The Simons Center
Fort Leavenworth, Kansas

InterAgency Journal

Weapons of Mass Destruction: Current Questions for the Interagency
John Mark Mattox

Additive Manufacturing: Implications for the Interagency's Nuclear Counterproliferation Task
John W. Andrews

Importing Nuclear Weapons Through the Selectively-Permeable Border of the United States
William T. Eckles

A Nation Unprepared: Bioterrorism and Pandemic Response
John B. Foley

Plutonium and Picasso – A Typology of Nuclear and Fine Art Smuggling
Joshua D. Foss

Optimizing the CWMD Enterprise Across the Interagency
Michael J. Kwon

Concurrent Biological, Electromagnetic Pulse, and Cyber-attacks: The Ultimate Interagency Response Challenge
Patricia Rohrbeck

Kinetic Energy Weapons: The Beginning of an Interagency Challenge
Daniel C. Sproull

Special Edition:

Weapons of Mass Destruction

The Journal of The Simons Center
Vol. 8, Issue 2 (2017)

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 military leaders with interagency operational skills 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. 8, Issue 2 (2017)

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
www.TheSimonsCenter.org

Editor-in-Chief
Roderick M. Cox

Managing Editor
Elizabeth Hill

Editor
Valerie Tystad

Contributing Editor
John Mark Mattox

Design/Production
Mark H. Wiggins
MHW Public Relations and Communications

Printing
Allen Press, Inc.
Lawrence, Kansas

Features

5 **Weapons of Mass Destruction: Current Questions for the Interagency**
John Mark Mattox

7 **Additive Manufacturing: Implications for the Interagency's Nuclear Counterproliferation Task**
John W. Andrews

18 **Importing Nuclear Weapons Through the Selectively-Permeable Border of the United States**
William T. Eckles

25 **A Nation Unprepared: Bioterrorism and Pandemic Response**
John B. Foley

34 **Plutonium and Picasso – A Typology of Nuclear and Fine Art Smuggling**
Joshua D. Foss

44 **Optimizing the CWMD Enterprise Across the Interagency**
Michael J. Kwon

53 **Concurrent Biological, Electromagnetic Pulse, and Cyber-attacks: The Ultimate Interagency Response Challenge**
Patricia Rohrbeck

62 **Kinetic Energy Weapons: The Beginning of an Interagency Challenge**
Daniel C. Sproull

69 **Worth Noting**

75 **Book Review**

From the Editor-in-Chief

The *InterAgency Journal* is pleased to once again partner with expert practitioners and scholars from across the Department of Defense to bring you this special edition on weapons of mass destruction. I thank Dr. Mark Mattox for his work in collecting and editing the manuscripts, and invite you to further investigate his work at the National Defense University's Center for the Study of Weapons of Mass Destruction.

This collection of articles illustrates the clear and present danger weapons of mass destruction continue to pose, and highlights that our response to protect the American people must be an interagency effort.

Having read this edition, I am reminded of the often asked question to senior government officials, "What is it that keeps you up at night?" From nuclear proliferation to bioterrorism to trafficking to simultaneous attacks, this edition of the *InterAgency Journal* provides a glimpse of the many causes of alarm.

Thank you for reading this issue of the *InterAgency Journal*. The Simons Center continues to strive to improve our utility to the interagency community. Your feedback is always welcome. I invite you to visit our website where you can stay abreast of the latest interagency happenings through our "News You Can Use" features and benefit from our various interagency speakers' presentations.

If you or your organization has expertise on a particular topic and desire to work with us to add your thoughts to the interagency discourse through publication of a special edition issue of the *InterAgency Journal*, please contact our Managing Editor at editor@TheSimonsCenter.org. – **RMC**

Contributors Wanted!

The Simons Center is looking for articles that involve contemporary interagency issues at both the conceptual and the application level.

The *InterAgency Journal* is a refereed national security studies journal providing a forum to inform a broad audience on matters pertaining to tactical and operational issues of cooperation, collaboration, and/or coordination among and between various governmental departments, agencies, and offices. Each issue contains a number of articles covering a variety of topics, including national security, counterterrorism, stabilization and reconstruction operations, and disaster preparation and response.

The *InterAgency Journal* has worldwide circulation and has received praise from various military, government, and non-government institutions, including the UN High Commissioner for Refugees.

Contact the Arthur D. Simons Center for Interagency Cooperation

www.TheSimonsCenter.org • editor@TheSimonsCenter.org
www.facebook.com/TheSimonsCenter
655 Biddle Blvd. • P.O. Box 3429 • Fort Leavenworth, KS 66027

The Simons Center is a major program of the CGSC Foundation, Inc.

Weapons of Mass Destruction:
Current Questions for the Interagency

by John Mark Mattox

Nothing is simple about weapons of mass destruction (WMD). The issues they raise are of enormous consequence by any imaginable measure; however, it is easy to lose sight of the magnitude of these issues for several reasons:

- The U.S. has never experienced a nuclear attack, and the last nuclear attack, August 9, 1945, in Nagasaki, Japan, is but a dim memory. George Weller, the first foreign reporter to enter Nagasaki following the attack, described it this way: "In swaybacked or flattened skeletons of the Mitsubishi arms plants is revealed what the atomic bomb can do to steel and stone, but what the riven atom can do against human flesh and bone lies hidden in two hospitals of downtown Nagasaki."[1]

- The U.S. has never undergone a chemical attack of the kind experienced in Belgium during World War I. It is hard for Americans to relate to British Lance Sergeant Elmer Cotton's diary description of the effects of chlorine gas: "It produces a flooding of the lungs—it is an equivalent death to drowning only on dry land. The effects are these: a splitting headache & terrific thirst (to drink water is instant death), a knife edge of pain in the lungs [and] the coughing up of a greenish froth off the…lungs and stomach [sic] ending finally in insensibility and death—the colour of the skin from white turns a greenish black or yellow, the tongue protrudes & the eyes assume a glassy stare—it is a fiendish death to die."[2]

- The U.S. has never undergone a biological attack that killed more than a half-dozen.

"Massive destruction"—whether the result of WMD or something else—is simply a concept that is difficult for Americans to get their minds around. They may have read in history books about massive numbers of deaths from the Black Death in 14th-century Europe, the 1942–1943 Battle of Stalingrad, or more recently, the 1984 Bhopal, India, Union Carbide chemical plant disaster, but in

John Mark Mattox, Ph.D., is the Director of the Countering Weapons of Mass Destruction Graduate Fellowship Program and a Senior Research Fellow at the National Defense University Center for the Study of Weapons of Mass Destruction.

reality, the broad ranges of numbers reported killed in these events are so imprecise that we cannot even pin down what "massive" really means when it comes to the loss of human life—not to mention losses of other kinds. Given the invitation to reflect seriously on what "massive destruction" means, the average lay person would probably find such an invitation no less than revolting. Nevertheless, government, if it is to take seriously the conventional wisdom that its first obligation is to protect its own citizens, must think about it. Moreover, no single agency of government can successfully undertake the task. It is truly an interagency effort.

This special issue of the *InterAgency Journal* presents a variety of topics that are timely for engagement by the interagency:

- John W. Andrews explores the important ramifications of emerging manufacturing technologies on the interagency's mission to contain the proliferation of nuclear weapons and materials.
- William T. Eckles notes that because the U.S. border is and must be semi-permeable, just as the borders of a healthy cell in a living organism must be, the passage of human beings through that border without a passport is not the only thing the interagency has to worry about. It also must concern itself with the illicit transit of nuclear weapons and materials.
- John B. Foley reminds the reader that in 2001 the interagency learned from its own war-gaming that the U.S. is not prepared to respond adequately to a pandemic-producing bioterrorist act, and that a decade and a half later, some important concerns identified then linger on today.
- Joshua D. Foss insightfully observes some interesting correspondence among all types of illicit trafficking, to include nuclear materials and fine art. Taking notice of this correspondence opens the door to important opportunities for cooperation and economies of effort across the interagency.
- Michael J. Kwon, noting that countering WMD is essentially an interagency task, recommends solutions for how that task might be more effectively managed with some relatively simple solutions for coordinating the task across a broad spectrum of organizations.
- Patricia Rohrbeck imagines the "perfect storm" that would result from simultaneous biological, electromagnetic pulse, and cyber-attacks.
- Finally, Daniel Sproull introduces a new WMD challenge to the interagency, namely, the one portended by the advent of kinetic energy weapons.

All of these important articles point to massive problems with massive consequences, but such is the nature of the interagency's task. ***IAJ***

NOTES

1 George Weller, "A Nagasaki Report," <http://www.nuclearfiles.org/menu/key-issues/nuclear-weapons/history/pre-cold-war/hiroshima-nagasaki/weller_nagasaki-report.htm>, accessed on January 31, 2017.

2 Elmer Wilgrid Cotton, diary, May 24, 1915, Imperial War Museum Document Collection, Imperial War Museum, quoted in Marian Giard, *A Strange and Formidable Weapon: British Responses to World War I Poison Gas*, University of Nebraska Press, Lincoln, NE, 2008, Introduction.

Additive Manufacturing:
Implications for the Interagency's Nuclear Counterproliferation Task

by John W. Andrews

The emerging technology of additive manufacturing (AM) is rapidly revolutionizing the world of industry. Additive manufacturing enables the layering of materials, using precise, computer-controlled machines, to quickly build objects with complex shapes at low cost. Indeed, AM promises to produce things that, only a few years ago, would have been utterly inconceivable to the traditional manufacturer. However, these same technologies include the potential for misuse in unthinkably, harmful ways, including the illicit production of nuclear weapon components. For over seven decades, the interagency has worked to create and maintain barriers that prevent the illicit development and transfer of nuclear weapon technology. However, these barriers were designed to counter traditional, "subtractive" forms of manufacturing; their efficacy does not readily transfer to newly emerging AM technologies. As AM matures, it certainly will become increasingly interesting to those seeking to produce nuclear weapons outside the established strictures of the international legal system. Additive manufacturing could be used to facilitate illicit nuclear weapon production by:

- Dramatically reducing both time and expense associated with nuclear weapon production.
- Dramatically increasing nuclear supply-chain efficiency.
- Providing more effective manufacturing options for aspiring proliferators, reducing the technical challenges associated with developing nuclear weapons.
- Reducing the footprint of illicit nuclear transactions.
- Exacerbating the problem of insider threats.
- Fundamentally altering the nuclear weapon acquisition pathway.

John Andrews is a Program Manager at the Defense Threat Reduction Agency's Research and Development Directorate. He received a M.S. Degree in WMD Studies as a National Defense University Countering WMD Graduate Fellow.

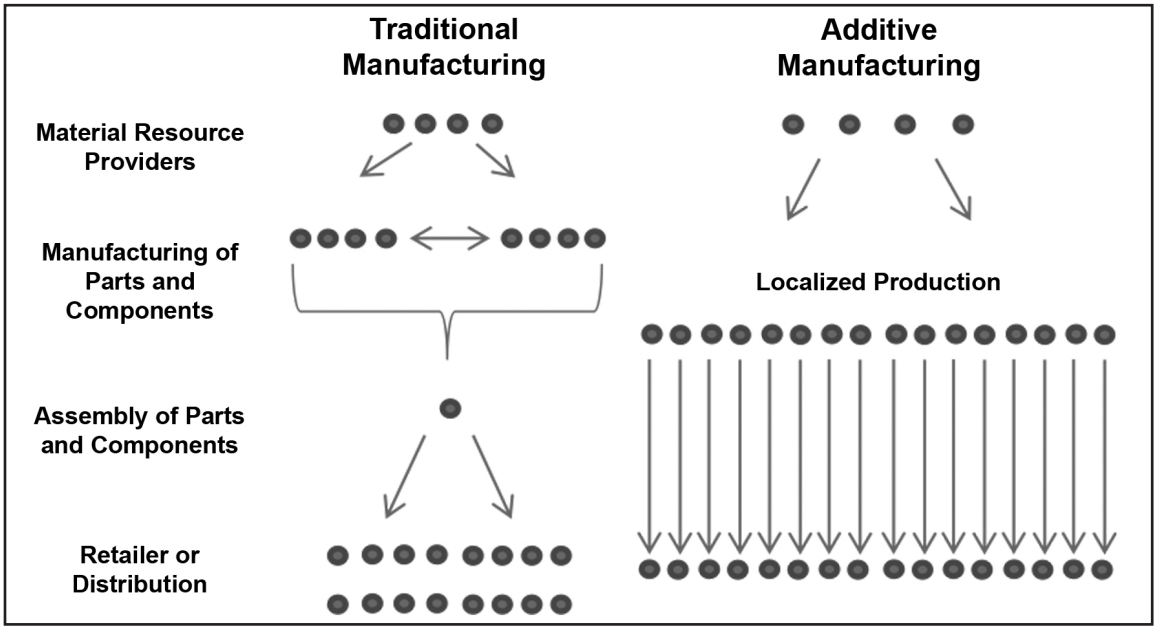


Figure 1. Supply chain comparison. [4]

Reducing Both Time and Expense of Nuclear Weapon Production

Although nuclear weapon development facilities are very large and include highly-sophisticated equipment, they generally do not require mass production techniques, and AM is particularly well-suited for sm all production runs. Indeed, Lawrence Livermore National Laboratory (LLNL) has embraced the use of AM systems to cut costs and increase the speed of operations for its nuclear stockpile lifetime-extension program.[1] The Department of Energy (DOE) National Nuclear Security Administration estimates that within five years AM systems will be capable of making 50 percent of its tools, which would cut tooling production costs by 75 percent, cut development time by 80 percent, and cut production time by 60 percent. These efficiencies would truly revolutionize DOE's nuclear stockpile lifetime-extension program. Nuclear proliferators may use AM systems to obtain similar efficiencies to streamline challenges associated with the illicit production of nuclear weapon technology.[2]

Increasing Nuclear Supply-Chain Efficiency

Material resource providers for traditional supply chains deliver to manufacturers of disparate parts and components. Those manufacturers might then ship their component parts to other manufacturers and then to an assembly plant. The assembly plant fabricates the final product and then delivers to a retailer or distributer. At any of the points or nodes in the supply chain, a disruption results in the delay of deliveries to the retailer or distributer. In contrast, the AM supply chain contains fewer nodes and, thus, less potential for disruption. Additive manufacturing may require no assembly of parts or components, with localized production occurring as additive systems utilize raw materials to fabricate the final product. However, these same efficiencies appeal to illicit networks because they are shorter and easier to compartmentalize, making them easier to conceal. Figure 1 illustrates the comparison between the supply chains of traditional manufacturing and AM.

Reducing the Technical Challenges Associated with Developing Nuclear Weapons

Additive manufacturing systems will provide more effective manufacturing options for aspiring proliferators, reducing the technical challenges associated with developing nuclear weapons. Nuclear weapon production facilities include lengthy, multi-step production processes. Each step requires specific expertise and careful planning and execution. Many steps in the process require parts with complex geometries made to very precise specifications that are difficult to fabricate with traditional methods. Very specific material designs and highly-precise process controls are required. The introduction of advanced AM systems with highly-precise control mechanisms and a vast array of material options could offer better alternatives to address some of these challenges.

Additive manufacturing systems can produce sophisticated parts with complex geometries and material properties that previously required several steps or were impossible to make with traditional subtractive manufacturing or forming methods. Traditional manufacturing techniques often require turning, milling, and grinding machines. These machines have multi-axis parts that must continually coordinate with each other to maintain a predetermined path. If state-of-the-art equipment is not available, significant work by hand is often required to re-position parts during machining or to produce component parts that are joined together later. The quality of the final product is heavily dependent on the skill of the machinist.[5] In the future, AM techniques will potentially meet or exceed the quality of some traditional techniques, while requiring far less machinist skill.

