerabilities is infeasible if not impossible; and development and production processes are now automated—relying on third-party or open-source libraries for hardware and source code.[3]

The IoT links individuals' daily lives to that of the internet. This interconnectedness between people and cyberspace gives criminals, extremists, and adversary nation-states a vector to target individuals, private and governmental organizations, and U.S. civil society as a whole, and, in the

U.S. Army Major Quan Hai T. Lu is the Deputy Chief of Systems Vulnerability & Assessment at the Defense Threat Reduction Agency. He served as a company commander with the 82d Airborne Division in support of Operation Iraqi Freedom. He holds a M.S. degree in nuclear engineering and is a Countering WMD Graduate Fellow at National Defense University.

process, it has inspired a fear of the unknown. In short, cyber is the new weapon of mass destruction (WMD) threat, and addressing it will require marshalling the resources of the entire interagency.

The methods and means may be different, but a cyber attack on chemical facilities, biological research labs, nuclear power plants, and the nuclear command and control nodes is, in important ways, effectively equivalent to an adversary using WMD. Cyber attacks causing an explosion at a chemical factory and releasing toxic industrial chemicals/toxic industrial materials (TICS/TIMS) into the surrounding environment may have the same physical and psychological effects as chemical weapons. Similarly, cyber attacks on nuclear power plants that cause a reactor meltdown and release harmful radioactive material may cause psychological and economic impacts similar to a radiological dispersal device (RDD). Genetic information for biological weapons stolen through cyber attacks from bioresearch facilities may accelerate adversaries' ability to acquire or develop biological WMDs. Insider cyber attacks on nuclear command and control systems may result in an unintentional detonation of a nuclear weapon or the disablement, disruption, and destruction of critical systems during a national emergency. The approaches and devices are nontraditional, but cyber attacks on chemical, biological, nuclear power, and military nuclear command and control facilities can have effects comparable to those of a WMD.

Cyber attacks on other U.S. critical infrastructure can also cause mass damage and casualties. For example, an attack on the power grid that stops the supply of power for a long time over a wide area may cause a humanitarian crisis. Cyber attacks on commerce may cause hundreds of billions of dollar in damages, hurting people at every socioeconomic level. Cyber attacks on one or more nodes in the complex system of infrastructures that sustains the U.S. may massively disrupt—or perhaps destroy—the conduct of U.S. civil society. Indeed, damages resulting from a successful cyber attack on critical infrastructure can be worse than some WMD attacks.

Because of the comprehensive nature of the cyber threat, the interagency cannot ignore the possible WMD-like consequences that a cyber attack could pose.

The cyber threat is not lurking somewhere over a distant horizon; it is here. News reports about a security breach or cyber attacks occur daily. Everything is connected to the internet or is in the process of being connected, and a cyber attack on these interconnected systems has the potential for WMD-like consequences. Millions of electronic devices transformed U.S. civil society into a world economic and military superpower in the latter half of the twentieth century. Trillions of devices—from planes, trains, and automobile to thermostats, smart watches, and everything in between—are increasingly getting connected to the internet. Because of the comprehensive nature of the cyber threat, the interagency cannot ignore the possible WMD-like consequences that a cyber attack could pose. Technology is advancing at an exponential rate, rendering traditional defensive measures or even simple legislation remedies to protect U.S. interests inadequate to the threat. Even if adequate, both are liable to become obsolete before they can be effectively implemented. A defensive posture alone is inadequate to protect the U.S. against cyber attacks because the U.S. cannot defend everywhere at all times. A determined adversary will only need to find one weakness and concentrate its resources to conduct a successful cyber attack. Hence, interagency

partners—and not just the Department of Defense—must consider their respective roles in both cyber-defensive and cyber-offensive operations.

A cyber attack that successfully shuts down the electrical grid for prolonged periods over a large geographic area may have WMD-like consequences.

The U.S. Electric Grid

A cyber attack that successfully shuts down the electrical grid for prolonged periods over a large geographic area may have WMD-like consequences. The vulnerability of the national electric grid to cyber attack is not a new revelation. The electric grid is the U.S. technological center of gravity. Transnational extremists and nation-states whose aims are to disrupt or destroy U.S. civil society have many ways to attack this U.S. center of gravity. In particular, the vulnerability of the electric grid industrial control systems (ICS) to cyber attacks and other critical infrastructures has given U.S. adversaries a relatively easy way to disrupt or destroy U.S. civil society. The outages could severely disrupt the delivery of essential services such as communications, food, water, waste water removal, health care, and emergency response. Moreover, cyber attacks—unlike traditional threats to the electric grid such as extreme weather—are unpredictable and more difficult to anticipate, prepare for, and defend against.

The Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works across the interagency "to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures."[4] In 2012, the ICS-CERT responded to 198 cyber incidents. More than 41 percent of these incidents involved the energy sector, particularly electricity.[5] Thwarting these attacks will require effective information sharing among interagency partners and state and local agencies working over a dispersed area, in addition to close collaboration with private sector entities.

The U.S. Chemical Industry

Chemical facilities share the same cyber-network commonalities as other U.S. critical infrastructures. Their industrial control systems have the same network vulnerabilities that can be exploited by adversaries. From 2006 to 2009, the Government Accountability Office found a 400 percent increase in cyber attacks on chemical facilities.[6]

The ubiquitous reliance on TICs/TIMs and their proximity to the civilian population make the chemical industry a target for terrorist hackers. A recent study found that one in three American schoolchildren attend school within the danger zone of a hazardous chemical facility. Some 19.6 million children in public and private schools in forty-eight states are within the vulnerability zone of at least one chemical facility, according to data the facilities provided to the Environmental Protection Agency.[7] In 2006, Congress established the Chemical Facility Anti-Terrorism Standards program to help regulate high-risk chemical facilities. However, in 2013, a massive chemical explosion that killed 15 people and injured another 226 at a fertilizer plant in the town of West, Texas, showed that the speed with which

the DHS is able to inspect high-risk chemical plants is inadequate.[8]

A cyber attack on chemical facilities designed to release TICs/TIMs is no different in effect than using chemicals in warfare or terrorist attacks. In fact, the effect might be greater, as the affected population is likely to be almost entirely unprotected. For example, hydrogen cyanide gas released from a deliberately staged industrial fire may cause severe respiratory distress to an unsuspecting civilian population. Hydrazine released in an improvised explosive device can cause skin burns and blisters. To take a historical example, the 1984 methyl isocyanate accident in Bhopal, India, killed thousands and injured over a hundred thousand civilians.[9] The triggering and dispersal method may be different, but the consequence of releasing TICs/TIMs could result in the same WMD-like consequences.

The Conventional Energy Sector

U.S. petroleum and gas systems are also vulnerable to cyber attacks. Vulnerabilities exploited in petroleum and gas facilities abroad presage possible similar exploitations in U.S. facilities. For example, the data-destruction attacks on Saudi Aramco and on Qatar's RasGas gas company in 2013 represent a major shift from cyber spying on oil and gas companies to more widespread destruction of their operations.[10] In June 1982, the Central Intelligence Agency (CIA) was alleged to have caused a Siberian pipeline to explode with a so-called logic bomb. The target was a Soviet pipeline and the resulting explosion was detected by U.S. early warning satellites.[11] The covert operation sabotaged the pipeline's control systems with malicious code. Even though the attack caused no direct casualties, harm came to the Soviet economy.[12] Coupled with the Soviet's weak economy and U.S. military build-up, one could argue that the cyber attack contributed to the fall of the Soviet Union. More recently and closer to home, in March 2012, the DHS reported ongoing cyber intrusions among U.S. natural gas pipeline operators.[13] A successful cyber attack on the U.S. petroleum and gas distribution and production system could cause significant harm to the U.S. economy.

The U.S. Health Care System

On August 18, 2014, one of the largest U.S. hospital groups reported that it was the victim of a cyber attack from China. Personal data including Social Security numbers belonging to 4.5 million patients were stolen in the largest cyber attack recorded to date by the U.S. Department of Health and Human Services.[14] Hospitals are soft targets where a cyber attack can cause a lot of damage easily.

A cyber attack can shut down an entire hospital network by threatening information security, system functionality, or device operation. For example, a patient receiving chemotherapy for cancer attends a therapy session where an automated pump administers the prescribed chemo. A cyber attack causes the routine automated procedure to spike the dose of the chemo into the patient's system, causing irreversible harm. The malfunction of one of the pumps puts in question the reliability of the remaining pumps. Meanwhile, the cyber attack also disrupts or halts normal hospital operations. New patients cannot be admitted and current patients' information is inaccessible. Now imagine similar cyber attacks occurring during or as part of a mass casualty event. The complex attack would cause mass fatalities.

A cyber attack can shut down an entire hospital network by threatening information security, system functionality, or device operation.

Nuclear Reactors

Cyber attacks that result in release of significant amounts of radioactive material may cause psychological and economic impact similar to that of an RDD. The number of cyber attacks on nuclear power plants is increasing at an alarming rate.[15] Radiological dispersal—whether from a bomb or a power plant explosion—may have the potential to cause significant loss of life, radiation casualties, lasting psychological trauma, and extensive property damage and contamination that will have lasting effects. Radiation released into the environment likewise has the potential for great harm. Even if a cyber attacker's objective is not to cause physical harm per se, the attacker still could inflict economic catastrophe on a populace worried with the "How clean is clean?" problem in the aftermath of a radiological release. Moreover, cyber attacks not calculated to cause physical harm could still result in the theft of proprietary information that could be used in later attacks. An increase number of attacks with few or no effects may simply be a case of hackers perfecting their skill or probing for vulnerabilities as they wait for a more opportune time to inflict substantial damage. The motives for attacks are elusive and have as many possible permutations as there are attackers. The rationale for why a disaster has yet to occur from a cyber attack is just as elusive. Nevertheless, the already-known certainties surrounding possible cyber attacks against nuclear reactors require the interagency apparatus to confront the cyber threat vigorously.

The computer systems at the National Nuclear Security Administration (NNSA) are under continuous cyber attacks. The NNSA experiences nearly six million hacking attempts daily...

The U.S. Nuclear Weapon Enterprise

U.S. Air Force General Robert Kehler, former Commander of the U.S. Strategic Command, stated in a 2013 Senate hearing that he was very concerned with the cyber-related attacks on the U.S. nuclear command and control (NC2) and weapon system.[16] Much of the NC2 system is analogous to the systems that control nuclear power plants. Even though the point-to-point and hard-wired nature of the system makes it resilient to external cyber-attacks, the system is still vulnerable to insider attacks.