Additive manufacturing systems will provide ways to more efficiently design and fabricate nuclear weapon detonation mechanisms. A nuclear weapon of any kind requires sophisticated technical expertise to build, but the degree of precision required to construct a highly-efficient detonation depends on the amount, shape, and purity of the weapons-grade material (uranium-235 or plutonium-239), as well as the quality of the weapon design. Additive manufacturing techniques could improve the precision and accuracy with which nuclear devices are built, mitigating some of these design challenges. Additive manufacturing systems also offer potential to print exotic materials, such as high explosives with material properties that improve performance. High-explosive performance is heavily dependent on small imperfections or pores in the crystal structure of the material. Because some AM systems can manipulate material at the scale of the pores, which is about 1 to 100 micrometers, materials can potentially be created that yield more effective and predictable explosions, a critical factor in creating effective nuclear weapon detonation mechanisms.[6]

Additive manufacturing systems will provide more effective manufacturing options for aspiring proliferators...

Researchers at LLNL are not just using AM systems to save time and money, they are also using AM to create technically-superior parts. For example, LLNL is using AM systems to optimize the structure of metal components associated with the U.S. nuclear stockpile. Also, researchers are creating complex metal lattice structures with millions of millimeter-high struts that can conform to a curved surface, allowing LLNL to address some previously unresolved technical challenges. Additive manufacturing systems have also been used to create parts with unique material properties, like pads that are easily compressible at one end and stiff at the other, enabling more uniformed production

for certain components.[7] The same spirit of resourcefulness and creativity exhibited by LLNL researchers to improve stockpile lifetime extension programs may be mirrored by aspiring nuclear proliferators whom seek to acquire nuclear weapons or transfer nuclear weapon technology.

Additive manufacturing techniques will allow nuclear proliferators to reduce the signatures associated with their illicit transactions.

Reducing the Footprint of Illicit Nuclear Transactions

Additive manufacturing techniques will allow nuclear proliferators to reduce the signatures associated with their illicit transactions. Acquiring nuclear weapons is not a trivial task. Many steps are needed to generate or obtain the fissile nuclear material and the required equipment and expertise. Because most countries or groups seeking nuclear capabilities cannot build them on their own, they must rely on assistance from external entities, which creates a vast network of people and organizations that are involved with the various steps or acquisition pathways required to obtain nuclear weapons. At each step or node along the acquisition pathway, proliferation networks generate signatures. Over the past several decades, the interagency has created mechanisms to detect these signatures, effectively creating barriers to nuclear proliferation. Illicit networks adapt to interagency barriers over time, often exploiting advancements in technology. Additive manufacturing is not the first great technological advancement to be utilized by proliferation networks—the invention of the internet is another example. However, AM represents a serious concern due to the rapid nature of its growth, both in popularity and sophistication. As proliferators embrace AM, the signatures associated with the many transactions along the nuclear weapon acquisition pathway will be reduced.

Additive manufacturing technology will reduce the signatures associated with purchasing parts. No matter how effective illicit networks are at concealing their activities, they must expose themselves to some degree when they purchase equipment and parts. Detecting suspicious purchases is one of the most effective interagency tools for discovering an illicit network. If a group seeking nuclear weapons can fabricate a part using a 3D printer or similar device, it does not need to engage with a supplier. As additive technologies become more sophisticated and compatible with more materials, proliferators will be able to build more parts on their own. The potential decrease in purchasing transactions will have a corresponding decrease in the ability of the interagency to detect them.

The vulnerabilities associated with protecting 3D design information will be exasperated due to the emergence of AM technologies. Additive manufacturing systems will alleviate the need for proliferators to order certain pieces of equipment that can be fabricated by an AM system. If a nuclear-related part is capable of being printed by an AM device, but a proliferator does not know how to fabricate it, the proliferator could buy or steal the 3D design information. For example, suppose Country A needs a "dual-use item" tracked by the Nuclear Supplier's Group (NSG). Instead of trying to purchase that item from a supplier, Country A may be able to obtain the 3D design information and simply print the item with an AM system.

Additive manufacturing systems will increase the difficulty of detecting illicit networks because the number of people and activities associated with individual nuclear weapon acquisition pathways will decrease. Each person or activity associated with a

nuclear black market offers an opportunity for the network to be discovered by authorities. If an illicit network can decrease the number of people and transactions associated with it, it can increase its chances of evading detection. Additive manufacturing will increase the pool of people capable of contributing to nuclear proliferation, but it will decrease the number of people involved with individual nuclear weapon acquisition pathways in many cases. For example, future AM advancements in selective laser sintering machines may allow groups to fabricate complex metals parts without the need for several other traditional manufacturing techniques requiring the use of multiple pieces of equipment and several different machinists. By substituting the selective laser sintering machine and its operator for several pieces of equipment and several people, the signature-creating activities associated with the previous method have been greatly reduced. This example covers just one node within the overall nuclear weapon acquisition pathway. Consider the AM supply chain cost and timeline efficiencies illustrated in Figure 1. Since AM supply chains contain fewer nodes than traditional manufacturing supply chains, they inherently create fewer exploitable signatures than traditional manufacturing supply chains. Not only do fewer nodes result in fewer interagency detection opportunities, they also result in fewer interdiction or sabotage opportunities.

Additive manufacturing systems decrease the ability of interagency mechanisms to interdict illegal shipments of equipment. Since proliferators will be able to fabricate more items using 3D design data, the number of items they will need to purchase for delivery will be decreased. Instead, they could simply purchase the 3D design data, which can be delivered via email. Interagency mechanisms to detect and interdict physical shipments of equipment, such as the Proliferation Security Initiative, will be less effective due to decreased nuclear-related trafficking of physical objects.

The emergence of AM will create the potential for aspiring proliferators to decrease their signature-producing activities. This will affect every facet of the complex patchwork of interagency safeguards designed to detect illicit activity. The effectiveness of these safeguards will be degraded across the entire spectrum unless they are modified to account for AM.

Additive manufacturing systems decrease the ability of interagency mechanisms to interdict illegal shipments...

Exacerbating the Problem of Insider Threats

The emergence of AM technologies may also increase the difficulty of detecting insider threats. Many people involved with peaceful nuclear energy installations have access to technology that would be of great value to a proliferator. A.Q. Khan, for example, gained access to nuclear technologies in the 1970s while working for an Urenco subcontractor in Amsterdam. Khan later exploited his access to create a black market that contributed to the nuclear weapon programs of Pakistan, Iran, North Korea, Libya, and possibly others. As AM becomes more sophisticated and the pool of people capable of contributing to nuclear proliferation increases, the black-market demand for 3D design information may also increase. Illicit networks, encouraged by the increased capabilities that AM techniques offer, may make more attempts to bribe or blackmail workers at legitimate nuclear facilities. Alternatively, a disgruntled worker may be more inclined to seek out a nuclear black market. Insider threats of this nature are very difficult to detect. Stealing a 3D design file from an organization can be done from behind a desk. The illegal spread of nuclear

weapon and technology design information was an issue long before AM existed; however, the emergence of AM may increase the likelihood of it occurring.

Due to advances in AM, aspiring proliferators will have more options to pursue while simultaneously having more capability to conceal their activities.

Fundamentally Altering the Nuclear Weapon Acquisition Pathway

Due to advances in AM, aspiring proliferators will have more options to pursue while simultaneously having more capability to conceal their activities. As AM devices become more sophisticated, this effect will become increasingly more exaggerated, which will exacerbate interagency detection and interdiction challenges.

Consider the idea of a nuclear weapon acquisition pathway. For a group to acquire a nuclear weapon, it must conduct a large number of activities. The number of activities between different proliferators will vary greatly depending on the ambition of the group, its resources, and many other factors. If a group is intending to develop its own fissile material and produce a nuclear weapon indigenously, it will face many more challenges and probably conduct many more activities than a group that is simply looking to buy or steal fissile material and fabricate a weapon using the acquired uranium or plutonium. Whichever way a group attempts to acquire a weapon, the path it goes down can be characterized as its nuclear weapon acquisition pathway. The pathway includes any entity or action associated with the acquisition network. This includes the facilities the group utilizes, the people associated with it, the supplier companies in its network, and any communications, financial transactions, or other activities it conducts. A nearly infinite number of possible pathways exist, and every country or group seeking nuclear weapons will have a unique pathway.

When an aspiring proliferator sets out to acquire nuclear weapons, every activity it conducts on its pathway creates a signature. These signatures can vary greatly and can include anything associated with a myriad of activities, including buying or building facilities, hiring people, purchasing equipment, mining materials, transporting items, and creating communication networks. The interagency relies on these signatures to detect illicit networks. The successful discovery and interdiction of an illicit network often can be attributed to a combination of detected signatures gathered over a long period, none of which would have independently provided sufficient evidence of illicit activity. Since almost all nuclear-related technology and equipment have other purposes in legitimate industries, proliferators have a myriad of options to consider when navigating its pathway. Weeding out the illicit activity from normal industrial activity can be very challenging for counterproliferation officials. Figures 2 and 3 represent two different notional nuclear weapon acquisition pathways: the traditional pathway and the pathway made possible by AM.[8]

The dots represent possible nodes, or steps, on the acquisition pathway, and the lines connecting the dots represent relationships between those nodes. For example, a centrifuge supplier company and the uranium enrichment facility of the aspiring proliferator would be two nodes that have a relationship or connection. The thicker lines connecting the stars represent the actual pathway the proliferator has chosen, and the stars represent signatures associated with the proliferator's actions that make it susceptible to detection by law enforcement. As shown in Figure 2, traditional manufacturing acquisition

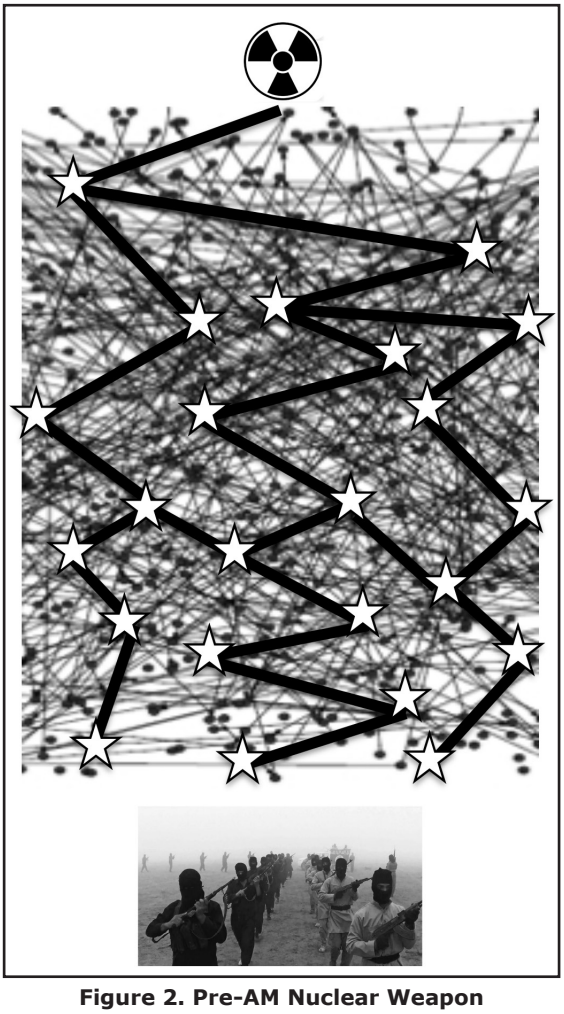


Figure 2. Pre-AM Nuclear Weapon Acquisition Pathway

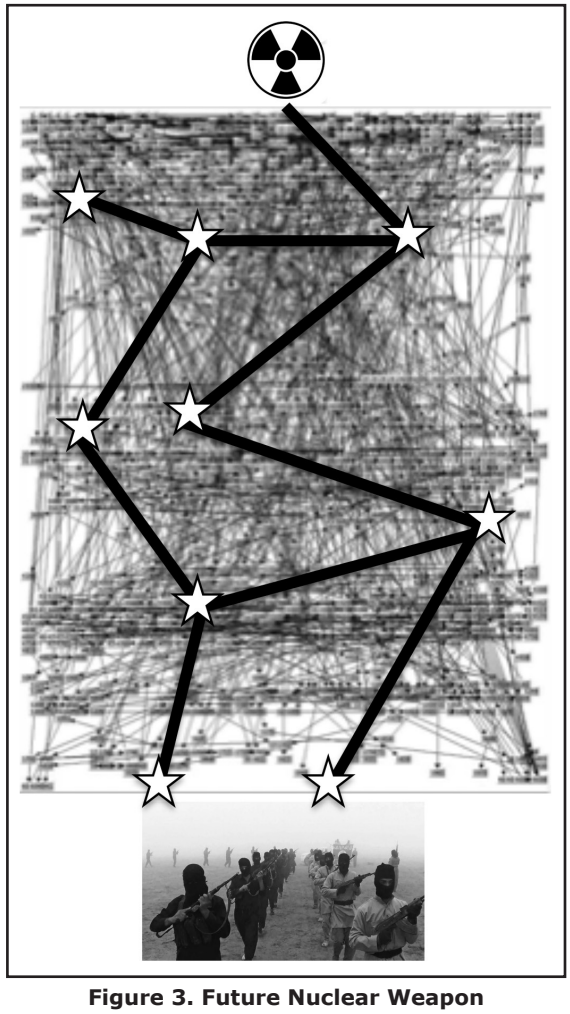


Figure 3. Future Nuclear Weapon Acquisition Pathway with AM

schemes provide interagency mechanisms with many opportunities to detect the signatures created by proliferation activities. In Figure 3, however, the number of potential illicit transactional pathways dramatically expands, while the transactional signatures—and the opportunity for interception—dramatically diminish. In short, law enforcement officials in the future will need to monitor a greater number of nodes in search of illicit activity, while the actual number of detectable illicit activities will decrease. If weeding out illicit proliferation transactions from legitimate industrial activities can be compared to searching for needles in a haystack, the introduction of AM effectively increases the size of the haystack while decreasing the number and size of the needles.

Looking Ahead

The AM industry is forecasted to grow exponentially in the coming years. While the forecasted growth is promising in many ways, it will increase the difficulty of detecting and tracking illicit nuclear technology procurement networks. All research suggests rapid growth of the AM industry. Some forecasts estimate a $20+ billion market by 2020.[9] This growth will create an entirely new segment of the world population with some level of engineering skill. Some members of this population will inevitably

be motivated, persuaded, or coerced to become involved in nuclear proliferation. The sheer increase in potential bad actors caused by the explosive growth of the AM industry will stress the capacity of intelligence and security agencies to track proliferation networks.

As different industries utilize AM to improve business, nuclear proliferators will utilize it to develop and transfer nuclear technology.

The growth of the AM industry will also put stress on export control enforcement. One of the great vulnerabilities of proliferation networks is their need to purchase dual-use equipment. Creating schemes to detect illicit procurement attempts may seem straightforward in theory, but it is difficult in practice. Only a very small fraction of inquiries that a legitimate company receives originate from a nuclear proliferator. Persistent efforts on the part of the nonproliferation regime are required to keep companies focused on preventing the inappropriate transfer of dual-use technology. Many companies that emerge during the inevitable explosion of the AM industry in the coming years will be completely unfamiliar with the nonproliferation regime. Without special efforts to educate and inform AM companies of illicit proliferation, it is unreasonable to expect them to prevent it. Even with ideal export-control policies and new intelligence collection schemes, the sheer number of new companies may strain interagency safeguards. The Department of Commerce, tasked with administering and enforcing export controls, will face especially difficult challenges in handling the rapid influx of companies emerging during the AM industry boom. The Department of Commerce relies on many interagency partners to carry out its nonproliferation-related export control duties, including the Departments of State, Homeland Security, Treasury, Defense, and Energy.[10] These partners will also be challenged to update policies and procedures commensurate with the vulnerabilities created by the influx of AM-related companies.

As different industries utilize AM to improve business, nuclear proliferators will utilize it to develop and transfer nuclear technology. Countries like China, Russia, North Korea, and Pakistan may be able to more effectively modernize their capabilities, enabling vertical nuclear proliferation. Horizontal proliferation is perhaps a greater concern. Countries previously discouraged by the technical, financial, and legal barriers associated with developing nuclear weapons may reconsider their options. Perhaps most troubling, non-state actors may embrace AM systems as a way to create an improvised nuclear device. Since a single nuclear weapon in the hands of a terrorist organization would have devastating consequences, the new risks posed by advances in AM must not be taken lightly. As the emergence of AM decreases the barriers to nuclear proliferation, the interagency will be forced to address new challenges.