A possible indirect effect of a cyber attack is the theft of nuclear weapons designs that, in turn, can advance an adversary's capability to threaten the U.S. For example, in April, 2013, the Department of Energy's Oak Ridge National Laboratory was successfully hacked and several megabytes of data were stolen.[17] The computer systems at the National Nuclear Security Administration (NNSA) are under continuous cyber attacks. The NNSA experiences nearly six million hacking attempts daily, thousands of which are categorized as "successful." Even without causing significant damage, the NNSA has already expended nearly $150 million just to identify and mitigate cyber attacks.[18]

Cyber attacks can also indirectly impact NC2 and U.S. weapon systems. The ability to maintain communication between the President and intercontinental ballistic missile (ICBM) installations, nuclear ballistic submarines (SSBNs), and nuclear bombers relies on a series of networks that are vulnerable to cyber attacks. The system relies on a communication and electrical backbone that a catastrophic cyber attack could disrupt or destroy for a prolonged period and thus have a profound effect on the U.S. ability to conduct its nuclear command and control.

Water, Food, and Agriculture Infrastructure

The risk to the U.S. posed by cyber attacks with the intention to harm consumer confidence in the U.S. food, water, and the agricultural system can cause severe damage and have large economic impact. In theory, cyber attacks on the food, water, and agricultural system are less costly and have a lower technology threshold than traditional WMD. Targets are more vulnerable, and the impact from a successful cyber attack may be more significant. The cost, lower technology barrier, and vulnerability of targets may make cyber attacks against the U.S. food, water, and agriculture system more likely than other kinds of WMD threats, thus requiring special interagency attention to protect against such attacks.

Similar to other U.S. critical infrastructure, the water and wastewater utilities rely on a network of computers and automated data acquisition and control systems to operate and monitor them. The delivery of potable water to hundreds of millions of people has become, like many other conveniences, routine. Prolonged interference in the delivery of the water or removal of wastewater may precipitate a severe environmental issue. A cyber attack that interferes with the purification process—either leaving the water under or over treated—may result in contaminated water being delivered to the local population and cause a significant public health problem. A cyber attack that interferes with the distribution of water or wastewater removal could likewise lead to an overflow of sewage in public waterways and drainage systems. An attack in a drought-stricken area may exacerbate the problem and have tremendous economic implications. Successful cyber attacks that interrupt or halt the delivery of potable water or removal of wastewater for prolonged periods over a wide geographic area may have WMD-like consequences.

The future of food and agriculture is in automation via large-scale robotics. Envision dozens or hundreds of robots with thousands of digital sensors monitoring, predicting, cultivating, and extracting crops from the land. The automation also produces meats genetically designed and grown from test tubes—completely independent of a living animal. Working with little or no human intervention, the automated system feeds the hundreds of millions. Implementation of the systems on a limited scale is already underway.[19] Now imagine a cyber attack that alters the genetic makeup of the meat to sicken the consumer or to destroy the crops. The cyber attacks would starve millions. The growing reliance on the automated systems—all vulnerable to cyber attacks—has the potential of producing mass damage and disruption to U.S. civil society.

The growing reliance on the automated systems—all vulnerable to cyber attacks—has the potential of producing mass damage and disruption to U.S. civil society.

The Task Ahead

Some critics argue that cyber attacks that cause WMD-like consequences may not be that easy and that technology is keeping pace to counter the problem. On the contrary, cyber attacks are relatively easy when compared to the increasingly sophisticated security software required to protect systems. Figure 1 (pg. 54) shows the exponentially growing complexity required to protect systems versus the relative constant size of malicious software.

With respect to hardware, the trend is just as troubling. Integrated circuits have over 2 billion transistors, and this number doubles every

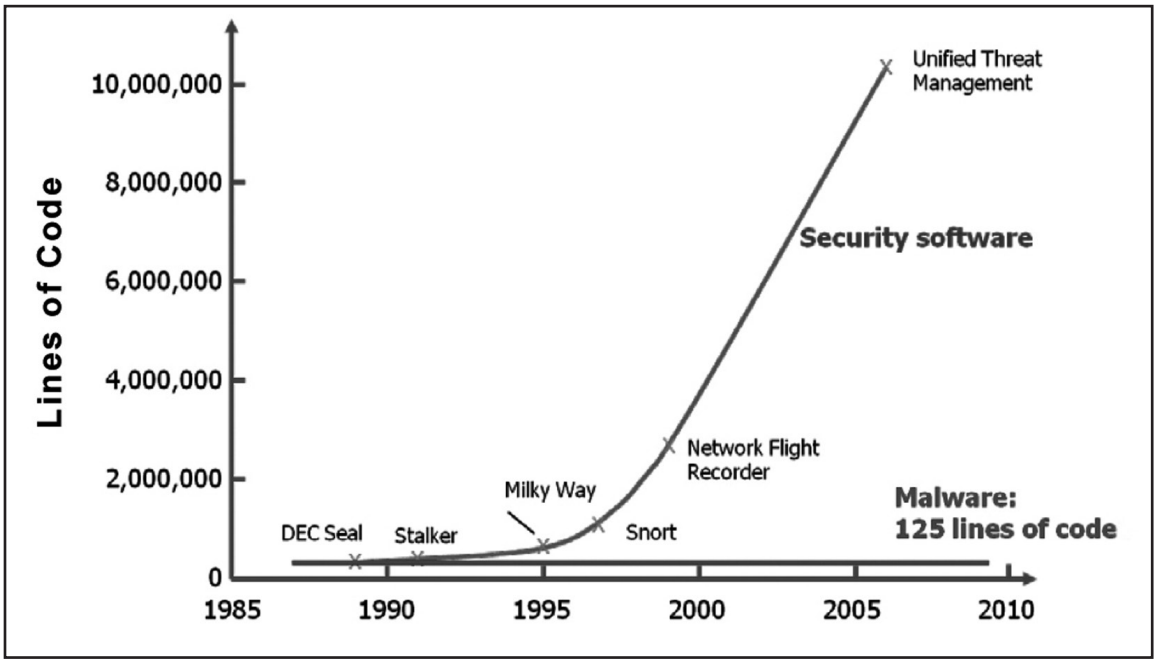


Figure 1: Complexity of Defensive Code vs. Offensive Code[20]

two years. Moreover, manufacturing the chips without flaws is nearly impossible. The flaws—whether accidental or by design—make modern IT systems built around the integrated circuits vulnerable to cyber attacks. Modern IT systems are ubiquitous in U.S. critical infrastructure. A well-resourced and determined adversary will be able to exploit the flaws and could cause WMD-level damage and fatalities.

Some may also argue that if the U.S. truly were vulnerable to cyber attacks that have WMD-like consequences, adversaries would have already attempted a catastrophic attack. In point of fact, attacks on the U.S. critical infrastructure occur routinely, and terrorists have announced their intention of using WMD against the U.S. Conducting a WMD-like attack through cyberspace would be an attractive option—providing a certain level anonymity while having plenty of media appeal. Adversaries, such as states or terrorists, could launch attacks and cause severe physical and psychological damage without leaving their safe havens.

Several plausible explanations may explain the lack of a successful cyber attack that would qualify as cyber terrorism—let alone a WMD-like attack. Many analysts believe that transnational terrorists lack the technical know-how to carry out a sophisticated WMD cyber attack. Sophisticated cyber attacks require a level of software literacy that may be beyond the capabilities of current terrorist cells. However, a determined terrorist cell may eventually bridge the capabilities gap by recruiting more computer-savvy extremists or by developing the capability themselves. Naturally, the interagency cannot wait until such a time to marshal its resources. It may also be that the U.S. has yet to face a WMD-like cyber attack because nation-states that have the means to do so are deterred by fear of U.S. instruments of power, including conventional and nuclear retaliation. Finally, the most probable reason why the U.S. has yet to experience a crippling cyber attack is because adversaries, with the capability and means to inflict mass death and casualties to the U.S., would rather steal from

the wealthiest nation in the world. Billions if not trillions of dollars in intellectual property, trade secrets, and military technology—including information that could accelerate adversaries' ability to develop or acquire WMD—have been lost as the result of cybercrime. Some economists have called it the greatest transfer of wealth in history.[21]

The Pentagon, in an annual report on China, directly charges that Beijing's government and military have conducted computer-based attacks against the U.S., including efforts to steal information from federal agencies. Hackers associated with the Chinese government broke into the computers of airlines and military contractors over 20 times in a single year, according to the U.S. Senate. The Senate report alleged that cyber attacks were targeted at systems tracking movement of troops and equipment. They included breaking into computers on a commercial ship and uploading malicious software on to an airline's computers.[22]

To characterize the point another way, a cyber attack that causes WMD-like damages is a "black swan event." Made famous by Nassim Nicholas Taleb, [23] a "black swan event" is a highly improbable event that has a significant impact. Events such as the creation of the internet and the attacks on 9/11 are examples of such events. No one could have predicted how the internet would transform the U.S. economy, military, and society. Cyber attacks that cause WMD consequences are difficult if not impossible to forecast in terms of the precise time or place they might occur. In some cases, critics are simply unaware or biased against the idea that cyber attacks and WMD are increasingly interconnected in the twenty-first century and pose a significant threat to the U.S. Nevertheless, as argued above, the possible WMD-like consequences of cyber attacks are sobering possibilities that the interagency must consider with all due gravity.

Similar to the Y2K problem at the turn of the present century, the whole of government will need to work together to deter, defend, and mitigate against sophisticated cyber attacks. Unlike Y2K, the threat posed by cyber attacks will be a persistent threat that the U.S. must be vigilant in defending against. In principle, catastrophic cyber attacks are preventable. This much, however, is certain: Left unchecked, the attacks may have WMD-like consequences—billions of dollars in damages, thousands of lives in jeopardy, and military operations compromised. The interagency, working with state and local agencies and in cooperation with the international community, can mitigate the risk and impact of cyber attacks. DoD and DHS should jointly develop a comprehensive plan to handle a catastrophic attack should one occur. In addition, government organizations should also share lessons learned across the interagency, both vertically and horizontally. Placing greater emphasis on offensive measures to prevent cyber attacks will also be necessary. All interagency partners should continue to invest in people, organizations, and technologies to build and maintain a robust cyber-security capability. No one strategy, no single organ or level of government, no one piece of technology, and no one person can prevent and deal with the consequences of a catastrophic cyber attack on U.S. critical infrastructure. ***IAJ***

NOTES

1 The views expressed herein are those of the author and do not necessarily reflect the official views of the U.S. government or any of its entities.