The keys to addressing the vulnerabilities created by AM systems are understanding AM technologies and how they might be leveraged to advance nuclear weapon development efforts. No single organization can obtain this level of understanding. Most leaders in the AM industry will not be aware of how their technologies might contribute to proliferation. Similarly, most interagency nonproliferation officials will not have a nuanced understanding of AM technologies. Even some engineers in the nuclear weapon stockpile complex familiar with traditional methods of fabricating nuclear weapons may not yet recognize the applicability of AM to nuclear weapon development. Organizations from all facets of the nonproliferation regime should team with the AM industry to enable a whole-of-government

approach to mitigating the risks of AM without inhibiting the economic benefits of the AM industry.

Officials responsible for crafting export and trade control laws and regulations will face considerable challenges. The interagency should consider how the effectiveness of the NSG's "trigger" and "dual-use" lists will be degraded by AM systems. For example, will AM systems be capable of printing any of the items on the lists? If so, proliferators will be able to circumvent detection measures. Perhaps those AM systems capable of printing "dual-use" or "trigger" list items should be added to one of the NSG lists, along with the raw materials needed to do so. However, what if the growth in the AM industry reaches a level such that thousands of different types of AM systems and materials can contribute to nuclear proliferation? Would it be realistic to include these in the NSG lists and expect them to be regulated? What about the countries that embrace AM techniques that are not members of the NSG? How much easier will it be for illicit networks to leverage those countries' capabilities to develop or transfer nuclear technology?

The interagency should strengthen mechanisms to protect nuclear-related design information. Since AM systems will allow for easier and faster fabrication techniques, the motivation to buy or steal 3D design information may increase. This is particularly concerning due to the recent surge of cyber-attacks that will likely only increase in quantity and sophistication in the future.

Since the technical barriers to creating nuclear weapons will be reduced, the interagency may be forced to strengthen detection techniques that focus on individuals. Counter-bioterrorism techniques offer an appropriate template for addressing a serious threat with very low technical barriers to proliferation. Biological weapon production requires far less expertise, infrastructure, and money than nuclear weapon production, yet a devastating biological attack on the U.S. has never occurred.[11] The counter-nuclear proliferation community should seek lessons learned from the biological community to address the threat posed by AM industry growth.

The intelligence community should consider how to best strengthen detection schemes. For example, some intelligence collection frameworks could simply be expanded to include AM-related entities. Other frameworks may have to be created from scratch to address the growing threat. Perhaps a starting point is to identify existing academic and industry groups with possible ties to foreign military programs that are investing in AM technologies.

Creative technical solutions to mitigate proliferation risks should be solicited from the AM industry. The potential to create AM systems that create unique microscopic tags or identifiers on each piece of equipment that they fabricate has been discussed as a way to improve attribution capabilities. This and other similar proposals are intriguing, but they must be balanced with commercial motivations to remain competitive in the marketplace.

The interagency should strengthen mechanisms to protect nuclear-related design information.

Perhaps most importantly, the interagency should identify AM as a priority and take steps to set up lasting, whole-of-government approaches to address it. The interagency should institutionalize periodic reviews of the AM industry to discuss how it might contribute to nuclear proliferation, and then update policies and procedures to prevent problems before they occur. These reviews should include personnel from the intelligence community; the nuclear weapon science and technology community

from the Departments of Energy and Defense; leaders from the commercial AM community; nonproliferation policymakers from the Departments of State, Commerce, Homeland Security, and Treasury; international partners; and possibly others. Only vigorous and iterative reviews, inclusive of all entities, can yield well-reasoned recommendations for implementation that both mitigate the threat and avoid over-regulation that stifles economic growth.

While the pool of possible contributors to nuclear proliferation is increasing, the methods of illicit networks that embrace AM capabilities are creating fewer detectable signatures. By circumventing interagency barriers like export control regulations, aspiring proliferators will be able to navigate the pathway to acquiring a nuclear weapon with greater ease. The path to acquiring nuclear weapons outside the international legal system remains a daunting task even with the help of AM, but the interagency must stay steps ahead of illicit networks by making this emerging threat a priority and implementing a process to address it. The explosive growth in AM technology will not wait for policymakers—it is naïve to think that adversaries have not already recognized the potential of AM. The time to address this problem is now. ***IAJ***

NOTES

1 "Next-Generation Manufacturing for the Stockpile," January 2015, <https://str.llnl.gov/january-2015/marrgraff>, accessed on September 27, 2015.

2 Ibid.

3 D.S. Thomas, and S.W. Gilbert, "Costs and Cost Effectiveness of Additive Manufacturing a Literature Review and Discussion," *NIST Special Publication 1176*, December 2014, <http://dx.doi.org/10.6028/NIST.SP.1176, accessed on October 3, 2015.

4 Ibid.

5 *Federation of American Scientists Special Weapons Primer*, October 1998, <http://fas.org/nuke /intro/nuke/produce.htm>, accessed on November 1, 2015.

6 "Next-Generation Manufacturing for the Stockpile."

7 Ibid.

8 Figures 2 and 3 are purely notional. They were not derived from a specific threat and are for illustrative purposes only.

9 Louis Columbus, "2015 Roundup of 3D Printing Market Forecasts and Estimates," March 31, 2015, <http://www.forbes.com/sites/louiscolumbus/2015/03/31/2015-roundup-of-3d-printing-market-forecasts-and-estimates/#2715e4857a0b79d5645b1dc6>, accessed on February 7, 2016.

10 "A Resource on Strategic Trade Management and Export Controls," <http://www.state.gov /strategictrade/resources/c43182.htm>, accessed on February 8, 2016.

11 The "Amerithrax" attacks in October 2001 were certainly disruptive and tragic for the victims, but are not considered "major" in this case due to the relatively low number of casualties when compared to what could occur in the event of a nuclear attack or a more serious biological warfare attack.


Welcome to the Arthur D. Simons Center for Interagency Cooperation
Arthur D. Simons Center
for Interagency Cooperation
Search for:
Attention Interagency Practitioners!
Looking for a comprehensive website for news across the U.S. government?
Look no further!
The Simons Center's website is a one-stop-shop for interagency news and publications. Our site is constantly updated to include the latest in interagency and U.S. government news. We also provide a variety of useful resources, including an annotated bibliography containing thousands of articles, papers, books and other sources of interagency knowledge.
Sign up for our weekly email alerts today!
www.TheSimonsCenter.org
News You Can Use: 07/25/16
Treasury discusses cybersecurity in banking
Public and private sector discuss Zika
GAO reports on human trafficking
Donate to the Simons Center
InterAgency Journal
InterAgency Paper
InterAgency Essay
InterAgency Study

Importing Nuclear Weapons Through the Selectively-Permeable Border of the United States

by William T. Eckles

The health of the U.S. parallels the health of a living organism. The body needs and seeks beneficial substances and interactions. The skin, lungs, and digestive tract of an organism are like the border. Food and gasses must freely enter and leave the organismfor basic functioning and good health. Likewise, legitimate commerce, travel, and information exchange across the border are necessary for the health of the U.S. Occasionally, the mechanisms that keep bad things out and facilitate beneficial transactions break down. In the body, the immune system reacts and in the U.S., various agencies and institutions respond to known threats. The border represents the transition from external threats and opportunities to internal concerns. The desired operation of the country depends on the selective permeability of a border that allows or facilitates desired cross-border transit while denying illicit passage. Of the many harmful things that the selectively-permeable border of the U.S. must exclude, none present more urgency than the illicit importation of nuclear weapons. However, despite the best efforts of the interagency, U.S. borders remain porous with respect to this urgent threat.

Nuclear and Radiological Detection

As part of the 2014 Quadrennial Homeland Security Review (QHSR), the Department of Homeland Security (DHS) identified two long-term foundational capabilities necessary to prevent nuclear terrorism: (1) nuclear detection, and (2) nuclear forensics.

Nuclear and radiological materials emit characteristic signatures that can alert screening personnel. Detection is critical to prevent illicit movement of nuclear material or an improvised nuclear devise (IND) into the U.S. Terrorist acquisition of a nuclear device may result from the theft, sale, or provision from a state production facility.

William T. Eckles is a European International Relations Specialist at Defense Threat Reduction Agency, Fort Belvoir, where he coordinates and facilitates the implementation of Arms Control, Threat Reduction, and counterproliferation programs in Europe and Eurasia. He received an M.S. Degree in WMD Studies as a National Defense University Countering WMD Graduate Fellow.

Nuclear forensics focuses efforts to find the source of nuclear material through technical means, relying on specific signatures (detectable attributes) of the material to help identify where and how it was produced. Nuclear forensics may provide conclusive, attributional evidence to hold a state accountable.[1]

The Domestic Nuclear Detection Office (DNDO) under the DHS is the lead agency to develop the Global Nuclear Detection Architecture (GNDA) that is a framework for detecting, analyzing, and reporting nuclear and radiological materials that are outside regulatory control.[2] Established in 2005 by U.S. Presidential directive, DNDO relies on other U.S. agencies and global partners to implement its strategic objectives. The National Academy of Sciences (NAS), asked to evaluate the GNDA, observed that it had no clear decision authority for program implementation. Although the DNDO is the coordinator, it is not obligated to the Congressional appropriation for any single program element of the GNDA.[3] Secretaries of State, Defense, and Energy maintain their responsibilities for guidance and implementation for any GNDA portion outside of the U.S. Early detection off the shores of the U.S. bolsters the defense against nuclear weapons. Although no attempt to smuggle an IND into the U.S. has been reported, inspections and programs to determine the effectiveness of safeguards against such attempts continue to point to vulnerabilities.

The DNDO is the proponent for domestic nuclear detection responsibility to coordinate federal, state, and local efforts to detect nuclear and radiological materials domestically. The DNDO partners closely with Customs and Border Protection (CBP) to provide detection at and between points of entry (POEs). In support of the GNDA and as part of the DNDO strategy, the CBP invested over $2.5 billion to acquire and deploy radiation detection equipment through 2013, principally in support of its outer layer of border security that resides offshore and is focused on foreign ports. Although as part of the 9/11 Commission Act of 2007, Congress mandated 100 percent of all U.S.-destined cargo ships at all 58 CBP-staffed foreign ports be scanned for radiation by July 2012, the current Secretary of Homeland Security has extended the deadline for the mandate to July 2016.[4] Extending the deadline is a way to acknowledge that the task is unfeasible given the imbalance between screening capacity and shipping volume. Risk-based methodologies and extended deadlines for implementing the mandate are symptomatic of capacity and capability shortfalls that leave the U.S. borders vulnerable.

The Domestic Nuclear Detection Office (DNDO) under the DHS is the lead agency to develop the Global Nuclear Detection Architecture...

Large radiation portal monitors (RPMs) are critical to land and sea-POEs. Radiation portal monitors are the workhorses of radiological inspection of cargo and conveyances and a keystone in the nuclear detection framework. Their presence at the borders, while not a 100 percent safeguard to screen cargo and conveyance are purposeful in potentially deterring a nuclear smuggler or terrorist from attempting to bring an IND on a conveyance or through POEs. Over 1,400 RPMs are in use at the 110 U.S. land POEs and 444 RPMs operate at seaports throughout the U.S, including the 22 busiest seaports that account 99 percent of containerized cargo who work together to establish a border-sensing network.[5]

Whether containerized from maritime cargo, on trains, or in vehicles, the United States Government Accountability Office (GAO), CBP, and DNDO all report that nearly 100 percent of cargo passes through a radiological portal at POEs and permanent checkpoints. In May

2009, the GAO reported that while RPMs are an effective deterrent for nuclear smuggling, they have limitations. Namely, they can only detect materials that are unshielded or lightly shielded.[6] Shielding is a term used to describe efforts taken to protect people and property from radioactivity. Shielding also prevents radioactive material signals from reaching sensors. Shielding tends to be heavy, and the detection of shielding is a flag for CBP inspectors to inspect cargo.

Although imperfect, the nuclear and radiological detection methodologies rely on multiple sensors in depth.

In 2005, the DNDO initiated an acquisition plan that relied on the procurement of the Cargo Advanced Automated Radiography System (CAARS). The system was fraught with requirements and implementation problems, and DNDO canceled the acquisition program in 2007. However, the DHS stated that DNDO/CBP CAARS production and deployment program was developed, and DHS 2010 and 2011 budget justifications included CAARS program elements. The dysfunction evidenced among the coordinating bodies is symptomatic of other unsynchronized efforts leading to ineffective border management. Poor management and unrealized technical solutions continue to leave the border vulnerable.

The DNDO continues to make advancements with its RPMs and replaces or upgrades RPMs as part of its core budgetary elements. In 2008, the DNDO implemented the Advanced Spectroscopic Portal Program. It completed installing portals along the northern border in 2010 and budgets upgrades and replacements through 2016.[7] Starting in 2013, the DNDO identified the need to scan aviation cargo at air POEs. DNDO funding anticipates enabling the CBP to scan more than 40 percent of inbound air cargo within three years. Scanning by portal remains a strongpoint in the CBP border defenses. After the bulk of RPMs were installed and operated by trained personnel in the U.S. by 2012, the priority of effort shifted toward more flexible and portable detection devices.

The DHS Office of Inspector General (OIG) investigated the use of RPMs at sea-POEs and observed that at the seven ports visited, an average of 10 percent of the RPMs and ancillary equipment was not used or rarely used. The OIG assessed that DHS personnel were not fully updating databases to share information that informs other systems as part of the GNDA.[8]

Although imperfect, the nuclear and radiological detection methodologies rely on multiple sensors in depth. At POEs, there are sensors that when tripped should trigger further investigation. Portable and handheld sensors may interrogate targeted cargo and conveyances. Portable and handheld detectors augment permanent detection systems such as RPMs at POEs. Portable and handheld detectors may be moved to other areas as the threat moves or attempts to circumvent known detector locations. Between permanent portals, CBP protects the border from radiological hazards with handheld or portable scanners. Even if a nuclear smuggler got away from CBP at the border, similar capabilities exist in major cities.

Nuclear smuggling into the U.S. would most likely occur via a monitored road or land-POE. CPB anticipates scanning 40 percent of all air cargo for radioactivity by the end of 2016. Air cargo is more scrutinized, subject to weight restrictions, and visually inspected with greater rigor due to the everyday hazards posed by flammable and volatile hazards to the airframe. A terrorist that attempted nuclear smuggling through an air POE would require inside support to thwart multiple layers of monitoring and scrutiny. Smuggling a nuclear or radiological device through an air POE is highly mitigated by existing security efforts and is a low risk.

Small aircraft and boat nuclear smuggling rely on cooperative interdiction efforts of the CBP, Department of Interior, Federal Bureau of Investigation, and the U.S. Coast Guard. Upon detection, authorities work together to characterize the intruder. As remote sensing technologies improve, the ability to characterize cargo will also improve. Until that time, interdiction is followed by search operations that use inspections to determine if contraband is present.

Less than 1 percent of all maritime containerized traffic is deemed high-risk and flagged for inspection. The CBP takes the risk to facilitate commerce and provides numerous waivers that allow rapid transit from POE holding facilities. The CBP and other agencies accept this risk in part because other systems like RPMs exist. Waivers, poorly-trained border agents, and failure to use a secondary detection system all result in a vulnerable border.

A terrorist with a radiological or nuclear device still can exploit vulnerabilities. Nuclear and radiological vulnerabilities are not wholly the result of technological deficiency. Much of the concern rests with ensuring individuals are trained appropriately, that they apply that training using the available equipment, and that they are given enough time to execute protocols. The GAO identified that DHS has not completely aligned gaps within the GNDO with science and technology efforts. Basic science funding and partnerships with industries have often resulted in redundant efforts and not addressed known vulnerabilities. Not aligning efforts potentially result in vulnerability propagation and drive unnecessary cost for unnecessary programs.[9]

During 2013–2014, 325 publicly reported incidents involving radiological and nuclear material were reported by the Center for Nonproliferation Studies Database.[10] The International Atomic Energy Agency categorized an incident involving less than one gram of weapons-grade uranium and 16 other international incidents as extremely or very dangerous. The majority of nuclear and radiological material incidents relate to regulatory control violations with industrial use. None of the publicly reported incidents involved CPB agents or attempted smuggling across the border. In fact, there have been no publicly disclosed radiological or nuclear interdictions at the U.S.