2 Barack Obama, "Remarks by the President on Securing our Nation's Cyber Infrastructure," White House, Washington, May 29, 2009, <http://www.whitehouse.gov/the_press_office /Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure>, accessed on January 12, 2015.

3 Defense Science Board, "Resilient Military Systems and the Advanced Cyber Threat," <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>, accessed on October 10, 2014.

4 Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, <https://ics-cert.us-cert.gov>, accessed on January 8, 2015.

5 "National Electric Grid Remains at Significant Risk for Cyber-Attacks," *Info Security*, <http://www.infosecurity-magazine.com/news/national-electric-grid-remains-at>, accessed on October 14, 2014.

6 Chemical Sector Coordinating Council and the Department of Homeland Security, "Securing Industrial Control Systems in the Chemical Sector, Roadmap Awareness Campaign —A Case for Action," <http://www.dhs.gov/xlibrary/assets/oip-chemsec-case-for-action-042011.pdf>, accessed on December 8, 2014.

7 "DHS Slow to Inspect High-Risk Chemical Plants," Homeland Security News Wire, <http://www.homelandsecuritynewswire.com/dr20140423-one-in-ten-american-schoolchildren-in-school-near-risky-chemical-facility>, accessed on December 2, 2014.

8 Ibid.

9 Richard Davies, "Bhopal Still Haunts Union Carbide 30 Years Later," ABC News, <http://abcnews.go.com/blogs/business/2014/12/bhopal-still-haunts-union-carbide-30-years-later>, accessed on December 2, 2014.

10 Kelly Jackson Higgins, "Destructive Attacks on Oil and Gas Industry a Wake-Up Call," <http://www.darkreading.com/attacks-breaches/destructive-attacks-on-oil-and-gas-industry-a-wake-up-call/d/d-id/1140525?>, accessed on November 13, 2014.

11 "Are the Mouse and Keyboard the New Weapons Of Conflict?" *The Economist*, <http://www.economist.com/node/16478792>, accessed on January 16, 2014.

12 Gus W. Weiss, "The Farewell Dossier," <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm>, accessed on January 16, 2015.

13 Paul W Parfomak, "Pipeline Cybersecurity Federal Policy, " Congressional Research Service, August 16, 2012.

14 Jim Finkle and Caroline Humer, "Community Health Says Data Stolen in Cyber-Attack from China," <http://www.reuters.com/article/2014/08/18/us-community-health-cybersecurity-idUSKBN0GI16N20140818>, accessed on December 3, 2014.

15 Mark Holt, "Nuclear Power Plant Security and Vulnerabilities," Congressional Research Service Report, No. RL34331, Washington, 2014, <http://fas.org/sgp/crs/homesec /RL34331.pdf>, accessed on January 16, 2015.

16 General C. Robert Kehler, USAF, Commander, U.S. Strategic Command, statement before the Senate Armed Services Committee, 2004, <http://www.armed-services.senate.gov /imo/media/doc/13-09%20 -%203-12-13.pdf>, accessed on January 16, 2015.

17 "U.S. Nukes Face Up to 10 Million Cyber Attacks D," *US News*, <http://www.usnews .com/news/ articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily>, accessed on November 6, 2014.

18 Ibid.

19 Michell Zappa, "15 Emerging Agriculture Technologies That Will Change the World," *Business Insider*, <http://www.businessinsider.com/15-emerging-agriculture-technologies-2014-4>, accessed on January 16, 2015.

20 Department of Defense, Defense Science Board, "Resilient Military Systems and the Advanced Cyber Threat," <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems .CyberThreat.pdf>, accessed on October 10, 2014.

21 "NSA: Cybercrime Is 'the Greatest Transfer of Wealth in History'," ZDNet, <http://www.zdnet.com/ article/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history>, accessed on December 8, 2014.

22 Kehler.

23 Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, Random House, New York, 2007.

The Interagency Challenge of *Biosecurity* in Dual-Use Research

by Matthew J. Moakler

On October 17, 2014, the White House Office of Science and Technology Policy announced a funding pause for "gain-of-function" research (i.e., research that increases an organism's ability to cause disease) in order to conduct a study to develop a new federal research policy.[1] This announcement is the latest in a long history of U.S. policies intended to mitigate the risk of advancements in the life sciences contributing unwittingly to a biological weapon (BW) program. While the intention to protect U.S. citizens from a BW attack may be noble, biosecurity policies and regulations appear to be implemented as reactions to discreet events without a comprehensive strategy to address potential future threats. This latest decision raises many questions about what must inform a discussion of the interagency's biosecurity task:

- Who can best determine whether specific biological research can contribute to BW development?
- What is the balance between advancing life-saving techniques and protecting the population from a BW attack?
- How do different biosecurity stakeholders interact with each other?
- Who gets the final say on allowing research to go forward?
- What measures should be taken to prevent the misuse of life science research?
- Who should have the responsibility to enforce such measures?

The urgency of these and similar questions becomes apparent in view of the fact that the pace of advancement in the life sciences is expected to increase not only in the realm of existing

U.S. Army Lieutenant Colonel Matthew J. Moakler serves at the International Security and Nonproliferation Bureau, Department of State. He holds a M.S. degree in biodefense and is a Countering WMD Graduate Fellow at National Defense University.

technologies, but also with the introduction of new technology, techniques, and venues for conducting research—including experiments conducted by do-it-yourself researchers in home laboratories.[2] In light of these expectations, it seems clear that those most familiar with the advancements in the life sciences should play a larger, more formal role in the indispensable allied task of biosecurity. Neither life science professionals nor security professionals fully possess the wide range of tools necessary to protect the nation from the threat of BW. Hence, life science, when viewed as a profession, should play a larger role in the task of biosecurity. Understanding the extent of the life science profession's role in the task of biosecurity will lead to more informed interagency discussion about ways to mitigate the risks of misuse of biology.

The idea of a "profession" itself involves having specially qualified practitioners who can deal in concrete ways with an abstract body of knowledge essential for accomplishing a specific task for the good of society. Additionally, the jurisdiction of a profession does not always have clear lines of separation from other professions that have a stake in the same task. This is especially true in the case of disciplines, like biosecurity, whose very name suggests competing jurisdictional claims. Moreover, biosecurity is a term that has different meanings depending on the community using the term.[3] It can refer to very specific threats, such as protection for "plant and animal health" and "biodiversity"; protection against bioterrorism; and "oversight of dual-use research."[4] Conversely, it can refer, as the National Academy of Sciences (NAS) defines it, to "security against the inadvertent, inappropriate, or intentional malicious or malevolent use of potentially dangerous biological agents or biotechnology, including the development, production, stockpiling, or use of biological weapons as well as natural outbreaks of newly emergent and epidemic diseases."[5] Underlying all of these definitions, however, is the problem posed by "dual-use research," namely research "intended for civilian application that can also be used for military purposes."[6]

Neither life science professionals nor security professionals fully possess the wide range of tools necessary to protect the nation from the threat of [biological weapons].

The following analysis focuses on the division of professional labor as it applies to the task of biosecurity in dual-use research. The task of biosecurity is caught between the competing professions of national security and life science research. For the purposes of this discussion, the relevant security professionals are composed of U.S. government policymakers on the White House Staff, administrators at the National Institutes of Health, and law enforcement professionals who have roles in regulating biological research. The life science profession, as it applies to the task of biosecurity, is composed of principal investigators, university administrators, and academics that are at the cutting edge of research intended to exploit the natural processes of living organisms for the benefit of society—many of them recipients of federal research grants from throughout the interagency.

The Current Biosecurity Management Approach

For the past several decades, the U.S. government security profession has primarily claimed the task of biosecurity by imposing a series of regulations. With the pace of advancement in the life sciences, government regulations characteristically lack the flexibility

to anticipate whether potential threats may develop as the science matures. Current legislation and the related regulations should balance protection from the threat without being "overly restrictive given the critical role that the development of effective vaccines, diagnostics, therapeutics, and detection systems, along with a responsive public health system, will play in providing protection against bioterrorism—and other serious health threats."[7] As Robert Carlson observes:

> There are currently calls to limit research in the United States on the basic biology of many pathogens to preempt their use as bioweapons, and the possession and transport of many pathogens was legislated into criminality by the Patriot Act. The main difficulty with this approach is not that it assumes the basic biology of pathogens is static—which because of either natural variation or human intervention it is not—but rather that it assumes we have already catalogued all possible natural pathogens, that we already know how to detect and defeat known and unknown pathogens, and that rogue elements will not be able to learn how to manipulate pathogens and toxins on their own.[8]

There are currently calls to limit research in the United States on the basic biology of many pathogens to preempt their use as bioweapons...

Given that there are too many unknowns—both natural and man-made—government regulations alone cannot provide full protection from the potential misuse of dual-use research. In fact, the current U.S. strategy and government-commissioned studies concede this point. The "National Strategy for Countering Biological Threats" states that "life scientists are best positioned to develop, document, and reinforce norms regarding the beneficial intent of their contribution to the global community as well as those activities that are fundamentally intolerable."[9] In a 2003 report "Biotechnology Research in an Age of Terrorism," the recommended system of governance over dual-use research "relies heavily on a mix of voluntary self-governance by the scientific community and expansion of an existing regulatory process that itself grew out of an earlier response by the scientific community to the perceived risk associated with gene-splicing research."[10] A 2006 NAS report "Globalization, Biosecurity, and the Future of the Life Sciences" states that the U.S. security community has "been unable to establish and maintain the breadth, depth, and currency of knowledge and subject matter expertise in the life sciences and related technologies that are needed" to anticipate future biological threats.[11]

However, despite the acknowledgement that the life science community must have a larger role in the regulation of dual-use research, the practice of the U.S. government has been to enact regulations with only the advice of the life sciences. This amounts to a weak relationship in which the life science profession is only allowed the "legitimate right to interpret, buffer, or partially modify actions"[12] that are within the full jurisdiction of U.S. security professionals.

The government regulation of scientific research in the U.S. has evolved along with the perception of the threat. Each regulation was developed in response to a specific perceived threat. For example, the original "NIH Guidelines for Research Involving Recombinant DNA Molecules" were developed in response to the perceived public-health threat posed by recombinant DNA research.[13] Unfortunately, a study of the effect of a reactionary approach to biosecurity policies developed almost exclusively by the security portion of the interagency apparatus reveals (not

surprisingly) both a decrease in motivation for self-governance from the science community and an increase in the amount of time required to issue policies and regulations after the threat is identified.

Bioterrorism and Dual-Use Research

The deliberate spread of anthrax through the mail in October 2001 caused both security and life science professionals to give renewed emphasis to the threat of bioterrorism. After the National Commission on Terrorism released a report in 2000 recommending that biological physical security standards "should be as rigorous as the physical protection and security measures applicable to critical nuclear material,"[14] the NAS Committee on International Security and Arms Control became concerned about how Congress might seek to implement this recommendation. Hence, it established its own committee to "review current U.S. mechanisms to prevent the destructive application of biotechnology research and to recommend improvements to those mechanisms that would still permit legitimate research to proceed."[15] In effect, the committee's work was an effort by the life sciences profession to preempt legislation that could further hinder scientific advancement. The committee's work, known popularly as the Fink Report, contained several recommendations that are still being addressed in policy recommendations over a decade after it was published in 2003. The overall tenor of the recommendations was to leave evaluation of the biosecurity risk in the hands of the life science community. The report identified seven "experiments of concern" to focus the discussion of whether an experiment should be conducted in the first place and, if conducted, whether the results should be published in the open literature.[16] Since the NIH Guidelines already provided a mechanism for evaluating research risk through its Institutional Biosafety Committee (IBC), the Fink Report recommended expanding the IBC role to include dual-use research.[17] Another important recommendation was the establishment of the National Science Advisory Board for Biodefense (NSABB). This board was to be composed of both science and security representatives to provide a strategic forum for science and security dialogue and a resource for advice on specific experiments being carried out at research institutions.[18]

The deliberate spread of anthrax through the mail in October 2001 caused both security and life science professionals to give renewed emphasis to the threat of bioterrorism.

After nine years, the U.S. government released the "United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern" in 2012. This policy requires federal departments and agencies to submit a biannual risk assessment for all experiments they conduct or fund as defined in seven categories. These categories are slight variations of the "experiments of concern" described in the Fink Report, but are now referred to as "dual-use research of concern" (DURC). After over two additional years of deliberation and development, the U.S. government issued an additional policy, "United States Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern," in 2014. This newest policy maintains all of the requirements for federal departments and agencies that fund DURC and adds additional responsibilities for the principal investigators—the lead scientists conducting an experiment—and the institution where the research is being conducted, regardless of whether the institution is receiving federal funding. The 2014 policy requires research

institutions to assign an institutional contact for dual-use research (ICUDR) and to establish a review committee that can evaluate the risk of misuse of a particular experiment. Institutions may use an existing IBC, create a new review committee, or use an IBC from a neighboring research institution.[19]

...the pace of advancement in the life sciences is increasing, limiting the effect that published policies may have on the problem.

Responding to the threat of bioterrorism and the potential misuse of DURC is a process, and research institutions have until September 2015 to develop relevant compliance procedures. However, it is still possible to discern the similarities between previous reactions to science security concerns and this one. First, the life science profession was the first to initiate a study on how to address the risk of potentially dangerous technology being made available to terrorists. It was, in fact, the science community—not the U.S. government—that established the initial recommendations for regulation, stressing the desire to retain the predominant jurisdiction with the scientists. Second, two government regulations emerged in response to the risk of DURC. The policies on oversight of DURC—both government and institutional—require researchers to define the scope of the research addressed and require institutions to create an internal review board. However, they retain the ultimate control of the biosecurity task within the government security profession. The most recent policies even use the same IBCs as options for institutions to evaluate the new threat.

To further complicate matters, the time that security professionals take between identifying the threat and issuing a policy is trending longer. It took at least nine years to determine how to control the DURC threat. At the same time, the pace of advancement in the life sciences is increasing, limiting the effect that published policies may have on the problem. Now is an opportune time for the interagency to reevaluate the relationship between the security and life science professions.

A Model for Conducting the Needed Reevaluation

The general bureaucratic model that has been followed thus far in regulating potential for misuse of life science research has been to identify the risk, consult the life science community, and develop government regulations to mitigate the risk.

This model assumes that U.S. government security professionals are uniquely qualified to be entitled to practically full jurisdiction over the task of biosecurity as it pertains to dual-use research. While the most recent policy regulations state the intention to reevaluate and update policies "as warranted," history has shown that new policies only add additional requirements on top of old ones, resulting in a perpetuation of the same relationship between professions. In situations like this one, it is useful to apply a different method of evaluating the problem to see if it may provide a more useful result.

In his seminal work *The System of Professions: An Essay on the Division of Labor,* sociologist Andrew Abbot describes what constitutes a "profession" and how professions relate to each other when confronted with the requirement to determine the extent of shared jurisdiction over a task. In doing so, he moves beyond the typical professional literature that focuses on "structures of operational control," such as "licenses, schools, journals, [and] associations."[20] Two aspects of Abbot's model that are pertinent to the discussion of the life science profession are his description of what

constitutes "professional work"[21] and his discussion of the legitimate and rational grounds for claims of professional "jurisdiction."[22] The first, as applied to the present subject, addresses the requirement for a profession to assume the task of biosecurity; the second addresses the issue of which profession should carry out which tasks associated with overlapping jurisdictional claims and to what extent.

Abbot argues that all professional work is composed of "human problems amenable to expert service."[23] These problems contain both objective and subjective properties that contribute to solving the task at hand. Objective properties are "given by natural or technological imperatives," while subjective ones are "imposed by the present and past of a culture itself."[24] When these properties are applied to the threat of biological weapons, one can easily establish that a threat exists, and that there is a need for an expert service to minimize that threat. The objective nature of the biological weapons threat is well documented. Both the U.S. and the Soviet Union amassed stockpiles of biological weapons during the Cold War. The 1972 Biological Weapons Convention had a great deal of success in establishing an international norm against state production, stockpiling, and use of biological weapons. However, a non-state threat remains. For example, in 1984, the Rajneeshees cult contaminated salad bars with salmonella in an effort to reduce voter turn-out and skew the results of a local election.[25] The Japanese cult Aum Shinrikyo attempted to disperse anthrax spores in Tokyo.[26] There is also evidence that al Qaeda attempted to develop an anthrax weapon with the assistance of Pakistani and Malaysian scientists.[27] Perhaps the most well-known act of bioterrorism occurred in 2001 when anthrax filled envelopes were sent to several locations in the U.S. through the mail.[28] Based on these examples, there should be no disagreement that, objectively, the threat of bioterrorism exists, and that by extension, a rational claim can be made to the effect that some societal organ is best positioned from among competing alternatives to assume jurisdiction in addressing the threat.

Subjective properties of a problem provide the arena where different professions may compete for jurisdiction of the task. Abbott divides subjective qualities into three parts: diagnosis, inference, and treatment. Diagnosis is the process of collecting information about a problem and then classifying it into a category for which there are treatments. Inference occurs "when the connection between diagnosis and treatment is obscure" and requires the most expertise in a given field in order to bridge the gap between diagnosis and treatment. Treatment is the prescription of a solution to the problem.[29] As these generic terms from Abbot's theory are applied to the problem of biosecurity in dual-use research, their usefulness quickly becomes apparent.

Both the U.S. and the Soviet Union amassed stockpiles of biological weapons during the Cold War.

Based on the three examples above, it is clear that both the life science and security communities have a stake in achieving the right diagnosis. Abbott contends that diagnosis "not only seeks the right professional category for the client, but also removes the client's extraneous qualities."[30] The difficulty in diagnosing the task of biosecurity lies in the fact that the clients are not only the researchers working in the field, but also the American public, whose concerns are not strictly the same as those of scientific researchers. Hence, security professionals cannot, or perhaps should not, attempt to remove from their calculus what they may consider to be "extraneous qualities" like fear, politics, and limited government resources from

the diagnosis. This fact, however, admittedly makes it harder to classify the resulting picture into a "dictionary of legitimate problems."[31] For when this happens, the result is a diagnosis of the problem that has to take into account every possible outcome, no matter how remote the chance.

After diagnosing the threats from DURC, NAS conducted a study to draw on the knowledge of the science community in order to bridge the gap between diagnosis and treatment. However, the two professions interpret inference differently. Once again, Abbot's analysis provides a perspective that assists in determining the overlap in jurisdictional claims. He delineates two types of inference: exclusion and construction. "Exclusion" assumes that a profession will get multiple attempts to apply treatment. If a treatment is not successful, the professional can apply different treatments in succession to solve the problem.[32] This type of inference is most closely related to the trial-and-error conducted by researchers in the life science profession. Professionals are able to conduct their experiments in a controlled environment (i.e., the laboratory) before arriving at their desired result. When developing a new medical treatment for anthrax, for example, the researcher must first test the drug on animal models, then a controlled group of human subjects, before the drug is ready for administration to the public. "Construction," on the other hand, assumes that the profession will only get one chance to solve the problem, requiring it to develop a more comprehensive treatment.[33] Security professionals are faced with the biosecurity challenge of preventing all misuse—one biological weapons attack would amount to a biosecurity failure from the perspective of the American public. Security professionals are not afforded the controlled environment of a laboratory. Security professionals appear to be using inference by exclusion when inference by construction is required based on the nature of their profession. This is apparent by the compounding treatments that are applied to the threat of misuse of scientific research. An understanding of the different types of inference and which is most appropriate for the competing professions will help to define the primary clients of each profession (discussed below).

...the clients of biosecurity are not just the American public; they are also the researchers and institutions themselves.

The final attribute of professional work is treatment. Where diagnosis removes the personal qualities of the problem, treatment needs to reintegrate them so that a treatment will be effective to the clients. Abbott calls this "the process of prescription."[34] Prescriptions that have been discussed thus far have come in the form of policies and regulations. Security professionals have retained the right to prescribe security classifications and institutional review boards on scientific research in order to make the treatment effective for the American public. However, the clients of biosecurity are not just the American public; they are also the researchers and institutions themselves. The security profession's prescription does not adequately take this additional constituency into account. Conversely, prescriptions from the life science profession, when it has been given the ability to prescribe, tend to lean more toward the researcher clients and tend to omit adequate consideration of the larger society.