The Operational Field Testing Division (OFTD) of the DHS challenged the ability of the CBP to detect nuclear material through covert means. OFTD tested the capacity and capability of the CBP to detect and interdict nuclear and radiological material attempting to cross the border. Although the OFTD was less than transparent in documenting deficiencies, the GAO findings indicate that the CBP has gaps and deficiencies to detect nuclear material under the test conditions. More troubling, the OFTD (and DHS) does not report to the GAO or Congress if found gaps are closed through appropriate action.

Nuclear and radiological vulnerabilities are not wholly the result of technological deficiency.

The Inadequacy of the Status Quo

Border and POE screening and enforcement appear adequate. A robust DHS directed Automated Targeting System (ATS) acts to rapidly and efficiently screen cargo.[11] Intelligently-assessed (and less risky) legal traffic is expedited for cross-border traffic through numerous special waivers and automation based on changing requirements. Targeting information and advanced algorithms are continuously refined to pinpoint dangerous cargo. Ensuring that legitimate cargo and persons transit borders and POEs not only supports the economic interest of the U.S., it far outweighs any harm

that a few "leakers" might potentially inflict if other internal systems do not mitigate the threat. The U.S., in theory, could absorb the cost of an IND functioning and manage the consequences. Perhaps the cost of a single failure to detect and interdict an IND or nuclear weapon, resulting in nuclear explosion within the U.S., is less than the cost of building the structures and institutions necessary to prevent a nuclear incident.

The amount of illicit contraband entering the United States is manageable. Only by decreasing the demand for illicit goods and contraband will supply stop. No publicly documented or recorded entry or attempt of entry of unauthorized radiological or nuclear material is available. Whether nuclear or radiological monitoring is sufficient in absolute terms is meaningless; it is obviously good enough to deter nuclear smuggling and identify suspicious cargo because there is not a confirmed case of nuclear smuggling across the U.S. border.

Whether nuclear or radiological monitoring is sufficient in absolute terms is meaningless; it is obviously good enough...

Conclusion

The defense of the homeland does not solely reside with CBP administered POEs and borders. The CBP in neither sourced nor expected to be able to implement an impenetrable barrier to unauthorized entry. The CBP is, however, supposed to act as the primary filter that keeps the majority of illicit, illegal, and, otherwise, non-sanctioned activity away from U.S. interests. Nuclear weapons present a special case that demands a 100 percent denial rate into the U.S. At current levels of staffing, training, and equipping, the CBP cannot guarantee a 100 percent nuclear weapon denial rate.

Because of resource availability and the necessity to expedite legitimate transactions, CBP cannot conduct 100 percent inspections of inbound cargo or persons. The task is prohibitive due to resource availability and necessity to expedite legitimate transactions. The volume of cargo traffic and the need to speed perishable goods to market and maintain supply chain viability all work to limit viable options. The CBP, therefore, relies on risked-based targeting to pinpoint suspicious cargo and persons for further examination. Targeting is reliant on numerous cross-referencing systems and predicated on accurate data entry. The ATS does not always "get it right." When cargo is flagged, supply chain disruption costs U.S. and international businesses money and time. When low or no risk cargo is wrongly flagged for high-risk examination, unnecessary disruption occurs. Not identifying high-risk cargo increases the risk that harmful cargo will be allowed into the U.S. Nuclear detection is the most robust architecture in place but has demonstrated vulnerabilities.

Cargo, conveyances, and persons can enter the U.S. illegally. A terrorist trying to bring in a nuclear weapon must skew the odds of discovery to ensure the mission succeeds. The majority of applied research and the subsequent U.S. detection network is tailored for nuclear weapon detection as opposed to chemical or biological agent detection. However, nuclear weapon detection tools along the U.S. border are not perfect. Moreover, the CBP may not conduct follow-up investigations of radiological readings or even use all of the detection equipment available to monitor cargo. A terrorist would not necessarily know when or where the CBP was not following protocols and cannot afford to guess with nuclear cargo. A nuclear smuggler might attempt to shield or disguise the cargo and assemble a device after movement through the border, but such activity increases the risk of detection and would not be preferred. The border is porous to a determined and unencumbered terrorist. Since nuclear weapons tend to be

heavy and their movement is restricted to a conveyance that must pass through POEs or permanent checkpoints, the ability to bring them across the border is limited. However, components and nuclear material are not encumbered by such restrictions.

A review of the DHS fiscal year 2016 budget proposal highlights a commitment to programs designed to provide early warning and detection capability.[12] Over $100 million of the $60 billion DHS budget is earmarked for radiological and nuclear detection equipment, such as portal and handheld monitoring equipment, and $85 million is earmarked for more imaging systems for cargo and conveyances.

As part of its Strategic Vision through 2020,[13] the CBP works with local and tribal officials to counter the growing threat of transnational criminal organizations (TCOs). Transnational criminal organizations dominate the smuggling domain and are increasingly involved in human trafficking. Effective border management must engage whole-of-government approaches, and nuclear weapon detection and interdiction remain critical concerns.

Border security that balances effective nuclear weapon interdiction with supporting the economy is problematic. Dedicated efforts to devise non-intrusive technology that rapidly scans all cargo continues but has not reached acceptable thresholds of capability. Obligating more resources to technological solutions may not achieve any marked increase in effectiveness. Trained personnel are required to use, analyze, and process any detected signals or ATS-flagged cargo and persons. Trained staff do not always use the current equipment available to them. The amount of cargo inspected, ATS-flagged or not, is throttled to match available resources with port throughput. To date, there have been no publicly documented attempts to smuggle a nuclear weapon across the U.S. border. However, a lack of documentation simply acknowledges two possibilities: (1) Either no nuclear weapon smuggling attempts have occurred, or (2) Detection has failed and there is a nuclear weapon somewhere within the U. S.

Terrorists may be deterred from nuclear weapon smuggling attempts because the risk of detection, the technical feasibility of manufacture and employment, and the associated attribution outweigh the possibility of a spectacular attack. A terrorist that perceives the detection network is not robust or susceptible might come to a different risk determination.

U.S. vital interests include security and the economy. The flow of trade is the lifeblood of the economy, and in seeking to guarantee safety, the security apparatus may interrupt the wanted flow. Detection capability and capacity are not sufficient, and personnel do not always use detection equipment or protocols appropriately. DHS and CBP are challenged to maintain pace with increasing populations, migrations, and trade. Nevertheless, until CBP and the interagency close the gaps identified in the nuclear weapon detection meshwork, the U.S. will remain vulnerable to nuclear weapons and materiel moving across a problematic semi-permeable border. ***IAJ***

NOTES

1 Department of Homeland Security, "The 2014 Quadrennial Homeland Security Review," 2014, pp. 63–64.

2 Department of Homeland Security, Global Nuclear Detection Architecture, <https://www.dhs.gov/global-nuclear-detection-architecture>, accessed on April 12, 2017.

3 Committee on Evaluating the Performance Measures and Metrics Development for the Global Nuclear Detection Architecture, 2013, p. 19. The NAS committee was tasked to find metrics. The observation referenced stems from the overall tone of the work that points to an international and interagency coordinating body that must use other organization's budgets to implement the DNDO coordination strategy. NAS found the challenge of assigning performance metrics to DNDO's coordination efforts difficult because the DNDO does not have budget or statutory authority over elements implementing the DNDO's goals.

4 Rebecca Gambler, "Border Security: Progress and Challenges in DHS's Efforts to Address High-Risk Travelers and Maritime Cargo," Government Accountability Office (GAO)-15-668T, testimony before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, House of Representatives, 2015, p. 16.

5 Gene Aloise and Stephen L. Caldwell, "Combating Nuclear Smuggling: Inadequate Communication and Oversite Hampered DHS Efforts to Develop an Advanced Radiological System to Detect Materials," statement for the record to the Committee on Homeland Security and Governmental Affairs, U.S. Senate, 2010, p. 2.

6 David C. Mauer, "Preliminary Observations on the Domestic Nuclear Detection Office's Efforts to Develop a Global Nuclear Detection Architecture," GAO-08-999T, testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC, July 16, 2008, p. 3.

7 Refer to <http://www.dhs.gov/publication/dhs-budget>, FY2003 through FY2016 budget submissions are available with a breakdown of program elements.

8 Department of Homeland Security, Office of the Inspector General, "United States Customs and Border Protection's Radiation Portal Monitors at Seaports," OIG-13-16, <https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-26_Jan13.pdf>, accessed on April 12, 2017.

9 Mauer.

10 Benjamin Lee, "CNS Global Incidents and Trafficking Database 2014 Annual Report," Center for Nonproliferation Studies, 2015, p. 3.

11 DHS/CBP/PIA-006(e), "Automated Targeting System," Privacy Impact Assessment Update, <https://www.dhs.gov/publication/automated-targeting-system-ats-update>, accessed on January 24, 2017.
12 U.S. Department of Homeland Security, "Budget-in-Brief," FY2016, Washington, DC, 2015, <https://www.dhs.gov/sites/default/files/publications/FY_2016_DHS_Budget_in_Brief.pdf>, accessed on April 12, 2017.

13 U.S Customs and Border Protection, "Vision and Strategy 2020," Washington, DC, 2015, <https://www.cbp.gov/document/publications/vision-and-strategy-2020>, accessed on April 12, 2017.

A Nation Unprepared:

Bioterrorism and Pandemic Response

by John B. Foley

In 2001, senior U.S. policymakers converged to participate in the still famous Dark Winter exercise. The exercise contemplated a covert, bioterrorist attack against the U.S. The scenario began with simultaneous attacks, involving smallpox, on shopping malls in 3 separate states, resulting in 3,000 people becoming infected. By the end of the exercise, 16,000 smallpox cases had been reported in 25 states, 1,000 people had died, the healthcare system could not meet the patient load, 10 countries were reporting smallpox outbreaks, and Canada and Mexico had closed their borders. The smallpox vaccine stockpile had been depleted, and new stocks would not be available for a month. States had imposed travel restrictions, and food supplies were dwindling. People were fleeing cities, and the economy was faltering.

Even in 2001, a bioterrorist attack was not simply the stuff of science fiction. Between 1970 and 1998, the U.S. recorded over 400 suspected terrorist activities involving chemical or biological agents. In the immediate aftermath of Dark Winter exercise, the U.S. grappled with the 2001 Amerithrax attack on government offices in Washington and subsequently opened the treasury's floodgates to address the shortfalls revealed both by the Dark Winter exercise and the Amerithrax attack. However, a decade and a half later, as the nation faced the 2014–2016 Ebola crisis, assessments of the U.S. government response led to a sobering conclusion: The U.S. still has not learned the lessons of Dark Winter.

Transporting Infected Persons

In the spring of 2014, the first reports of an Ebola outbreak in West Africa came from Guinea. The virus quickly spread throughout the West African countries of Sierra Leone, Liberia, Nigeria, Senegal, and Mali. Of the more than 10,000 people infected with the Ebola virus, more than half died.[1] The initial response by the international community was viewed as a failure. President Obama declared the Ebola outbreak a top national security priority.[2] What had been a distant public health crisis had now been elevated to a national security threat. Obama ordered U.S. troops to West Africa

John B. Foley, Lieutenant Colonel, U.S. Army, Ret., serves at the National Guard Bureau, J39 Combating Weapons of Mass Destruction. He received a M.S. in WMD Studies as a National Defense University Countering WMD Graduate Fellow.

in September to provide humanitarian assistance. U.S. efforts in West Africa centered on containing the epidemic and limiting the spread of disease. The Department of Defense (DoD) spent almost $400 million in its response support. The Ebola outbreak became the predominant news story, and bodies of Ebola victims lying in the streets greeted news watchers. The Centers for Disease Control and Prevention (CDC) assured the public that the U.S. healthcare system could deal with any outbreak.

In 1978, the U.S. military developed a patient transport capsule that could safely contain an individual exposed to highly infectious diseases like Ebola.

The U.S. military had worked with highly infectious agents like Ebola for many years. Treating highly infectious patients required the highest isolation standards. In 1978, the U.S. military developed a patient transport capsule that could safely contain an individual exposed to highly infectious diseases like Ebola. These isolation capsules were part of the Aeromedical Isolation and Special Medical Augmentation Response Team (AIT-SMART). An AIT-SMART team could transport one infected patient directly into a Biosafety Level 4 (BSL-4), the biosafety level at which the deadliest pathogens can be safely contained, and two such teams could be deployed simultaneously.[3] Given the number of persons likely to be affected by any bioterrorist attack, the idea that this capability could be applied to a mass-infection scenario seems almost farcical. When AIT-SMART teams were retired in 2010 and replaced by U.S. Air Force Critical Care Air Transport Teams (CCQTs), patient capacity expanded from one to five ventilator patients or ten less-critical patients. Naturally, even this tenfold capability increase did nothing to address the mass-infection problem.

Disease Recognition and Response Training

Even a limitless transportation capability is potentially useless unless infected persons can be properly identified. Ebola entered the U.S. hitchhiking in the living cells of an international traveler. The first reported U.S case of Ebola came on September 30, 2014 in Dallas. A man who had recently returned from Liberia became ill. A week later, he was dead. Two of the man's healthcare providers developed similar symptoms. Although they were treated and recovered, both lacked the requisite knowledge and training needed for isolating patients infected with such a deadly pathogen. Protective barrier requirements established for deadly pathogens such as Ebola were nonexistent. Personal protective equipment was inadequate. Isolation of the patient was done in a facility that was not equipped to contain the pathogen. So simple a matter as patient waste removal became a major bureaucratic challenge. Poorly executed coordination and communication between federal and local officials resulted in unnecessary delay in cleanup and disposal of hazardous waste from the victim's apartment. The victim's family was kept in quarantine by law enforcement. Compounding the various local miscues, the CDC itself was forced to revise its previously published guidelines and protocols for the treatment of Ebola patients. The CDC now assessed that it was possible to become infected from droplets up to three feet away.[4]

A subsequent case of Ebola was diagnosed in in a New York City healthcare worker who had returned from abroad. After several days in New York, he developed a fever, notified city health authorities, and was immediately put in isolation. The governors of New York and New Jersey responded by imposing 21 day quarantines on any medical workers returning from countries

affected with Ebola. Conflicts soon arose between the states and the federal government. The federal guidelines called for individuals to self-monitor for fever and regularly report their status to local health departments for 21 days. Reports circulated that people were afraid to ride the subway for fear of catching Ebola. Additional cases of Ebola infection were treated in specialized isolation facilities at Emory University Hospital, Nebraska Medical Center, and at the National Institutes of Health (NIH). By this point, Dr. Francis Collins, the Director of NIH, observed, "We need to take this current outbreak as a wake-up call. Diseases will come, and we have to be prepared, by investing in the public health infrastructure that keeps America safe."[5]

Following the Ebola crisis, two subcommittees (Emergency Preparedness Response and Communications) of the House Committee on Homeland Security assembled to investigate U.S. preparedness for a biological attack. Representative Martha McSally (R-Arizona) raised concern that a terrorist organization could launch a bioterrorist attack against the U.S. homeland. She said, "The risk of a biological terrorist attack to America is an urgent and serious threat. A bio attack could cause illness, and even kill hundreds of thousands of people, overwhelm our public health capabilities and create significant economic, societal and political consequences. Our nation's capacity to prevent, respond to and mitigate the impacts of biological terror incidents is a top national priority."[6]

While the Ebola crisis did not mushroom into a pandemic, it is not clear how much was due to preparedness as opposed to an enormous turn of good luck—as seductive as it might be to assume otherwise.