Diagnosis, inference, and treatment provide a lexicon that allows the analysis of how different professions may establish relative jurisdiction within a given task. In the previous discussion, examples illustrated the different perspectives of security and life science professions within this lexicon. The following discussion will focus on how these professions,

as a whole, relate to each other.

Claim of Jurisdiction

Abbott provides a useful method that can be applied to analyze the relationship between security and life science professionals. Both have a stake in ensuring that life science research is conducted safely within the lab and that the results of the research cannot be easily misused by those that wish to do harm. Jurisdictional claims are at the heart of what constitutes a profession. Abbott explains:

> A jurisdictional claim made before the public is generally a claim for legitimate control of a particular kind of work. This control means first and foremost a right to perform the work as professionals see fit. Along with the right to perform the work as it wishes, a profession normally also claims rights to exclude other workers as deemed necessary, to dominate public definition of the tasks concerned, and indeed to impose professional definitions of the task on competing professions. Public jurisdiction, in short, is a claim of both social and cultural authority.[35]

Since tasks frequently fall within the jurisdictional claim of multiple professions, those professions must establish a relationship that is accepted by the public and reinforced in laws. Abbott describes five relationships or "settlements of a jurisdictional dispute" ranging along a spectrum of "full," "subordinate," "intellectual," "divided," and "advisory."[36] Based on the cases described above, security professionals appear to claim "full" jurisdiction over biosecurity. This is demonstrated by the fact that the prescription of treatments comes in the form of policies and regulations that are imposed upon the life science profession. In the past, even when the life science profession has attempted to prescribe its own treatment, security professionals have imposed additional regulations.

Currently, the life science profession can best be described as claiming an "advisory" jurisdiction on the task of biosecurity. Abbot describes this jurisdictional relationship as "a weak relation, in which one profession seeks a legitimate right to interpret, buffer, or partially modify actions another takes within its own full jurisdiction."[37] This advisory role is manifest in NAS committees and the NSABB. However, some have questioned the continued relevance of the NSABB, the main component of the life science profession's already limited role in biosecurity. The NIH stripped the NSABB of its oversight role in 2012, and the NSABB currently meets less frequently than called for in its charter.[38]

Both [security and life science professionals]...have a stake in ensuring that life science research is conducted safely...

Several examples illustrate the current advisory role of life science professionals in relation to security professionals. In the past, the science community took the lead in initiating moratoria on experiments that caused it concern, such as experiments with recombinant DNA. In contrast, today the Office of Science and Technology Policy and the Department of Health and Human Services—the bureaucratic institution—pauses funding for certain experiments until it—and not the scientific community—can conduct a "deliberative process to assess the potential risks and benefits associated with a subset of life science research."[39] In another example, The Cambridge Working Group, a group concerned about "potential pandemic pathogen" research, called for a pause in research similar to the one that introduced this article; however, the group appears to support the security

profession's claim of jurisdiction by posting the government's research pause announcement at the top of its website without any disclaimer whatsoever.[40] What little claim that an advisory jurisdiction provides to the life sciences over the task of biosecurity appears to be dwindling.

Abbott states that advisory jurisdiction is "sometimes a leading edge of invasion, sometimes the trailing edge of defeat."[41] If the life science profession intends to assert a claim on biosecurity, it must work its way up Abbott's spectrum of settlements to gain public legitimacy. The next level of settlement on Abbott's spectrum is "division of labor." This is a "division of the jurisdiction into functionally interdependent but structurally equal parts."[42] A step up to settlement by division of labor may improve the task of biosecurity by leveraging the life scientists' knowledge, maintaining the benefit of the profession's inference, and prescribing treatments that benefit both types of client—the public and the research institutions.

Benefits of Division of Labor

In order to remain relevant in the task of biosecurity, the life science profession needs to expand its jurisdiction to assume a larger claim on diagnosis and treatment of the task. The profession should do this to protect its own researchers and institutions from overregulation, but also to avoid the indirect consequences on the public. After the release of the March 2012 DURC Policy, the Federal Bureau of Investigation (FBI) Weapons of Mass Destruction (WMD) Directorate, the American Association for the Advancement of Science, the Association of American Universities, and the Association of Public and Land-grant Universities hosted a series of meetings with academic scientists and research administrators. Representatives from both the security and life science professions discussed the security profession's techniques of implementing oversight regulation requirements and its effects on conducting research. Among researchers' concerns was the potential that "overly restrictive" government policies and regulations could deter research institutions from working with the regulated agents and experiments. Abandonment of this type of research "could have negative repercussions on biodefense preparedness, health, and agriculture, and possibly result in increased vulnerability to biological threats."[43] This observation demonstrates that overregulation by a security profession that has sole jurisdiction of biosecurity could create consequences for the American public as well.

...overregulation by a security profession that has sole jurisdiction of biosecurity could create consequences for the American public as well.

The Obama Administration has affirmed a need for the contributions of the life sciences in achieving protection from biological threats.[44] The Fink Committee highlighted the importance of government regulations in conducting experiments of concern. Refinement is needed in determining where division of labor should occur. Abbott's model for professional work provides a lexicon that may be used to analyze the boundaries of this relationship between professions.

As discussed above, diagnosis of the DURC risk differs between the two professions depending on their predominant clients. The security profession could draw on the objectivity of the life science profession, releasing some of its claim in order to scope the problem correctly. A more accurate diagnosis of the threat would lead to better prescriptions for both the public and the researchers. If all DURC is deemed suspect until it is proven otherwise, the inevitable delay will only lead to more

funding pauses and "deliberate" analysis. In the meantime, less research will be conducted to protect the population from certain germs—and to protect the population from possible biological weapon threats.

"Inference" is an area of work where more collaboration can occur. In the examples given above, after the threat was identified, inference occurred in series—first in a NAS committee, then in the security professional's evaluation of the recommendations. Both professions could benefit from combining their respective bodies of knowledge in a collaborative inference exercise to address both security and research concerns in parallel, thereby addressing the needs of both types of client—the American public and the professional researcher.

Finally, "prescription of treatment" is an area where the life sciences could play a much larger role. Abbott argues that "measurability of results" can contribute to the relative vulnerability in a jurisdictional claim.[45] Hence, simply stating that a bioterrorism attack has not occurred as the result of published results of DURC, as some may cite in defense of full jurisdiction for the security profession, is not an accurate measurement of success. Success should be determined by the demonstrated functioning of an oversight system. As revealed by the Sunshine Project surveys in 2004 and 2006, the NIH Guidelines IBC requirements for evaluating the research at issue were not accurately measured by the security professionals that imposed them. Life science researchers with experience in laboratories can more accurately assess the capacity for their institutions to conduct a DURC review. Starting with the existing capacity, the life science profession can work with the security profession to build that capacity over time. This security-life science collaboration is already occurring in certain fields. For example, the FBI WMD Directorate creates partnerships between its own WMD coordinators and academia, institutions, industry contacts, and other organizations.[46] The intent of these partnerships is to change the attitude within the research community from a code of ethics for "safeguarding science" to developing a "not on my watch" attitude among life science professionals.[47] Partnerships like these will help develop capacity to conduct DURC risk analysis over the long term and should lead to a culture change within the life science profession that will help to validate its increased claim on the jurisdiction of biosecurity.

Conclusion

The life science profession is losing what little jurisdictional claim it had on the task of biosecurity. Government policies and regulations have replaced the life sciences' self-imposed moratoria and guidelines on research of the past. Leaving biosecurity within the full jurisdiction of security professionals, while it may provide improved protection to American citizens from a bioterrorism attack, imposes an increasing burden on the other clients of biosecurity—the researchers. A jurisdictional settlement that involves a division of labor between security and life science professions could improve the results of biosecurity for both professions' predominant clients.

Leaving biosecurity within the full jurisdiction of security professionals... imposes an increasing burden on the other clients of biosecurity—the researchers.

Most discussion about biosecurity for DURC has been about trying to find the proper balance between security and an open and collaborative scientific community. Some have interpreted the increase in security regulations

as an imposition on the life science community. This article argues that, by taking a cue from Abbot's sociological model, it is possible to change the method of analysis that currently impedes, rather than facilitates, the teleological aim of biosecurity—an aim that transcends professional boundaries and speaks to the greater societal good. Once one can identify the type of relationship that currently exists between the life sciences and the security professions, it is possible to discuss the benefits of adjusting that relationship. Jurisdictional claims are an ever-changing competition between professions that desire to control a specific task. In the case of biosecurity, the life science practitioners that are most associated with DURC must now shape the discussion and justify an increased ability to self-regulate, especially in the attributes of diagnosis and treatment. ***IAJ***

NOTES

1 The White House, "Doing Diligence to Assess the Risks and Benefits of Life Sciences Gain-of-Function Research," <http://www.whitehouse.gov/blog/2014/10/17/doing-diligence-assess-risks-and-benefits-life-sciences-gain-function-research>, accessed on October 28, 2014; Francis S. Collins, "Statement on Funding Pause on Certain Types of Gain-of-Function Research," The NIH Director-National Institutes of Health (NIH), <http://www.nih.gov/about/director /10172014_statement_gof.htm>, accessed on October 28, 2014.

2 Robert Carlson, "The Pace and Proliferation of Biological Technologies," Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science, Vol. 1, No. 3, September 1, 2003, pp. 203–209.

3 Gregory D. Koblentz, "Biosecurity Reconsidered: Calibrating Biological Threats and Responses," International Security, Vol. 34, No. 4, March 17, 2010, pp. 104–107.the rise of globalization, the emergence of new diseases, and the changing nature of conflict have increased the risks posed by naturally occurring and man-made biological threats. A growing acceptance of a broader definition of security since the end of the Cold War has facilitated the rise of biosecurity issues on the international security agenda. Developing strategies to counter biological threats is complicated by the lack of agreement on the definition of biosecurity, the diverse range of biological threats, and competing perspectives on the most pressing biological threats. A comprehensive definition of biosecurity that encompasses naturally occurring, accidental, and deliberate disease outbreaks can help to further research, analysis, and policymaking. Operationalizing this broad conception of biosecurity requires a taxonomy of biological threats based on a levels-of-analysis approach that identifies which types of actors are potential sources of biological threats and the groups most at risk from these threats. A biosecurity taxonomy can provide a common framework for the multidisciplinary research and analysis necessary to assess and manage these risks. It also has implications for how to prevent and respond to biological threats, as well as for the future of biosecurity research.","DOI":"10.1162/isec.2010.34.4.96","ISSN":"0162-2889","shortTitle":"Biosecurity Reconsid ered","journalAbbreviation":"International Security","author":[{"family":"Koblentz","given":"Gregory D."}],"issued":{"date-parts":[["2010",3,17]]},"accessed":{"date-parts":[["2014",7,11]]}},"locator":"104-107"}],"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}

4 Ibid., pp. 105–106.the rise of globalization, the emergence of new diseases, and the changing nature of conflict have increased the risks posed by naturally occurring and man-made biological threats. A growing acceptance of a broader definition of security since the end of the Cold War has facilitated the rise of biosecurity issues on the international security agenda. Developing strategies to counter biological threats is complicated by the lack of agreement on the definition of biosecurity, the diverse range of biological threats, and competing perspectives on the most pressing biological threats. A comprehensive definition of biosecurity that encompasses naturally occurring, accidental, and deliberate disease outbreaks can help to further research, analysis, and policymaking. Operationalizing this broad conception of biosecurity requires a taxonomy of biological threats based on a levels-of-analysis approach that identifies which types of actors

are potential sources of biological threats and the groups most at risk from these threats. A biosecurity taxonomy can provide a common framework for the multidisciplinary research and analysis necessary to assess and manage these risks. It also has implications for how to prevent and respond to biological threats, as well as for the future of biosecurity research.”,”DOI”:”10.1162/isec.2010.34.4.96”,”ISSN”:”0162-2889”,”shortTitle”:”Biosecurity Reconsidered”,”journalAbbreviation”:”International Security”,”author”:[{“family”:”Koblentz”,”given”:”Gregory D.”}],”issued”:{“date-parts”:[[“2010”,3,17]]},”accessed”:{“date-parts”:[[“2014”,7,11]]}},”locator”:”105-106”}],”schema”:”https://github.com/citation-style-language/schema/raw/master/csl-citation.json”}

5 Committee on Advances in Technology and the Prevention of Their Application to Next Generation Biowarfare Threats, National Research Council, Globalization, Biosecurity, and the Future of the Life Sciences, The National Academies Press, Washington, 2006, p. 32, <http://www.nap.edu/download.php?record_id=11567>, accessed on August 27, 2014.

6 Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, Biotechnology Research in an Age of Terrorism, National Academies Press, Washington, 2004, p. 18.

7 Ibid., pp. 2–3.

8 Carlson, p. 210.

9 The White House, “National Strategy for Countering Biological Threats,” November 23, 2009, p. 8.

10 Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, p. 3.

11 Committee on Advances in Technology and the Prevention of Their Application to Next Generation Biowarfare Threats, p. 9.

12 Andrew Abbott, The System of Profession: An Essay on the Division of Expert Labor, University of Chicago Press, Chicago, 1988, p. 75.

13 Gerald L. Epstein, “Preventing Biological Weapon Development Through the Governance of Research,” *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, Vol. 10, Issue 1, March 28, 2012, p. 19.and Science”,”page”:”17-37”,”volume”:”10”,”issue”:”1”,”source”:”online.liebertpub.com.mutex.gmu.edu (Atypon

14 National Commission on Terrorism, “Countering the Changing Threat of International Terrorism,” <http://fas.org/irp/threat/commission.html>, accessed on November 13, 2014.

15 Epstein, p. 20.and Science”,”page”:”17-37”,”volume”:”10”,”issue”:”1”,”source”:”online.liebertpub.com.mutex.gmu.edu (Atypon

16 Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, p. 5.

17 Ibid., pp. 6–7.

18 Ibid., p. 9.

19 Office of Science and Technology Policy, “United States Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern,” February 22, 2013, <http://www.phe.gov /s3/dualuse/Documents/oversight-durc.pdf>, accessed on May 3, 2014.

20 Abbott, pp. 315–316.

21 Ibid., pp. 35–58.

22 Ibid., pp. 59–85.

23 Ibid., p. 35.

24 Ibid., p. 36.

25 World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism,

Vintage Books, 2008, p. 10.

26 Ibid.

27 Ibid.

28 Ibid., pp. 9–11.

29 Abbott, pp. 40–52.

30 Ibid., p. 41.

31 Ibid.

32 Abbott, p. 49.

33 Ibid.

34 Ibid., p. 46.

35 Ibid., p. 60.

36 Ibid., pp. 69–79.

37 Ibid., p. 75.

38 Gregory Koblentz, "Is the NSABB Still Relevant to Today's Biosecurity Challenges?" The Pandora Report, <http://pandorareport.org/2014/07/16/is-the-nsabb-still-relevant-to-todays-biosecurity-challenges>, accessed on August 9, 2014.

39 The White House, "Doing Diligence to Assess the Risks and Benefits of Life Sciences Gain-of-Function Research."

40 "The Cambridge Working Group," <http://www.cambridgeworkinggroup.org>, accessed November 3, 2014.

41 Abbott, p. 76.

42 Ibid., p. 73.

43 Pete Kelly et al., "Bridging Science and Security for Biological Research: A Discussion about Dual Use Review and Oversight at Research Institutions,"American Association for the Advancement of Science Meeting Report, Washington, SMichell Zappaeptember 13–14, 2012, p. 22.

44 The White House, "National Strategy for Countering Biological Threats," p. 3.

45 Abbott, p. 46.

46 Federal Bureau of Investigation, "Inside the Biological Countermeasures Unit, Part 1," February 21, 2012, <http://www.fbi.gov/news/stories/2012/february/wmd_022112 /wmd_022112>, accessed on February 7, 2014.

47 Supervisory Special Agent Edward You, personal conversation, September 2014.

Worth Noting

Compiled by Elizabeth Hill

Sewell Provides Update on Atrocity Prevention Board

Under Secretary for Civilian Security, Democracy, and Human Rights Sarah Sewell spoke at the Council on Foreign Relations on March 30, on the subject of the Atrocities Prevention Board (APB). Sewell reviewed the origin, purpose, and progress of the APB, and answered questions from the audience.

The APB was established by Presidential Study Directive 10 in August 2011 to coordinate a whole-of-government approach to preventing mass atrocities and genocide. According to Sewell, the APB "feeds into a larger interagency process of decision-making," and complements and enhances the work of the State Department and other U.S. government agencies.

Sewell discussed the increased focus on atrocity prevention in the years since the APB was established, noting various atrocity prevention efforts across government agencies, such as the State Department's Anti-Atrocities Coordination Group. Sewell also spoke about the State Department's Bureau of Conflict and Stabilization Operations (CSO) and how CSO works with the U.S. Agency for International Development to "develop evidence-based, civilian-focused intervention options, including diplomatic, programmatic, multilateral, and economic efforts."

During her remarks at the Council on Foreign Relations, Sewell gave many examples of the APB's efforts in atrocity prevention, citing interagency efforts to prevent and respond to violence in Burundi and the Central African Republic, as well as helping to counter the Islamic State of Iraq and the Levant.

While Sewell did note that there is more to be done, she remains encouraged by the progress made by the APB so far, saying "As imperfect as our current efforts are, they represent undeniable progress – both in symbolism and in concrete results. As we approach the APB's third anniversary, we are certainly closer to realizing the President's intent that the United States government embraces the mission of preventing mass atrocities. It is my hope that three years from now, the United States will have made its decision-making, tools, resources, and actions even more effective in preventing mass violence against civilians." ***IAJ***

Cybersecurity Bill Passes Senate Intelligence Committee

On March 13, the Senate Select Committee on Intelligence voted the Cybersecurity Information Sharing Act of 2015 through by 14 to 1. The bill will now move on to the Senate.

The Cybersecurity Information Sharing Act of 2015 creates additional incentives to increase voluntary sharing of cybersecurity threat information between the private sector and the federal government while protecting individual privacy and civil liberties interests. The bill also offers liability protection to the private sector.

The bill tasks the Department of Homeland Security with setting up a mechanism to receive threat indicators from network operators, and includes plans for government to share classified and other non-public threat information with "cleared representatives of relevant entities."

The Cybersecurity Information Sharing Act of 2015 was co-sponsored by Committee Chairman Richard Burr (R-NC) and Vice Chairman Dianne Feinstein (D-CA). ***IAJ***

Air Force Restructures Nuclear Weapons Center

The Air Force Nuclear Weapons Center was recently restructured to better serve the Nuclear Enterprise. On March 30, the center added two new directorates, including the Nuclear Technology and Interagency Directorate.

The new Nuclear Technology and Interagency Directorate focuses on nuclear weapons technology and interagency cooperation and partnership in the nation's nuclear enterprise. The Nuclear Technology and Interagency Directorate enhances the Air Force Nuclear Weapons Center support of the U.S. nuclear deterrence and assurance responsibility, and ensures this mission is carried out through the acquisition, sustainment, and support of powerful weapon systems.

Air Force Nuclear Weapons Center commander Maj. Gen. Sandra Finan spoke of the center's reorganization, saying "Our mission is still to deliver nuclear capabilities and winning solutions that warfighters use daily to deter our enemies and assure our allies. Implementation of this [structure] will better align our organization to that mission." ***IAJ***

Interagency Strategy Needed on Drones

On March 18, members of the House Homeland Security Subcommittee on Oversight and Management called for better comprehensive strategy to combat the potential threats of domestic drones, sometimes referred to as unmanned aerial systems or unmanned aerial vehicles.

In his opening statement, Subcommittee Chairman Rep. Scott Perry (R-PA) expressed concerns about the potential for drones to be utilized by terrorists, drug smugglers, and spies, and cited recent security incidents, such as the quadcopter crash at the White House and drones flying over Parisian landmarks and nuclear power plants.

Several witnesses spoke about the need for interagency cooperation to address the drone issue in their statements to the Subcommittee.

Major General (Ret.) Frederick Roggero, United States Air Force, called for interagency cooperation to draft strategy and policies to deal with drones, saying that "it will take a joined effort across all government departments since it will require navigating through current rules and

regulations in the face of the unique capabilities of [drones]".