The Interagency Problem

Remarkably, there is not a single official who ensures that all agencies of the federal government work together on biodefense, even though at least five federal departments that have significant responsibilities in the event of a bioterrorist incident. A covert, bioterrorist attack would require a whole unity of effort response by the U.S. Presidential Decision Directive (PDD)-39 attempted to address this concern. PDD-39 specifies how federal agencies are to divide responsibilities among themselves with respect to weapons of mass destruction exercises and incidents.[7] It assigns central roles to the Federal Bureau of Investigation (FBI) and Federal Emergency Management Agency (FEMA) in the federal response to any terrorist event that results in mass casualties—the FBI as the lead agency for crisis management and FEMA as the lead agency for consequence management

While the Ebola crisis did not mushroom into a pandemic, it is not clear how much was due to preparedness as opposed to an enormous turn of good luck...

of mass casualty events. However, epidemic crisis management is not something that the FBI does daily. Likewise, FEMA does not have the skill, the correct personnel, or the authority and responsibility to act as a trusted agent when it comes to coordinating the necessary public health response required to mitigate an epidemic. FEMA is structured to deal with things such as earthquakes, floods, hurricanes, and tornados involving mass casualties, but not events involving biohazards. Responsibility for planning, equipping, and training requirements likewise must be identified. However, PDD-39 does not address how the U.S. should prepare for a covert, biological event. It does not provide guidance on how to improve existing efforts that were in place or identify areas that could be improved. Moreover, because it states that agencies "will bear the costs of the participation

in terrorist incidents and counterterrorist operations, unless otherwise directed,"[8] bureaucratic inertia and protectiveness of budgets serve to create a disincentive for interagency cooperation.

In an effort to move forward in a coordinated, unified fashion, President Obama named an Ebola "Czar"[9]; however, the temporary nature of the positon lacked the authority or power to bring about change. This situation called for the designation of a single responsible federal official to coordinate authority and make executive decisions across the interagency with respect to the biodefense enterprise.

The federal government does not lack funding to protect against bioterrorism as much, it would appear, as it lacks a coordinated investment strategy.

Budgeting to Protect against Bioterrorism

The federal government does not lack funding to protect against bioterrorism as much, it would appear, as it lacks a coordinated investment strategy. The present piecemeal approach to biodefense preparedness opens the possibility to numerous acquisition problems, including duplication of purchases, over or underestimation of requirements, purchasing improper equipment, and mismanagement of inventory.

- The Department of Homeland Security (DHS) was appropriated $47 million in supplemental funding to prepare for a pandemic. It spent this funding on personal protective equipment, research, and exercises. In 2014, an audit conducted by the DHS Inspector General found that DHS had not effectively managed pandemic personal protective equipment and antiviral medical countermeasures. DHS did not adequately conduct a needs assessment prior to purchasing personal protective equipment and medical countermeasures.[10]

- Following the 2001 anthrax letter attacks, Congress appropriated almost $3 billion to counter biological threats against the populace. The appropriation included over $1 billion to purchase antibiotics and vaccines as part of the Strategic National Stockpile (SNS). The CDC was tasked with determining the most probable and dangerous biological threat to the civil populace. The CDC used the following criteria set to make their determination:[11]
  - Impact on public health based on death and illness.
  - Ease of delivery to a large population. The stability of the agent, ability to mass produce and distribute and the R_0, its potential for person-to-person transmission of the agent.
  - Public fear perception and potential civil disruption.
  - Special public health preparedness requirements based on stockpile requirements (vaccines), enhanced surveillance, or diagnostic needs.

- In 2002, Congress also earmarked $1 billion for state-level public health system improvements.

- The Project BioShield Act of 2004 authorized the U.S. government to spend $5.6 billion over 10 years to acquire medical counter measures.[12]

The biodefense enterprise budget witnessed a huge increase in funding from FY 2001 to FY 2014, with civilian biodefense funding totaling $78.8 billion. Of this, $64.93 billion went to programs that included both biodefense and non-biodefense lines of effort. The remaining $13.89 billion went for programs which are

solely dedicated to biodefense.[13] A closer look at the FY2001–FY2014 Civil Biodefense Funding shows that approximately $80 billion was spent on biodefense from FY2001 through FY2014. The majority of those expenditures went toward multi-hazard programs, and only about 17 percent went toward biodefense as such.

Although the biodefense enterprise receives multiyear funding for some of its programs, it receives only annual appropriations for others. A case in point is Project BioShield. This annual appropriation approach stymies strategic planning and execution to prepare programs for such things as changing political priorities and continuing budget resolutions. Moreover, budgets for the biodefense enterprise are difficult to predict from year to year. For example, the CDC's FY2014 proposed budget was $47.7 million less than its FY2013 budget. Three of the CDC's biodefense programs had significant reductions. The State and Local Preparedness and Response Capability, which includes the Public Health Emergency Preparedness (PHEP) cooperative agreement grant program, was reduced by $8.2 million to $658 million. PHEP provides funding for public health departments to upgrade their ability to respond to public health threats such as natural disasters, infectious diseases, and nuclear, biological, and chemical events. This was a 30 percent reduction from FY2002 funding. The SNS's funding was also reduced by $38.4 million to $510.3 million, and the CDC Preparedness and Response Capability would be reduced by $1.1 million. Thus, enormous appropriations notwithstanding, a lack of a comprehensive investment plan, based on a strategic vision not subject to annual caprice, makes it impossible to determine if the biodefense enterprise is adequately funded.

A Strategic Approach

A lack of a strategic vision as to what exactly biodefense seeks to accomplish is the greatest barrier to the success of interagency efforts at biodefense. The old maxim that "defense does not win wars" should not be ignored by biodefense planners. History is replete with examples of strategies that circumvented known defenses. If the nation is well protected against, for example, anthrax or smallpox, an intelligent adversary would not attack with anthrax or smallpox when nature is replete with a wide range of pathogens that could be considered for use against humans. Novel viruses and new disease continue to emerge, and advances in biotechnology make it possible to manipulate how a virus behaves. Biological weapons programs, once only the domain of state-sponsored research organizations, are now within the reach of non-state actors. An individual with a graduate-level degree has all the tools and technologies to implement a sophisticated program to create a bioweapon.[14] The costs associated with the setup and operation of facilities to explore, develop, and cultivate biological hazards are within the reach of well-funded terrorist organizations. A terrorist organization with several hundred thousand dollars, a dedicated group of graduate-level students, and a space of several hundred square meters could establish a small-scale biological weapons program.[15]

Biological weapons programs, once only the domain of state-sponsored research organizations, are now within the reach of non-state actors.

On the other hand, the U.S. government has made significant strides in biodefense. It has actively pursued efforts at the federal level and in concert with the states to deter, protect, and respond to a biological event. Funding has been appropriated to provide for the infrastructure, training, and equipping of local, state, and national responders. National-level exercises

have been conducted to test and refine local, state, and national level response.

The CDC has consolidated various bio surveillance programs into its National Electronic Surveillance System (NEEDS). This consolidation resulted in reducing confusion and easing the reporting process. All 50 states and the District of Columbia use a NEEDS-compatible system.[16]

The CDC has provided grants for states to upgrade their laboratories forensic capabilities. The Laboratory Response Network was set up to provide local and state laboratories a rapid confirmatory process of suspected pathogens. The CDC and NIH continue research efforts on vaccines against diseases that have the potential to be weaponized.

DoD hospitals, as well as the health facilities of the Veterans Affairs (VA), can be called upon in the event of a national emergency.[17]

All 50 states have plans in place that provide a framework to respond to a biological event.

The Department of Justice (DOJ) has provided biological terrorism training to law enforcement personnel and first responders. DOJ has also provided grants to states and cities to purchase personal protective gear for law enforcement and first responders.

DHS has developed a strategy toward improving the health security of the nation. The National Health Security Strategy (NHSS), published in 2010, provides for a unified approach for improving the health security of the nation. This unified approach relies heavily on the collaborative efforts of government agencies, community organizations, private enterprise, and academia. The NHSS lines of effort focus on community resilience, public health emergency medical countermeasures, health situation awareness, and healthcare coalitions. Community partners have made significant progress in health security improvement. There are now more than 24,000 members in the Hospital Preparedness Program. Of the nation's 6,340 hospitals, 5,288 are affiliated with the Hospital Preparedness Program.[18] This consortium has significantly improved hospital to hospital and responder to hospital communication capabilities. Critical information regarding the availability of resource and beds can now track critical data when trying to determine where to route ambulances. These partnership programs have resulted in stronger state and local public health agencies. Federal preparedness grants from Department of Health and Human Services and FEMA have benefited states and local communities' ability to respond to a bioterror event.

The National Response Framework (NRF) incorporates plans from the interagency. These interagency plans become the supporting plans or operational supplements to the NRF. Even though the NRF takes an "all-hazards" approach to consequence management, it is intended to be sufficiently flexible to orient interagency efforts to respond even to a bioterror attack.

All 50 states have plans in place that provide a framework to respond to a biological event. All states have a SNS plan in place. These all-encompassing plans detail the receipt, storage, and distribution of the SNS push packages. Some states that have either large metropolitan statistical areas or large cities have plans in place supporting the Cities Readiness Initiative. The Cities Readiness Initiative, located in 72 cities, provides coverage to roughly percent of the U.S. population.[19] In important ways, therefore, federal investments have increased the country's ability to respond to a bioterrorists attack. Biodefense funding has provided states and local communities the means to improve their public health networks preparedness and response capabilities. First responders and law enforcement have been trained and equipped to respond to a bioterrorist event. State and local

emergency management planners have developed plans to mitigate a bioterrorist event.

Conclusion

In the final analysis, however, the U.S. government is still haunted by, and should give heed to, the principal lessons of Dark Winter:

- The nation still lacks sufficient drugs and vaccines to mitigate an epidemic—which it must have, if for no other reason than as a deterrent against the possibility of an informed adversary attacking with pathogens against which the U.S. is already protected.
- The nation's healthcare cadre is inadequately trained and equipped to confront a major bio-attack.
- The nation's healthcare system lacks adequate surge capacity.
- Lines of authority across the interagency for responding to bioterrorism are ill-defined at best, and centralized leadership and coordinating authority is not firmly in place.
- Coordination efforts at all levels must thoroughly integrate medical expertise.
- Means for ensuring the accurate and timely dissemination of public information must be refined.

Failure to heed these lessons simply leaves the U.S. vulnerable, beyond what prudent risk management would suggest, to the threat of bioterrorism.

The U.S. has never had a bioterror attack that has resulted in an epidemic. The U.S. has had hundreds of suspected terrorist activities that have involved chemical or biological agents. The Anthrax attack mailings, coming just weeks after the attacks of 9/11, demonstrated how vulnerable the U.S. was to a bioterror attack. The federal response to the Anthrax attacks was so fraught with problems and ineptitude, it warranted the government's watch dog agency to proclaim that "the response was not only problematic but the response clearly indicated that the U.S. was not prepared for a terrorist biological attack." The world's largest outbreak of Ebola in West Africa gripped the world's attention and revealed troubling gaps and seams in federal bioterrorism response capabilities even though, despite collective miscues at all levels of government, only one fatality occurred.

The U.S. has conducted a massive effort to prepare the nation to respond to a bioterrorist event against several known weaponized pathogens. Billions of dollars have been spent on biodefense programs, but a very low percentage of those funds have gone toward the biodefense of the civil populace—the sole and proper object of biodefense in the first instance. Sir Ernest Rutherford is reputed to have once said, "we haven't the money, so we've got to think."[20] It may be that no amount of money will adequately substitute for the imperative to think. In any case, instead of waiting for a real "dark winter" to occur, serious thinking—in a coordinated manner across the interagency—about the bioterrorism problem is much needed and long overdue. ***IAJ***

NOTES

1 Salaam-Blyther Tiaji, "U.S. and International Health Responses to the Ebola Outbreak in West Africa," Congressional Research Report, Congressional Research Service, October 29, 2014.

2 Daniel Halper, "Obama: 'Ebola A Top National Security Priority,'" *The Weekly Standard*, October 2014, <http://weeklystandard.com/blogs/obama-ebola-top-national-security-priority/article/808599>, accessed on August 26, 2014.

3 George Christopher, "Air Evacuation under High-Level Biosafety Containment: The Aeromedical Isolation Team," *Emerging Infectious Diseases*, Vol. 5, No. 2, 1999, pp. 241–242.

4 Siobhán O'Grady, "What Did the U.S. Learn from Ebola? How to Prepare for Bioterrorist Attacks," *Foreign Policy*, April 2015, <http://foreignpolicy .com/2015/04/23/what-did-the-u-s-learn-from-ebola-how-to-prepare-for-bioterrorist-attacks/>, accessed on August 12, 2015.

5 Rosa Delauro, "Ebola: A Preventable Catastrophe," *Huffington Post*, October 14, 2014, <http://huffingtonpost.com/rep-rosa-delauro/ebola-a-preventable-catas_b_5977808.html>, accessed on August 28, 2015.

6 Amanda Vicinanzo, "Biological Terrorist Attack on US an 'Urgent and Serious Threat,'" *Homeland Security Today*, April 23, 2015, <http://hstoday.us/briefings/daily-news-analysis/single-article/biological-terrorist-attack-on-us-an-urgent-and-serious-threat/0ce6ebf3524d83c537bif4f0cc578547.html>, accessed on August 23, 2015.

7 Richard A. Falkenrath et al., *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack*, MIT Press, Cambridge, MA, 1998, pp. 269–274.

8 Ibid.

9 Carol L. Lee, "Obama to Name Ron Klain as Ebola Czar," *The Wall Street Journal*, October 17, 2014, <http://www.wsj.com/articles/obama-to-name-ron-klain-as-ebloa-czar-1413557184>, accessed on August 6, 2015.

10 "DHS Has Not Effectively Managed Pandemic Personal Protective Equipment and Antiviral Medical Countermeasures," Department of Homeland Security Office of the Inspector General, U.S. Department of Homeland Security, August 1, 2014, <http://oig.dhs.gov/assests/Mgmt/2014/OIG_14-129_Aug14.pdf>, accessed on September 12, 2015.

11 Malcom Dando, *Bioterror and Biowarfare*, Oneworld Publications, Oxford, 2006, p. 62.

12 Bruce Maxwell, *Homeland Security: A Documentary History*, CQ Press, Washington, DC, 2004, pp.327–328.

13 Rebecca Katz, "Biological Weapons: A National Security Problem that Requires a Public Health Response," Working Paper 2001–2004, Office of Population Research, Princeton University, Princeton, NJ, 2004, p. 198.

14 "U.S. Unprepared for Biological Attack," *Homeland Security News Wire*, December 1, 2011, <http://homelandsecuritynewswire.com/dr20111201-u-s-unprepared-for-biological-attack>, accessed on October 5, 2015.

15 James Jay Carafano, Ph.D., "Improving Federal Response to Catastrophic Bioterrorist Attacks: The Next Steps," The Heritage Foundation, November 13, <http://heritageorg/research/reports/2003/11/improving-federal-response-to-catastrophic-bioterrorist-attacks-the-next-steps>, accessed on August 28,

2015.

16 "Today, all 50 States and Washington, DC Use a NEDSS-Compatible System to Send Case Notification to NNDSS," Centers for Disease Control and Prevention, <http://cdc.gov/nndss/nedss.html>, accessed on August 31, 2015.

17 Carafano.

18 "2015 National Preparedness Report," Federal Emergency Management Agency, March 30, 2015, <http://fema.gov/media-library-data/1432751954859-fcaf2acc365b5a7213a38bbeb5cd1d61/2015_NPR_508c_20150527_Final.pdf>, accessed on August 16, 2015.

19 Jacqueline Langwith, *Bioterrorism*, Greenhaven Press, Farmington, MI, 2008, pp. 162–163.

20 Sir Ernest Rutherford, quoted by R.V. Jones, *Bulletin of the Institute of Physics*, 1962, Vol. 13, No. 4, p. 102, <http://todayinsci.com/R/Rutherford_Ernest/RutherfordErnest-Quotations.htm>, accessed on January 16, 2016.

Plutonium and Picasso – A Typology of Nuclear and Fine Art Smuggling

by Joshua D. Foss

The global security environment continues to evolve. Globalization, advances in technology, and greater connectedness of people and economies have enabled transnational organized crime and new and existing illicit markets to expand. Never has the prolific and rapid dissemination of technology and information enabled transnational organized criminals and terrorists to work together at such a speed and scope. Nefarious actors undertake a broad range of illicit activities—to include human smuggling, software and music piracy, illegal wildlife trade, product counterfeiting, and fine art smuggling—to exploit global advancement and global interconnectedness for financial gain. Persons not directly affected by these smuggling activities may see them as benign (as in the case of music piracy) or as cases of lawlessness (as in the case of illegal wildlife trade) or even as cases of human tragedy (as in the case of human trafficking), and indeed, they are all of these things. However, close examination of illicit activities like these reveals profound implications and consequences for U.S. national security. For example, consider a terrorist organization using the proceeds from illicit trafficking of pirated music to finance terrorist recruitment and procurement of weapons. The illicit trafficking of pirated music could fund terrorist operations against U.S. Soldiers abroad or against the U.S. homeland. Thus, the seemingly benign threat of pirated music could affect U.S. national security and U.S. interests around the world.

Some smuggled goods such as illegal arms trafficking and radiological and nuclear material trafficking, are obvious threats to national security. Anecdotal evidence shows that characteristics associated with smuggling and trafficking of nuclear material are no different than the characteristics associated with smuggling and trafficking other illicit commodities. This commonality allows us to identify a typology among the illicit trafficking of humans, drugs, weapons, fine art, and nuclear material. Lessons from one of these forms of illicit trafficking are applicable to all, and that commonality can provide important insights in support of interagency efforts to counter illicit trafficking.

The illicit black market is a global enterprise that according to some estimates generates between $1.63 trillion and $1.98 trillion annually.[1] Commodities found in illicit markets include drugs,

Joshua D. Foss is a WMD Analyst at Defense Threat Reduction Agency. He received a M.S. Degree in WMD Studies as a National Defense University Countering WMD Graduate Fellow.

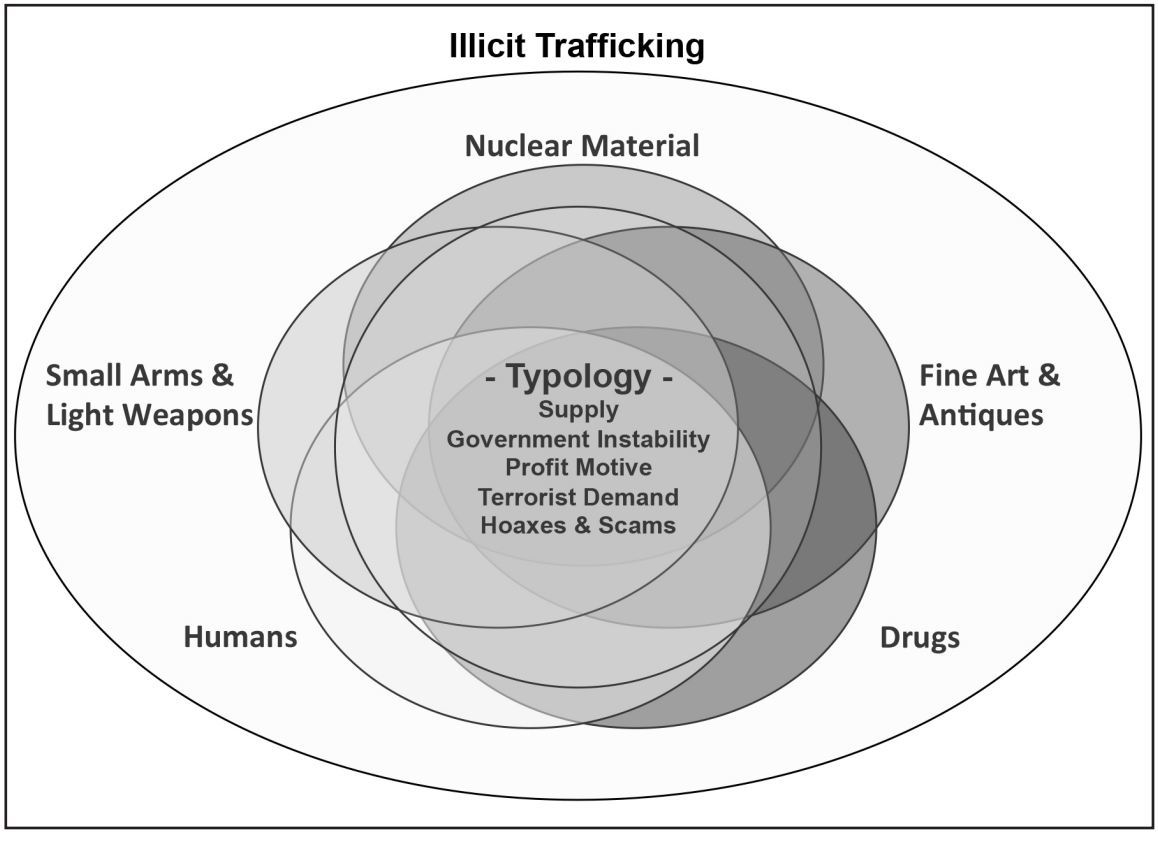


Figure 1. Illicit Trafficking

counterfeit products, arms, cigarettes, diamonds, humans, oil, exotic wildlife, fine art, and nuclear material. These commodities—for all their differences—exhibit certain remarkable similarities. For example, both fine art and nuclear material are physical, inanimate items that are generally safeguarded and secure; require extraordinary physical access to steal; are generally small and portable; can be obtained illegally only within the bounds of well-defined parameters; and have a niche demand and market. Thieves generally have a hard time finding buyers for stolen nuclear material and fine art. Generally, the more famous the art piece or art heist, the harder it is to sell in both licit and illicit markets. Similarly, selling nuclear material is also a challenge in the underworld of the black-market exchange. Without receiving the attention of intelligence or law enforcement agencies, identifying demand or the end-user of stolen nuclear material can be a challenge. More often than not, original sellers of nuclear material rarely find a single buyer of the material.[2] These similarities provide at least five interesting bases for comparison:

1. Supply.
2. Government instability.
3. Profit motive.
4. Terrorist demand.
5. Hoaxes and scams.

Supply

While the exact quantity of fine art and nuclear/radiological material around the globe is unknown, both are large. However, neither fine art nor nuclear/radiological material is easily acquired, since both are generally well protected and access to them is restricted. Nevertheless, there is no shortage in supply for would-be smugglers of fine art and nuclear/radiological material to exploit, and this abundance presents an opportunity for would-be traffickers.

...most art is stolen from private residences, followed by museums and galleries, churches, and companies.

According to the Art Loss Register—the world's largest private database of lost and stolen art, antiques, and collectibles—most art is stolen from private residences, followed by museums and galleries, churches, and companies. These thefts result in billions of dollars of fine art theft each year.

Though private companies, such as the Art Loss Register, and law enforcement entities around the globe try to maintain records on stolen art, the illicit art trade is much larger than documented. Recordkeeping inconsistencies and the inability to include the uncatalogued artifacts that are stolen from archaeological sites make having a complete picture of the size and scope of stolen art a challenge.

According to the International Atomic Energy Agency (IAEA), millions of radiological sources have been distributed worldwide over the past 50 years, with hundreds of thousands currently being used, stored, or produced.[3] The common use of radiological sources worldwide presents an opportunity for the theft and acquisition by would-be nuclear traffickers. A nuclear trafficker could acquire or pilfer radiological material through licensing fraud and from a variety of places, such as universities and hospitals.

In addition to radiological material, fissile nuclear material likewise exists in abundance. Many tons of highly enriched uranium (HEU) and plutonium (Pu) are processed and stockpiled in bulk each year by several countries. As with fine art, there is no current comprehensive, authoritative inventory of HEU globally; however, estimates of global HEU is estimated at 1,345 tons with almost 99 percent of the HEU in nuclear weapon states.[4] Seizures of fissile nuclear material is rare on the illicit black market but not non-existent. The IAEA reports 15 confirmed incidents of unauthorized possession of HEU and Pu between 1993 and 2012. Cumulatively, these incidents included a total of about 20 kg of weapons-usable nuclear material. According to the Database on Nuclear Smuggling, Theft, and Orphan Radiation Sources, the most recent nuclear smuggling event occurred in 2011, when Moldovan police arrested six people for attempting to sell four grams of HEU.[5] The traffickers thought they were negotiating with a North African buyer and were selling the HEU from between $29 million and $144 million per kilogram [6]—highlighting that a paucity of confirmed incidents does not indicate a paucity of demand.

Government Instability

Both nuclear and art traffickers thrive in struggling nations, particularly those weakened by civil war, insurgency, poverty, and corruption. Criminals profit from instability, where control of governance is weak, security is inadequate, and other dimensions of state control and structure are poor.

As countries become plagued with conflict and political strife, the difficulty and challenge of protecting art, antiques, and cultural artifacts increase. Robert Wittman, the founder of the

FBI's Art Crime Team identifies that "semi-lawless, war-torn regions have long been vulnerable" to illicit art and antiques trade.[7] Both Iraq and Syria serve as great examples of the correlational relationship between fine art trafficking and government instability. The FBI has alerted art collectors and dealers to be cautious trading Near Eastern antiques, warning that artifacts plundered by terrorist organizations such as Islamic State in Iraq and the Levant (ISIL) are entering the marketplace.[8] ISIL and similar groups are exploiting the instability in Iraq and Syria—a region rich with ancient treasures and artifacts—by profiting from stolen fine art in the region.

Government instability likewise enhances opportunity for the illicit transfer of nuclear materials. The most nuclear trafficking events occurred during the early 1990s in Eastern Europe and former Soviet Union. The IAEA's Incidents Trafficking Database dramatically peaked in the early 1990s, concurrent with the fall of the Soviet Union. Between 1992 and 1994, 300 employees at storage and production facilities in Russia were caught stealing, illegally transporting, or possessing radioactive waste.[9]

Conflict or post-conflict areas are particularly vulnerable to nuclear theft and smuggling. The conflicts in Iraq and Libya serve as great examples of this correlational phenomenon. After the U.S. invasion of Iraq in 2003, looting of Iraq's nuclear infrastructure became a nuclear proliferation and trafficking concern for the U.S.

During Libya's civil war in 2011, the international community became increasingly concerned about nuclear proliferation as a result of government instability. Lawlessness and the absence of state-controlled security and order led to the theft and looting of Libya's nuclear infrastructure and material holdings. Because of Libya's civil war, 1,000 metric tons of yellowcake was abandoned and came into the possession of rebel fighters.[10]

Profit Motive

The single most prominent motive for art theft is profit. The amount of criminal income generated by art crime each year is estimated at $6 to $8 billion.[11] A single stolen painting can earn a trafficker millions of dollars. For instance, in 2004, two paintings—Edvard Munch's *Scream* and *Madonna*—stolen from the Norwegian Munch Museum had an estimated value of around $19 million. Although the paintings would be recovered two years later, the theft demonstrates the significant value fine art can potentially generate for art thieves and smugglers.[12] In the art world, a single set of pliers and a screw driver have been used to steal millions dollar paintings for fine art traffickers.[13]

The most nuclear trafficking events occurred during the early1990s in Eastern Europe and former Soviet Union.

In a similar way, the expectation of financial gain from selling nuclear material on the black market is the primary motivation for nuclear theft. Nuclear proliferation expert Lyudmila Zaitseva identifies profit as the number one motive for stealing nuclear/ radiological material.[14] Most known thefts of actual weapons-usable nuclear material have been committed by impoverished insiders with the hope of selling nuclear material on the black market.[15] In 1992, Leonid Smirnov, the first known thief of weapons-usable nuclear material, diverted 1.5 kg of HEU from the Luch Scientific Production Association in Podolsk, Russia, to improve his financial situation. Smirnov, a technician at the nuclear facility, stole the HEU in 25-30 gram increments. Investigation of the theft reveals that Smirnov intended to sell the material to make enough money to buy a new stove and

refrigerator.[16] The Smirnov case is just one of many cases involving the theft and illegal acquisition of nuclear material for financial gain.

Given the demand of nuclear/radiological material and fine art by terrorists, the international community has developed legal instruments to prevent terrorist access to and use of both commodities…

Terrorist Demand

The biggest enabler of terrorism is money; the theft and trafficking of stolen art is one of the many illicit activities terrorist undertake to fund their efforts. Terrorist desire both fine art and nuclear material. Perhaps the best-known example of terrorist connection between terrorism and illicit art comes from the 9/11 hijacker, Mohammed Atta. In 2005, the German secret service reported that Atta, in an attempt to fund's terrorist activity, tried to sell Afghan antiques to a German professor. ISIL reportedly have earned as much as ten million U.S. dollars from fine art stolen from Syria and Iraq.[17] Matthew Levitt of the Washington Institute for Near East Policy told a House Congressional committee that the sale of antiques—both those stolen from collections and those from archeological sites—was the group's second-large source of revenue after illicit oil sales.[18]

Several international legal instruments have been adopted to prevent and reduce stolen fine art and nuclear/radiological material being introduced on the black market. In February 2015, the United Nations Security Council unanimously voted for Resolution 2199, which obligates member states to take steps to prevent terrorist groups in Iraq and Syria from receiving donations and from benefiting from trade in commodities, like fine art and antiques. This action was intended to curb art theft and prevent revenue streams by terrorist organizations in Iraq and Syria.[19] Similarly, in 2005, the UN recognized the terrorist demand for nuclear/radiological material and the threat that material posed. As a result, the International Convention for the Suppression of Acts of Nuclear Terrorism is a legal instrument developed to address the threat. Under this convention, member states would have an obligation to criminalize a wide range of activities involving nuclear/radiological material.[20] Given the demand of nuclear/radiological material and fine art by terrorists, the international community has developed legal instruments to prevent terrorist access to and use of both commodities, be it for profit or to cause terror.

Terrorist groups have also demonstrated a demand for nuclear material and have made serious attempts to acquire nuclear material since at least 1993. Long before the 2003 *fatwa*—which Osama bin Laden received from Shaikh Nasir bin Hamid al-Fahd, a radical Saudi Islamic scholar justifying the permissibility of nuclear weapons under Islamic law—global jihadist networks have made explicit their desire for nuclear weapons for use against the U.S. and its allies.[21] Bin Laden called the acquisition of weapons of mass destruction a "religious duty," and *al-Qaeda* operatives have made repeated attempts to buy stolen nuclear material in order to make nuclear weapons.[22] Though Bin Laden was killed in 2011, *al-Qaeda* and similar groups may still continue to pursue nuclear efforts. For instance, the emergence of the apocalyptic and political-religious group ISIL may have no reservations against employing an improvised nuclear device. Although no open source evidence links terrorist organization with cases of illicit trafficking of fissile material, ISIL's radical and apocalyptic agenda may increase the possibility of future nuclear smuggling and nuclear terrorism.[23]

Hoaxes and Scams

The black market of stolen fine art and nuclear material is fraught with hoaxes and scams. Fraudulent dealers and scam artists recognize that stolen art and nuclear material are potential lucrative markets. Most fine art scams involve the replication of fine art to sell in both licit and illicit markets. The replication of art is commonly referred to as forgery. A scam artist can forge fine art in several different ways. Forgery can be a direct copy of an art piece, attempting to complete an accurate recreation of a known existing piece of art, or it can be pastiche, where an art forger takes elements and style and patches them together in such a manner to capture the era.[24] For nuclear material scams, the most prevalent scam on the black market is sellers misrepresenting their wares using hoax non-nuclear material. Scam artists attempt to sell non-nuclear material as nuclear material to unwitting buyers. The propensity for fraud, hoaxes, and scams are high in the underworld of illicit black markets because black markets operate on a level beneath legitimate markets and are not regulated. The relative ease of misrepresenting factual information and products makes scams and hoaxes considerably more prevalent than instances where actual fine art and antiques and nuclear material is undertaken.

Parallel factors contribute to the abundance of hoaxes and scams found in the underworld of nuclear/radiological smuggling and fine art smuggling. The act of procuring nuclear/radiological material and stolen art on the black market is a criminal act. Reporting fraudulent nuclear/radiological or art to authorities would self-incriminate and expose the illicit activity. There is, generally, no formal, legal dispute settlement procedures or legal recourse when a procured item is found to be fraudulent.