In his statement, Chief Richard Beary, President of the International Association of Chiefs of Police, cited a lack of instruction for law enforcement regarding the use of drones, and spoke of the need for greater tactical guidance to law enforcement from federal agencies, including the Departments of Homeland Security, Justice, Defense, and the Federal Aviation Administration. According to Beary, such guidance "would benefit the law enforcement profession immensely".

Dr. Gregory S. McNeal, Associate Professor at the School of Law at Pepperdine University, also expressed a need for greater interagency cooperation, suggesting that the Department of Homeland Security be responsible for coordinating interagency efforts, as opposed to the agencies working separately. McNeal also suggested the department engage in a comprehensive risk assessment. ***IAJ***

CSIS Report Provides Recommendations on Cyber Threat Information Sharing

In early March, the Center for Strategic & International Studies (CSIS) published a report outlining their recommendations to Congress in regard to cyber threat information sharing between the government and the private sector.

To identify lessons learned from existing and previous information sharing efforts, CSIS convened three workshops to discuss the technical, structural, and legal challenges to cyber threat information sharing. These workshops were attended by a cross-sector stakeholder group that included government, industry, and privacy organizations, as well as experts from the financial services, telecommunications, electricity, oil and gas, retail, and commercial information technology sectors, and the privacy community.

After analyzing the comments and suggestions of the participants, the authors have provided Congress with 11 recommendations for policy and legislation. These recommendations cover both structural and legal issues, and include:

- Private-to-private sharing with a minimal role for government can help promote voluntary information sharing and alleviate privacy concerns.
- Build upon existing information-sharing organizations and mechanisms.
- Cyber threat information shared voluntarily with the government should be protected from disclosure through Freedom of Information Act (FOIA) requests and barred from use in civil litigation or regulatory purposes.
- Identify ways for information sharing models to demonstrate value for all parties involved.
- Permissible law enforcement uses of cyber threat information shared by companies with the government should be restricted to cybersecurity purposes and a limited set of other activities.
- Legislation should authorize monitoring and sharing of cyber threat information, and provide a safe harbor from civil and criminal liability for good-faith actions in conducting such activities.

While the authors recognize that there is much to be gained through improved cyber threat information sharing, they also note that it is not "an end in itself," and suggest that the government and other sectors "articulate the objectives and goals for information sharing, and tailor mechanisms for information sharing to achieve those goals." ***IAJ***

DHS Officials Push for Cyber Information Sharing

In late February, two Department of Homeland Security (DHS) officials testified before a congressional panel on President Obama's proposal on cybersecurity information sharing.

Under Secretary Suzanne Spaulding and Deputy Under Secretary for Cybersecurity & Communications Phyllis Schneck addressed the House Committee on Homeland Security, highlighting the National Protection and Programs Directorate cybersecurity role and capabilities, and speaking of DHS's plans to facilitate better information sharing of cyber threats between private industry and the federal government through the National Cybersecurity and Communications Integration Center (NCCIC).

Spaulding and Schneck described NCCIC's relationship with its partners – which include both private sector organizations and federal departments and agencies, among others – and NCCIC's work sharing cyber threat indicators with these partners.

The officials discussed President Obama's recent visit to NCCIC, where he announced new cybersecurity legislation to better facilitate information sharing between the government and the private sector. According to Spaulding and Schneck, "Our vision is that this may reduce the time to receive and act on indicators from hours to milliseconds, create consistency in information provided to interagency partners, law enforcement, and the private sector".

Spaulding and Schneck also reviewed new developments in DHS's cyber threat information sharing efforts, including specifications which standardize the representation and exchange of cyber threat information. ***IAJ***

Cybersecurity, Consumer Protection Subject of White House Summit

Stanford University hosted the White House Summit on Cybersecurity and Consumer Protection on February 13. The summit centered around cybersecurity information sharing and the efforts private industry is taking to better protect the data of their customers. The event brought together leaders from various industries, law enforcement, consumer and privacy advocates, academics, and students.

Lisa Monaco, homeland security and counterterrorism advisor to the President, opened the summit. Monaco, who recently announced the creation of the Cyber Threat Intelligence Integration Center (CTIIC), spoke of the growing importance of cybersecurity issues related to national and homeland security, including in the financial, energy, and technology sectors. Monaco also spoke about the continuing rise in cybersecurity breeches and attacks, the effort needed to meet a "constantly evolving enemy," and the value of private sector cooperation with the government to address cyber threats.

The summit included several plenary panels, the first of which dealt with public-private collaboration on cybersecurity. Panelists included CEOs from consumer retail, banking, health care, and utility companies, and the panel was moderated by Secretary of Homeland Security Jeh Johnson. In his remarks, Kenneth Chenault, Chairman and CEO of American Express, described the cyber threats faced by the U.S. as "increasingly challenging, increasingly complex" and went on to say that "information sharing may be the single, highest impact, lowest cost, and fastest way

to implement capabilities we have at hand as a nation to accelerate our overall defense from the many varied and increasing threats that we are facing every second."

President Obama made the keynote address, centering his remarks on confronting cyber threats and the future of cybersecurity. During his address, the President also introduced and signed an executive order encouraging the sharing of cybersecurity threat information within the private sector and between the private sector and government.

Later panels focused on consumer data protection, and featured panelists from various industries, including credit card companies and large businesses. ***IAJ***

Executive Order Calls for Information Sharing of Cyber Threat Data

On February 13, President Obama signed an Executive Order to encourage and promote sharing of cybersecurity threat information within the private sector and between the private sector and government. The Executive Order lays out a framework for expanded information sharing designed to help companies work together, and work with the federal government, to quickly identify and protect against cyber threats.

The Executive Order encourages private sector cybersecurity collaboration through information sharing and analysis organizations (ISAOs), and directs the Department of Homeland Security to fund the creation of a non-profit organization to develop a common set of voluntary standards for these ISAOs. The Executive Order also increases collaboration between ISAOs and the federal government, and will streamline private sector companies' ability to access classified cybersecurity threat information.

The new Executive Order complements the Administration's January 2015 legislative proposal, and paves the way for new legislation, by building out the concept of ISAOs as a framework for the targeted liability protections that the Administration has long asserted are pivotal to incentivizing and expanding information sharing. ***IAJ***

New Agency to Investigate Cyber Threats

In February, the White House announced that it is creating a new office analyze and integrate intelligence data about cyber threats and combat cyber attacks. The Cyber Threat Intelligence Integration Center (CTIIC) will fall under the purview of the Office of the Director of National Intelligence.

Lisa Monaco, assistant to the President for homeland security and counterterrorism, introduced the CTIIC during a talk at the Wilson Center, saying that "What we need is critical, rapid, integrated intelligence."

The CTIIC will be modeled after the National Counterterrorism Center (NCTC), and will integrate intelligence from the Central Intelligence Agency, National Security Agency, and other federal agencies, as well as the private sector. The CTIIC will focus on four priorities:

- Improving cyber defense, including widespread adoption of the NIST Cybersecurity Framework;

- Improving the ability to disrupt, respond to and recover from attacks;
- Enhancing international cooperation; and
- Making cyberspace intrinsically more secure, including eliminating passwords as the default security tool and enhancing consumer protection.

In her remarks, Monaco stated that "Cybersecurity is and will remain a defining challenge of the 21st century," and that "The choices we make today will define the threats we face tomorrow. ***IAJ***

White House Discusses Strengthening U.S. Cybersecurity

On January 14, President Obama visited the National Cybersecurity and Communications Integration Center (NCCIC) where he spoke about plans to strengthen U.S. cybersecurity in 2015. His remarks at NCCIC come a week before his State of the Union address.

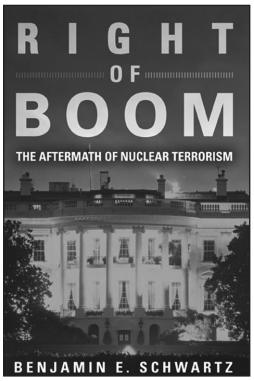
During his address at NCCIC, the President announced new cybersecurity legislation to better facilitate information sharing between the government and the private sector. This legislation improves upon prior legislation, builds on discussions with the federal government and private industry, and includes safeguards to protect Americans' privacy and civil liberties.

The new cyber efforts also include updating the authorities used by law enforcement when investigating and prosecuting cyber criminals. This would include prosecuting those involved in the sale of botnets and spyware, and expands the authority of courts to shut down botnets and other malware.

The President also announced that a White House Summit on cybersecurity and consumer protection would be held in February at Stanford University. The summit will include participants from the U.S. government and across various industries, technology companies, and consumer and privacy advocates, as well as law professors and students.

President Obama concluded his remarks saying that the U.S. government and private sector would work together to "detect, prevent, defend, and deter" cyber attacks. ***IAJ***

Book Review



Right of Boom: The Aftermath of Nuclear Terrorism

Benjamin E. Schwartz

The Overlook Press, New York, NY, 2015, 237 pp.

Reviewed by Major William "Bay" Dobbins, USMC
- Graduate Fellow, Countering Weapons of Mass Destruction
National Defense University

Right of Boom: The Aftermath of Nuclear Terrorism provides a glimpse of the issues associated with responding to a nuclear terrorist attack, in this case, the detonation of a small nuclear weapon in Washington, D.C. Against this background, Benjamin Schwartz describes the inherent danger of a world with nuclear-armed states (some which may not have the will or capability to appropriately secure such weapons) and new types of terror threats, the lessons learned in nuclear deterrence and counter terrorism, the global impact of a nuclear terror attack, and the "red lines" that would forever change as a result. What emerges is a bleak picture of potential political and policy consequences of both the terror attack and the American response.

In the aftermath of a nuclear terrorist attack on the most important political capital in the world, the confusion, the desire for attribution and retaliation coupled together with the overarching question, "How did this happen?" combine to produce the environment that political leaders would face. At first glance, the author posits, the response to such an event seems straightforward: The U.S. undergoes a nuclear attack, and the U.S. responds in kind. However, the follow-on questions reveal that things are not nearly so simple: From where did the weapon come? In a terror attack in which attribution is not certain, against whom do national leaders direct a response?

The history of international nuclear agreements, from the Non-Proliferation Treaty (NPT) to the Nunn-Lugar Cooperative Threat Reduction (CTR) program are all predicated on international relationships that operated at the nation-state level. However, the attack in question reveals that these state-to-state agreements may no longer be sufficient in the face of nuclear terrorism. The proliferation of nuclear knowledge and technology now makes the nuclear terror threat plausible. Hence, Schwartz argues, "we are more vulnerable to nuclear terrorism than at any time since the dawn of the nuclear age."

Could an attack like this actually happen? On the one hand, Schwartz notes legitimate reasons for skepticism. After all, since 9-11, there have been no societally significant terror attacks and no nuclear terror attacks. Moreover, the continual crying of "wolves at the door" by national leaders only makes the lack of terrorist success more pronounced. The failure of intelligence regarding WMD threats—leading to the Global War on Terror—has also cast a pall over the intelligence community's predictive powers. On the other hand, Schwartz also notes that neither past intelligence failures nor

the absence of a nuclear terrorist attack changes the fact that the proliferation of knowledge and technology—especially dual-use technology—increases the threat of nuclear terrorism. Access to the knowledge necessary for nuclear proliferation has itself proliferated since World War II. Even if the hardest part of developing a nuclear weapon is acquiring fissile material, the plans for simple weapon systems can now be found with a quick internet search. Hence, Schwartz argues that, while the threat of thermonuclear war recedes into history, a new threat—like that of the detonation of a small nuclear weapon in a city such as Washington, D.C.—is actually growing. The breakup of the former USSR states created one of the most dangerous situations for the "loose nuke" phenomenon. While CTR provided one of the most successful bi-lateral programs to protect against that possible threat, nations, such as Pakistan or North Korea, outside the scope of CTR may provide material support to terror organizations, or they may simply have insufficient control over their nuclear materials.

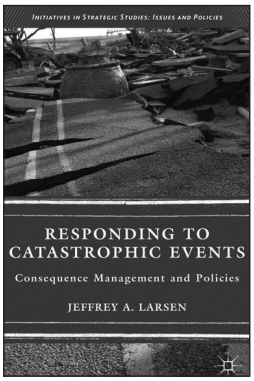
In light of these complexities, the question naturally, but uncomfortably, arises as to the ongoing role of nuclear deterrence. The working assumption has been that, when faced with total annihilation between two warring states, each opponent may be deterred from nuclear weapons employment. Although this very model arguably worked well for 60 years between the USSR and the United States, Schwartz highlights that the present nuclear world is faced with a different problem: How does a nation-state deter a stateless organization? For that matter, how does a nuclear nation-state deter even a non-nuclear nation-state committed to the support of nuclear terrorists? As a testament to such, since World War II, four out of the five NPT nuclear powers has "lost" a war to a non-nuclear foe without ever using nuclear weapons.

In the immediate aftermath of a nuclear terror attack in the United States, the political need to demonstrate control, resolve and to hold someone accountable will be intense. Yet, how does the U.S. determine what objectives to pursue? It is simple to say, "Go kill the terrorists!" It is another to comply with that statement. Individual targets in multiple nations with multiple governments involved do not necessarily constitute an effective counter-terrorism program. How does the U.S. build an international coalition when political interests diverge and intelligence agencies have different opinions about governmental complicity? How does it create a coalition of allied governments whose very citizens may be involved? How does it counter terrorism when "terrorism" itself is an amorphous concept? On this account, Schwartz provides historical examples that run from the Comanche to the United States' current fight with Al Qaeda and its affiliates. Countering terrorism will be the battle of the future; it will not be an easy one—particularly if it acquires a nuclear dimension.

A nuclear terror attack on the United States will affect more than the U.S. It will re-write the international legal system. There may still be treaties and agreements, but after a nuclear weapon detonates, they may simply be pieces of paper. Establishing new arrangements and treaties will have to follow. The idea that what happens within the borders of another nation-state is only that nation-state's business will be robustly challenged. The risk is simply too great to trust that another government would even be capable of keeping its nuclear issues within its borders. The Peace of Westphalia may simply fade away. Further, the people of the United States could be affected by unprecedentedly intrusive surveillance of goods, materials, and information being imported and exported. In this environment, it is possible that the Baruch plan—or a reasonable facsimile—may be pursued with broader support than it originally had. In the end, Schwartz suggests, an event like this would do more to change the global security calculus than did 9-11.

The advances in technology, the free flow of information coupled with the rise in extremism has made the world a more dangerous place than it used to be. Technologies like additive manufacturing make the possibility of nuclear proliferation greater than ever. The challenge of acquiring fissile material remains the greatest obstacle to overcome, yet the possibility exists that it will be achieved by a non-state actor. Indeed, what happens if the question moves from being "If?" to "When?"

In sum, *Right of Boom* represents a thoughtful but accessible treatment of a complex subject, particularly for one who is uninitiated in the subject. While the historical presentation it contains may seem at times to outweigh the specific idea of "right of boom", it provides necessary context in support of the central theme. It is a particularly valuable reference for students of interagency operations. ***IAJ***



Responding to Catastrophic Events: Consequence Management and Policies

Edited by Jeffrey A Larsen

Initiatives in Strategic Studies Series, Palgrave Macmillan, New York, NY, 2013, 276 pp.

Reviewed by John Mark Mattox
- Director, Countering Weapons of Mass Destruction Graduate Fellowship Program, National Defense University

"Catastrophic events", particularly as the term gets applied to weapons of mass destruction events, are, curious as it may seem, easy to dismiss as someone else's problem in the big, lumbering federal bureaucracy. This is so because the events thus characterized are so overwhelming that they befuddle the imagination (and certainly would exhaust the resources) of any one agency that sought to deal with them. However, it is this fact which, more than any other, makes the response to catastrophic events the quintessential interagency challenge. The present anthology assembles the work of some of America's most insightful public servants and clearly demonstrates that every organ of government at every level—tribal, local, state, and federal—is remiss if it fails to ask the question, "What is my role when the unthinkable happens?" and "With whom should I be talking as I imagine the unthinkable?"

Editor Jeffrey A. Larsen reminds us that when the unthinkable happens, it always happens somewhere: "All disasters are local." Nevertheless, he also notes that "From the local perspective, federal resources often seem to arrive too late and leave too early." While this is largely perceptual and part of that perception is unavoidable when people are suffering catastrophic loss, it is nevertheless the case that such perceptions, just like catastrophes themselves, must be managed if the public is to have and retain confidence in the proposition that, when all the local, familiar agencies have been overwhelmed, government will still be there to restore public order and function.

Part I examines the immediate aspects of a coordinated response: The first of these requires obtaining a proper degree of situational awareness, i.e., one that correctly scopes the problem, enables an effective, unstymied response, and discerns larger implications. However, as author James J. Wirtz notes, "larger implications" may arise in unexpected ways: anthrax in the food supply, the collapse of a major dam, or a chemical release in an urban setting. None of these

examples necessarily involve malicious activity by a foreign power, but the threats they pose are no less far reaching. The second aspect involves planning and acting within the actual constraints of time—this latter dimension constituting, in author Jerry Barnhill's words, its own "tyranny" of sorts.

Part II provides a useful overview of the federal response, beginning with Richard Love's dissection of the ideas of "homeland security" and "homeland defense" in which he explains the relationship of the Department of Defense to an interagency response effort. This overview is complemented by two pieces: one by Greg Moser and Garry Briese that explains the balancing act required to ensure that the federal government assists local jurisdictions without overwhelming them, and another by Pat Allen Pentland that explains the particular features of the Department of Defense's apparatus and method.

Part III undertakes two areas which, although easy for the operator to set aside as issues better left to specialists, are thus relegated at peril. G. Roderick Gillette explains, in accessible terms, the intricate and (to the lay person) sometimes mysterious legal considerations that inform all responses to catastrophic events. His exposition is an invitation to reflect upon the far-reaching consequences of legal decisions leaders at all levels are called upon to make under chaotic circumstances. George Haddow deals with another sina qua non of consequence management, namely, foolproof (or at least as foolproof as bureaucracies can make it) communications and public information protocol. Brian Lewis then compares domestic and foreign consequence management and effectively highlights the reality that what one assumes or takes or granted at home cannot necessarily be assumed or taken for granted abroad.

In Part IV, *Responding to Catastrophic Events* moves helpfully from the theoretical to the practical, with important contemporary case studies: the chemical attack on the Tokyo subway, by Erin R. Mahan; the response to Hurricane Katrina, by Jessica Iannotti; and the lessons that both of these events yield for WMD consequence management, by Shane Smith.

Finally, in Part V, Kerry M. Kartchner captures, in a concluding essay, the essence of the nexus between consequence management and national security—illustrating that the even if all disasters are local, anything that can be called a disaster inevitably has national security ramifications.

Responding to Catastrophic Events is a "must-read" for government leaders at all levels, regardless of whether their work-a-day activities involve the label "consequence management" or not. Its length, breadth, and accessibility make it a first choice as a graduate-level textbook in consequence management courses taught by federal agencies, in that it affords the thoughtful reader the opportunity to reflect upon such questions as:

- What is my role and that of my agency as part of a whole-of-government response to a catastrophe?
- What capabilities does my agency possess that will be essential in a response but which may not be obvious to those outside my agency?
- What information sharing needs to occur once a catastrophe occurs—and with whom? What information needs to be shared now, and what liaisons need to be established now?
- How can my agency best contribute to a successful encounter with the worst possible scenario when it is not (and may never be) in the lead?

The vexing (and, as a practical matter, probably insurmountable) challenge for texts of this kind is the dynamic nature of the bureaucratic structures, and to a lesser degree, the bureaucratic policies that they describe; and in no field of government action is that dynamism likely more operative than in the evolving world of response to catastrophic events. Terms like "crisis management" and "consequence management" may mean one thing to the lay person and quite another thing to the specialist—and both terms are now bureaucratically subsumed under the term "incident management". However, it is difficult to imagine any team of authors being more successful at de-mystifying the relevant nuances than the present team of expert has been. Hence, it may be hoped that they will, in due course, prepare subsequent editions reflecting the relevant bureaucratic changes as they occur over time. ***IAJ***

The Simons Center
P.O. Box 3429
Fort Leavenworth, Kansas 66027
ph: 913-682-7244
www.TheSimonsCenter.org
facebook.com/TheSimonsCenter

CGSC Foundation, Inc.
100 Stimson Avenue, Suite 1149
Fort Leavenworth, Kansas 66027
ph: 913-651-0624
www.cgscfoundation.org
facebook.com/CGSCFoundation
twitter.com/CGSCFoundation
LinkedIn.com >>CGSC Foundation, Inc.