The sale of counterfeit art is reported to generate tens of millions of dollars each year. A factor that contributes to the abundance of forged art on the black market is the lack of technical expertise and the inability to properly authenticate fine art. The underworld of art smuggling requires a higher level of understanding and expertise to authenticate stolen art. The current system of fine art authentication is based on a three-pillar approach of connoisseurship, provenance, and technical analysis.

Fraudulent dealers and scam artists recognize that stolen art and nuclear material are potential lucrative markets.

For connoisseurship, an expert can distinguish fraudulent art and antiques with training in characteristic features of an artist's style and techniques. Through provenance, an authenticator evaluates the history of an artwork's origin, ownership, location, and transaction. Technical analysis allows for scrutiny with scientific equipment of a work's material components to determine consistency or inconsistency with a purported era, age, or attribution.[25] Ironically, as with the authentication of nuclear/radiological material, proper and thorough authentication of art requires special equipment for technical analysis to determine authenticity. Scientific methods such as carbon dating and various tests involving X-rays are used for authentication. The lack of proper authentication allows forgers to flood both the licit and illicit market with forged art.

Similar to the authentication of fine art, to ensure its *bona fides*, nuclear/radiological material must also be authenticated on the black market. The authentication of nuclear/radiological material requires a level of technical expertise and a basic understanding of nuclear properties to differentiate nuclear and nonnuclear material. Failure to properly authenticate

nuclear/radiological material can result in being scammed.

To ensure the legitimacy of nuclear/radiological material on the black market, one must understand nuclear material and have proper equipment, such as radiation or gamma and neutron detectors to test and verify the properties of the material. Proper authentication is vital for nuclear/radiological verification and possibly something terrorists lack. For instance, according to former CIA Director, John Brennan, *al-Qaeda* has "been scammed a number of times" in its quest for nuclear material.[26] As previously identified, *al-Qaeda* is reported to have searched for weapons-grade nuclear material in the 1990s, but was conned into buying low-grade or hoax material, such as "red mercury."[27] In 1993, *al-Qaeda* operatives in Sudan sought to purchase what they believed was uranium being offered for sale but ultimately proved to be a scam.[28] Though *al-Qaeda* may have been scammed on a number of occasions with fake nuclear/radiological material, these scams pose a threat because it shows *al-Qaeda's* quest for nuclear material.[29]

...al-Qaeda has "been scammed a number of times" in its quest for nuclear material.

Over the last 25 years, several reoccurring non-nuclear material scams have occurred on the nuclear black market. These scams include the sale of lead pigs containing hoax nuclear/radiological material and the sale of "red mercury," as identified above. Lead pigs—a colloquial term describing a nuclear container—is used to ship or store radioactive material. For instance, one such persistent scam, primarily centered in Southeast Asia included the sale of irregular shaped metal pigs allegedly containing HEU or Pu with the markings of "uranium," "made in USA," or a skull-and-crossbones symbol.[30] Generally, the contents of the pig would be non-nuclear hoax material. Another persistent nuclear material scam includes the so-called "red mercury" scam. Nuclear scam artists identify "red mercury" as constituent or essential component of nuclear weapons.[31] "Red mercury" is a non-nuclear substance—typically mercury oxide, mercuric iodide, or mercury mixed with red dye—and has been found to be sold on black market for $100,000 to $300,000.[32] The ease of misrepresenting or exaggerating nuclear/radiological material on the black market is much more prevalent than instances in which nuclear/radiological material is actually sold or intercepted.[33]

Conclusion

As Walter Kemp of the United Nations Office of Drugs and Crime has observed:

> In the last 20 years, globalization has outpaced the growth of mechanisms for global governance. This has resulted in a lack of regulations—whether it be on the Internet, in banking systems, or free trade zones. The same conditions that have led to unprecedented openness in trade, travel, and communications have created massive opportunities for criminals. As a result, organized crime has diversified, gone global, and reached macro-economic proportions. This is having an impact on security.[34]

Although fine art and nuclear materials may appear to reside on opposite ends of the national security threat spectrum, unique typological characteristics can be developed to draw similarities between the trafficking of both commodities. The typological characteristics of supply, government instability, profit motive, terrorist demand, and hoaxes and scams are characteristics associated with both the illicit trafficking of nuclear material and fine art.

The typology suggests illicit trafficking

is a multi-layered phenomenon and can be captured in a rather simple rubric. Illicit smuggling activities such as drug smuggling, human trafficking, precious metal smuggling, arms smuggling, and other illicit trafficking can apply the same typological characteristics used to compare nuclear and art smuggling. Accordingly, this typology can serve as a starting point to help understand illicit trafficking of all kinds, to include nuclear/radiological material trafficking. As such, the entire interagency—charged, as it is, with the responsibility of protecting the nation against varied and multifaceted threats—can only benefit from recognizing the commonalities that exist among those threats. ***IAJ***

NOTES

1 These figures were determined by combining the total value of 50 contraband products and illegal activities with the total value of criminal markets in 91 countries. See "Havocscope Market Value," Havocscope Global Black Market Information, <http://www.havocscope.com/market-value/>, accessed on October 11, 2015.

2 Lyudmila Zaitseva, "Nuclear Trafficking: 20 Years in Review," Contribution to the World Federation of Scientists Meeting, August 2010.

3 "Illicit Trafficking of Nuclear and other Radioactive Material," Vertic.org, last modified April 2012, <http://www.vertic.org/media/assets/Publications/ITR_WEB.pdf>, accessed on April 12, 2017.

4 Zia Mian and Alexander Glasser, "Global Fissile Material Report 2015," International Panel on Fissile Material, Nuclear Non-Proliferation Treaty Review Conference, United Nations, New York, May 8, 2015, <http://fissilematerials.org/library/ipfm15.pdf>, accessed on November 13, 2015.

5 Lyudmila Zaitseva, and Friedrich Steinhäusler, "Nuclear Trafficking Issues in the Black Sea Region," EU Non-Proliferation Consortium, Non-Proliferation Papers, No. 39, April 2014, pp. 1–23, <http://www.nonproliferation.eu/web /documents /nonproliferationpapers/ lyudmilazaitsevafriedrichsteinhausler53451ed0bbecb.pdf>, accessed on October 17, 2015.

6 Andrew Kramer, "Arrests in Moldova Over Possible Uranium Smuggling," *The New York Times*, June 29, 2011, <http://www.nytimes.com/2011/06/30 /world/europe/30moldova.html?_r=0>, accessed on October 17, 2015.

7 Robert Wittman and John Shiffman, *Priceless, How I went Undercover to Rescue the World's Stolen Treasures*, Crown Publishers, New York, 2010, p. 20.

8 "ISIL and Antiques Trafficking," FBI, August 26, 2015, <https://www.fbi.gov /news/stories/2015/ august/isil-and-antiquities-trafficking>, accessed on April 12, 2017.

9 David Claridge and Bruce Hoffman, *Illicit Trafficking in Nuclear Materials*, Research Institute for the Study of Conflict and Terrorism, January-February 1999, p. 10.

10 Richard Spencer, "Dumped in the Desert…Gaddafi's Yellowcake Stockpile," The Telegraph, last modified September 25, 2011, http://www.telegraph.co.uk/news/worldnews /africaandindianocean/ libya/8784507/UN-agency-confirms-raw-uranium-in-Libya.html>, accessed on April 12, 2017.

11 Kris Hollington, "After Drugs and Guns, Art Theft Is the Biggest Criminal Enterprise in the World," *Newsweek*, July 22, 2014, <http://www.newsweek.com/2014/07/18/after-drugs-and-guns-art-theft-biggest-criminal-enterprise-world-260386.html>, accessed on October 16, 2015.

12 "8 Stolen Art Stories—The Biggest Heists in History," Finances Online, July 12, 2013, <http://financesonline.com/8-stolen-art-stories-the-biggest-heists-in-history/>, accessed on November 13, 2015.

13 Alex Mayyasi, "How Do You Make Money Off Stolen Art?" Priceonomics, November 21, 2013, <http://priceonomics.com/how-do-you-make-money-off-stolen-art/>, accessed on December 6, 2015.

14 Lyudmila Zaitseva and Kevin Hand, "Nuclear Smuggling Chains: Suppliers, Intermediaries, and End-Users," *American Behavioral Scientist*, Vol. 46, No. 6, 2003, pp. 822–844, <http://fsi.stanford.edu/sites/default/files/abs_zaitseva.pdf>, accessed on October 15, 2015.

15 Ibid.

16 Kimberly L. Alderman, "Honor Amongst Thieves: Organized Crime and the Illicit Antiquities Trade," *Indiana Law Review*, Vol. 45, No. 3, 2012, <https://mckinneylaw.iu .edu/ilr/pdf/vol45p601.pdf>, accessed on November 2, 2015.

17 Ibid.

18 Ana Swanson, "How the Islamic State Makes Its Money," *The Washington Post*, November 18, 2015, <https://www.washingtonpost.com/news/wonk/wp/2015/11/18/how-isis-makes-its-money/>, accessed on November 21, 2015.

19 "Unanimously Adopting Resolution 2199 (2015), Security Council Condemns Trade with Al-Qaida Associated Groups, Threatens Further Targeted Sanctions," Meetings Coverage and Press Releases, UN News Center, February 12, 2015, <http://www.un.org/press/en/2015/sc11775.doc.htm>, accessed on November 12, 2015.

20 *Combating Illicit Trafficking in Nuclear and Other Radioactive Material: Technical Guidance*, Reference Manual, International Atomic Energy Agency, Vienna, 2007, Nuclear Series, No. 6, 2007, <http://www-pub.iaea.org/MTCD/publications /PDF/pub1309_web.pdf>, accessed on September 16, 2015.

21 Sammy Salama and Edith Bursac, "Jihadist Capabilities and the Diffusion of Knowledge," in Gary Ackerman et al. (eds.), *Jihadist and Weapons of Mass Destruction*, CRC Press, Boca Raton, FL, 2009, p. 206.

22 Matthew Bunn and Anthony Wier, "The Seven Myths of Nuclear Terrorism," in Russell Howard et al. (eds.), *Weapons of Mass Destruction and Terrorism*, McGraw-Hill, New York, 2008, p. 126.

23 "Illicit Trafficking in Weapons-Useable Nuclear Material: Still More Questions Than Answers," Nuclear Threat Initiative. Center for Nonproliferation Studies, December 11, 2011, <http://www.nti.org/analysis/articles/illicit-trafficking-weapons-useable-nuclear-material-still-more-questions-answers/>, accessed on November 3, 2015.

24 Thomas Hoving, "The Game of Duplicity," "Art Forgery": The Metropolitan Museum of Art Bulletin, Vol. 26, No. 6, p. 243.

25 "Intent to Deceive: Fakes and Forgeries in the Art World," *On View Magazine*, June 4, 2014, <http://onviewmagazine.com/pg-80-intent-to-deceive-fakes-and-forgeries-in-the-art-world/>, accessed on November 2, 2015.

26 "Nuclear Security Summit Hears of Terror Risk," BBC News, April 13, 2010, <http://news.bbc.co.uk/2/hi/8616855.stm>, accessed on October 7, 2015.

27 "Nuclear Black Markets: Pakistan, A.Q. Khan and the Rise of Proliferation Networks," International Institute for Strategic Studies, London, 2007, p. 122.

28 United States Central Intelligence Agency, *Nuclear Smuggling Handbook: Case Studies and Detection Methods*.

29 Ibid.

30 I.D. Hutcheon, et al., *Handbook of Nuclear Chemistry*, Vol. 6, Nuclear Energy Production and Safety Issues, Nuclear Forensic Materials and Methods, Springer Science, New York, 2011, p. 2885.

31 *Combating Illicit Trafficking in Nuclear and Other Radioactive Material: Technical Guidance*.

32 Rensselaer Lee, *Smuggling Armageddon: The Nuclear Black Market in The Former Soviet Union and Europe,* St. Martin's Griffin, New York, 1999, p. 17.

33 *Combating Illicit Trafficking in Nuclear and Other Radioactive Material: Technical Guidance*.

34 Walter Kemp, "Organized Crime: A Growing Threat to Security," Stockholm International Peace Research Institute, <http://www.sipri.org/media /newsletter/essay/feb10>, accessed on April 12, 2017.

Optimizing the CWMD Enterprise Across the Interagency

by Michael J. Kwon

In recent decades, interagency cooperation has enabled the U.S. government in countering weapons of mass destruction (CWMD) organizations. This interagency cooperation, collectively referred to as the U.S. CWMD enterprise is an ongoing effort to protect the nation from the threat of WMD. Progress, such as it is, has not been easy; regulatory, budgetary, bureaucratic, and cultural obstacles abound. Nevertheless, so do opportunities for process improvement. As this extraordinarily complex enterprise continues to grapple with its equally complex problem set, particularly pertaining to issues of process standardization and conformance with the goal of optimizing interagency effectiveness, the enterprise would do well to avail itself of some valuable lessons from an unlikely, but highly effective interagency of another kind—the ecosystem of honeybees.

Five Lessons from Honeybees

Honeybees are responsible for cross-pollinating 80 percent of the world's fruits and vegetables and nearly half of all other food crops. In the U.S. alone, bees contribute $20 billion dollars to the economy. Bees are considered to be the highest form of insect life, showing sophisticated colonies and complex behaviors. The study of their enormous efficiency and effectiveness reveals some fundamental lessons, five of which are directly applicable to the U.S CWMD enterprise's quest for process improvement:

1) Unity of purpose.[1]

Honeybees have one overarching purpose—the survival of the hive. They make far more honey than they really need for survival, but the honey guarantees the survival of their colonies during the harshest winters, as well as several generations of bees. Similarly, if the CWMD enterprise

U.S. Air Force Major Michael J. Kwon serves as the Bioenvironmental Engineering Flight Commander at Osan Air Base in the Republic of Korea, where he provides medical counter Chemical, Biological, Radiological, and Nuclear defense expertise to the Air Force commanders and warfighers. He holds M.S. Degree in WMD Studies and is a Countering WMD Graduate Fellow at National Defense University.

acts with a single-minded purpose, its focus on national survival will enable it to overcome environmental obstacles. Accomplishing this means that the enterprise's individual organizational or leadership preferences must be subordinated to an overarching aim to which all interagency CWMD activities are directed.

2) Independent but complementary roles with clear lines of effort.[2]

During a honeybee's short lifespan, the worker bees learn and perform all the interlocking functions necessary for life in the hive. These functions are seamlessly connected. Every individual bee knows what it needs to do to maintain the health of the entire system. If the CWMD enterprise understands the importance of performing and completing individually-assigned processes and how each agency's efforts are related to and interdependent with other processes, the enterprise elements will continually streamline and realign their individual processes to facilitate aims outside the agency but complementary to the whole.

3) A flexible, dynamic system based on teamwork.[3]

Worker bees change from one task to another within seconds. They are highly skilled at teamwork. They communicate easily with one another. They have no personal agendas. They live to serve and support the hive. Indeed, the hexagonal structure of honeycomb demonstrates the connectedness of the entire work system. Each wall of the hexagon serves as a support wall for neighboring cells. The same principle is at work within the life of the colony. This system is not created not by one bee but by thousands upon thousands of bees. Yet, the honeycomb is perfect in design, function, and strength. It evidences standardization, teamwork, and communication throughout. The CWMD enterprise must be similarly integrated, achieving uniformity and connectivity wherever possible.

4) Highly effective communication and a strong sense of community and support.[4]

As honey bees forage for nectar, they can communicate with precision about the distance, direction, species, and quality of nectar. They communicate these details through a complex language that has been the object of long scientific study. As information is passed from bee to bee, the accuracy of this information is never doubted because meanings are clear and standard. If the CWMD enterprise fosters simple, clear, and direct communication with interagency partners in a way that lifts discourse above agency biases, both effective communication and mutual trust will become the general rule rather than the exception.

5) Identification and resolution of problems in real-time.[5]

When honey bees sense a problem, they pause work and immediately communicate to activate the hive's defense system. Bees focus on assessing and analyzing a situation with an eye toward a unified solution. In this recovery effort, every bee in the hive knows exactly what it needs to do for the survival of the hive. Bees precisely coordinate their response actions to defend and protect the hive, sacrificing as necessary to eliminate a threat. Bees leave nothing to chance for the survival of the hive. If the CWMD enterprise effectively communicates problems and works toward solutions with a sense of a shared responsibility through the interagency process, it will achieve solutions to complex problems more quickly than by any other method.

While it would be easy to dismiss these principles as nothing more than platitudes, they are, in fact, the very things the CWMD enterprise must move toward if it is to achieve its aims. As it seeks to do so, two issues demand priority attention: First, the U.S. government has no single, overarching interagency policy document, guidance, or instruction. In general,

...interagency coordination is often limited to temporary, ad hoc arrangements without mechanisms in place to enable agile response...

planning and executing CWMD activities take place under each departmental policy and planning documents.[6] One can only imagine what would happen to any hive that took this approach. Second, the bewildering array of the following national-level documents ostensibly aimed at providing guidance for CWMD issues leaves little doubt as to why unified effort is difficult: [7]

- 2015 National Security Strategy.
- 2012 Sustaining U.S. Global Leadership: Priorities for 21st Century Defense.
- 2012 National Strategy for Biosurveillance.
- 2012 National Strategy for Global Supply Chain Security.
- 2011 National Strategy for Counterterrorism.
- 2011 National Strategy for CBRNE Standards.
- 2010 Nuclear Posture Review Report.
- 2009 National Strategy for Countering Biological Threats.
- 2007 National Strategy for Homeland Security.
- 2006 National Strategy for Strategic Interdiction.
- 2002 National Strategy for Combat Weapons of Mass Destruction.
- Add to these the agencies, each with its many relevant components:[8]
  - National Security Council.
  - Department of Defense.
  - Office of the Director of National Intelligence.
  - Department of State.
  - Department of Homeland Security.
  - Department of Justice.
  - United States Agency for International Development.
  - Department of Treasury.
  - Department of Commerce.
  - Department of Health and Human Services.
  - Department of Transportation.
  - Department of Energy.

As a result, interagency coordination is often limited to temporary, *ad hoc* arrangements without mechanisms in place to enable agile response to increasingly rapid developments in the world of WMD threats. This modular approach can be effective to handle urgent and short-term tasks, but it will never be suitable for complex, long-term tasks.

Taking the Honeybees Seriously

While humans may never be as effective at formalizing processes as honey bees, some of the greatest scientific minds have produced systems that could at least serve as basic templates for improving CWMD enterprise processes in the interagency. The International Organization for Standardization (ISO) 9001, arguably by far the world's best established process standard and used by over 1.5 million organizations in 191 countries,[9] is a case in point. It suggests that, even if the CWMD enterprise cannot be bureaucratically organized

under one organization, agencies with CWMD responsibilities still can benefit greatly by having a shared subject-matter management system and lexicon. The ISO 9001 model contemplates integrative and interactive knowledge management that can capture, develop, share, and measure organizational knowledge and institutional memory for the best use of knowledge.[10] The fruits of the good-faith application of such a system are predictable: Policy and operational outputs that are standardized, easier to execute, less expensive and quicker to produce, are more reliable, and hence, more trusted by all involved.

ISO 9001 in Practice

Imagine the interagency governance structure based on ISO 9001 principles for the CWMD enterprise as shown in Figure 1 (pg. 48). Enterprise governance consists not of a new agency but of (1) an interagency CWMD council, (2) an interagency CWMD office, and (3) organizational CWMD councils. The interagency CWMD council establishes and improves the interagency CWMD strategy for the enterprise, "owns" interagency CWMD policies and decision-support processes (as opposed to the policies themselves), and approves interagency standards for the organization's work practices that are embodied in the interagency CWMD decision-support processes.

The interagency CWMD office analyzes and reports to the interagency CWMD council the status of the interagency CWMD decision-support process across the enterprise and also identifies needs and requirements for process improvements. In order for this office's work to be efficacious, its analyses must be clear, succinct, and amenable to easy implementation. The National Security Council (NSC), as the interagency "center for excellence," provides the interagency CWMD council with staffs and consultative support, oversees the interagency and organization decision-support processes for CWMD, and provides interagency CWMD decision support to the President and all other CWMD council and office members through interagency CWMD knowledge management.

Policy and operational outputs that are standardized, easier to execute, less expensive and quicker to produce, are more reliable, and hence, more trusted by all involved.

Interagency CWMD Knowledge Management Process

The interagency CWMD knowledge management process transfers CWMD knowledge as a part of the day-to-day interagency CWMD decision-support process across the CWMD enterprise within interagency CWMD governance. It is based, again appropriating the ISO 9001 model, on four elements: plan, do, check, and act (PDCA).

Plan. In the interagency CWMD decision-support process, planning starts with reviewing CWMD strategies, policy, interagency and resource requirements, product lines, operation relevance, and tasks. This information created within organizations is acquired from CWMD councils and offices or the intelligence community. Planning includes gap analyses and enables knowledge production by assessing references data from the planning element, as well as the other elements of the PDCA cycle. Learning gained through this analysis effort itself becomes knowledge and get incorporated along with other knowledge produced at this stage.

Do. While doing or executing, the interagency CWMD decision-support process generates experience and knowledge that is fed back to the planning element on a continual basis. This, of course, requires the deliberate sharing of all lessons learned and experience across the enterprise.

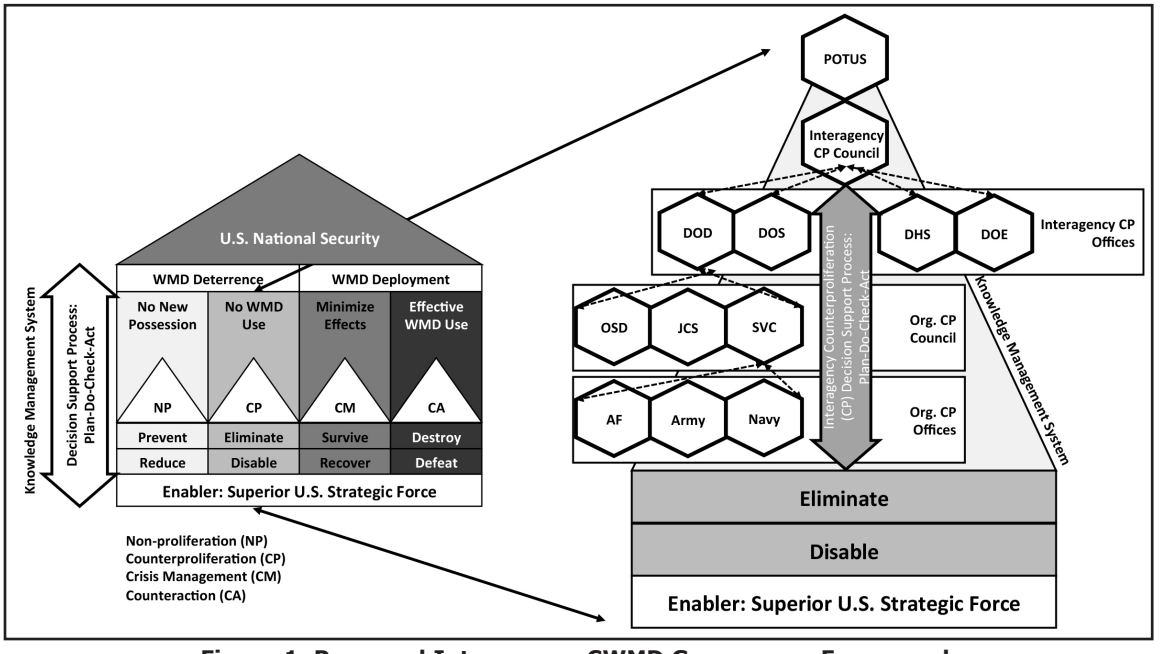


Figure 1. Proposed Interagency CWMD Governance Framework

Check. This element collects data sets through monitoring, measurement, assessment, investigations, and audits. Its focus is to identify non-conformance in interagency CWMD management system and processes. Findings are captured in management system review and communicated to relevant parties.

Act. This element ensures continuous improvement of processes and performance through top management involvement. Knowledge acquired in the preceding elements contains critical evaluations of the performance of the interagency CWMD management system and indicates actions for improvements. Because this element takes knowledge to the NSC and the President, this knowledge then gets incorporated into national security strategies for CWMD; the enterprise policies, objectives, resources; and other CWMD elements.

As shown in Figure 2 (pg. 49), the interagency CWMD knowledge management process continuously optimizes effectiveness of knowledge and its practices, improving interagency and organizational performance.

Benefits of the CWMD Knowledge Management

Interagency CWMD knowledge management based on the ISO 9001 model focuses on innovative and effective knowledge practices through systematic steps within interagency CWMD governance and the CWMD enterprise. It also emphasizes the free flow of knowledge across the enterprise.

Because of its ability to increase the effectiveness and the relationship of all resources and innovation in discernible ways, as CWMD knowledge cycles and evolves, interagency CWMD knowledge management increases the credibility and value of the interagency CWMD management system and the CWMD enterprise.[11] It establishes baselines for CWMD product lines, tasks, and interagency management system reviews. CWMD organizations and practitioners are freed to focus more on assessing WMD risks based on available knowledge and thus help the enterprise to develop better and timely CWMD strategies.

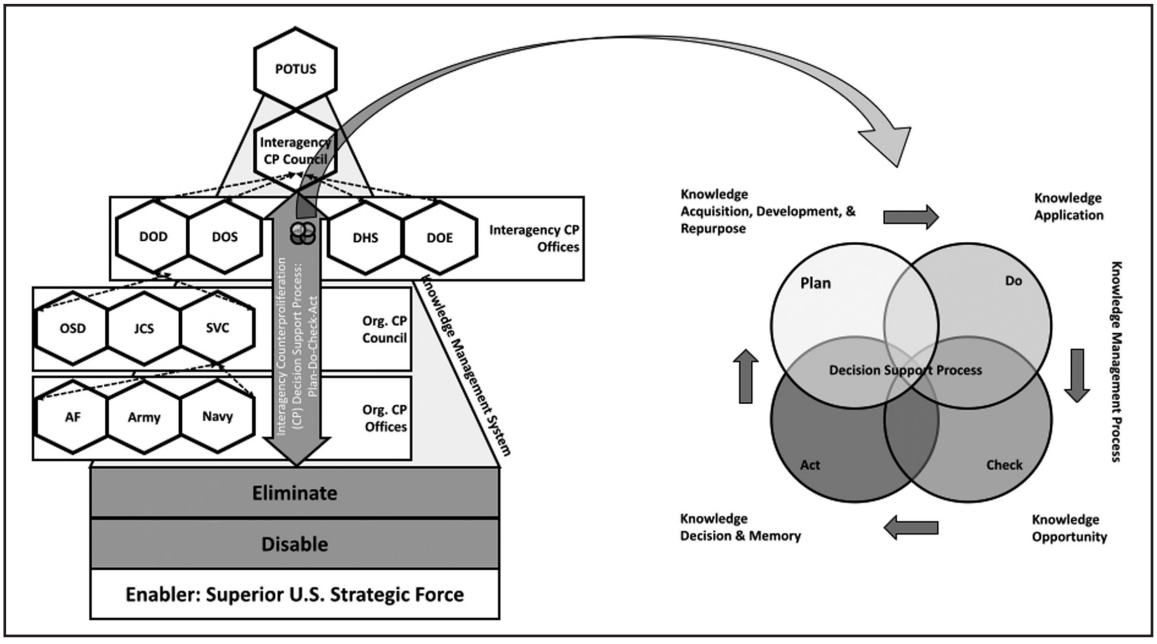


Figure 2. Interagency CWMD Knowledge Management Process

Potential Criticisms of the Proposed Interagency Management System

Nothing associated with the effort to standardize interagency activities is easy, and this reality serves as the basis for the most obvious likely criticism of the present proposal: However laudable the proposal may be, it is simply too hard to implement. Indeed, many scholars, government officials, and lawmakers have published and tried to make the interagency better, but most have failed.

Many Government Accountability Office (GAO) and government investigation reports have addressed and identified what needs to be done for interagency issues but fail to recommend who needs to do what to improve the interagency. At best, they may recommend with undefined, ill-defined, or non-existing processes for interagency improvement.

However, the ISO 9001 model is hardly an untried model. It has been used with success in such a wide variety of organizational settings that to dismiss it out of hand would be premature indeed. Even if many models from the commercial world do not translate well into the governmental sphere, the fact that the success of the ISO 9001 model does not appear to hinge on a profit motive commends it as a model worth trying.

One might also object that this proposal cannot succeed without steady and concerted leadership involvement. This is certainly true. It is true of any attempt to improve the management processes—particularly knowledge management—of any organization. The issue is precisely why an interagency CWMD management system is needed. At the very least, the system would provide a vehicle for meaningful leadership involvement in process and knowledge management. The "check" and "act" elements specifically enjoin leaders to provide appropriate oversight and to review policy, resources, strategy, and performance data in systematic ways, so that the eventual inclusion of knowledge in national-level policy documents occurs in non-idiosyncratic ways.

One might even object that processes for obtaining results of the kind sought by the ISO 9001 model are already in place in the CWMD

enterprise. If this is so, however, GAO and other evaluations of the performance of the CWMD enterprise do not lead easily to this conclusion.

While certain interagency management protocols exist with respect to CWMD, the decision support that these protocols lend to the effective management of WMD risks is, at very least, not well understood. Moreover, the perpetual formation and re-formation of *ad hoc* organizations can never produce the kind of continuity that enables genuine process problem resolution. Indeed, accomplishment of concrete mission objectives is more likely than not with the establishment of processes calculated to produce continuity across political administrations and ideological divides—two of the forces most likely to inhibit the effective function of the interagency.

...effective leaders in both government and industry value clear vision...and most importantly, trust.

In point of fact, ISO standards have already been adopted and incorporated in various U.S. government programs. Although government differs from industry in significant ways, effective leaders in both government and industry value clear vision, communication, empowerment of people, teamwork and team performance, flexibility, innovation, and most importantly, trust. The ISO is about standardizing these values through management system. ISO standards, it may be argued, would lead the proposed interagency CWMD management system to be effective and trusted, enabling those underlying values.

The proposed interagency CWMD management system is conceptual, and some might see this as too broad or difficult to understand. However, to be conceptual is not really a basis for criticism. The imperative which underwrites the success of any system is the education and training of its practitioners.

Professional practice is the means by which professionals acquire conceptual understanding over time, and indeed, understanding concepts that are not readily reducible to simple words or phrases is the fundamental trait of true professional expertise. Moreover, a serious focus on training and education relating to process and knowledge management may well be one of the best way to produce genuine organizational cultural and perspectival change where warranted. This, however, does not argue for a system that is unduly rigid or inflexible.

Even though the present proposal seeks long-term solutions rather than a parade of one-time fixes, the interagency CWMD decision-support process outlined here would still be able to provide time-sensitive solutions using process prioritization metrics under the "Do" element of the process. Moreover, because interagency CWMD knowledge management provides large data sets and new knowledge, CWMD practitioners could focus more on building solutions and options with other CWMD councils and offices and less on the perpetual *ad hoc* data collection efforts that are the hallmark of broken bureaucracies and ineffective leaders.

Conclusion

The U.S. CWMD enterprise is comprised of multiple executive departments, many subsidiary agencies, and thousands of people. If anything, it is becoming more complex—not less—as the nature of CWMD problems themselves increase in complexity. Even so, the five key lessons from honeybees remain foundational to the function of any organization, no matter how complex its tasks. As argued above, a CWMD enterprise process and knowledge management system modeled on ISO 9001 principles could go a long way toward operationalizing the lessons from the honeybees. Institutionalizing the interagency CWMD management system as described

could be expected to eliminate, or at least significantly reduce, CWMD enterprise gaps in national strategies, collaboration, and budgeting and funding. Perhaps the most important benefit of this proposal is that the interagency CWMD management system requires top management's periodic participation, decision, and action. Through the interagency CWMD governance framework, CWMD councils and offices would be established, calibrating process differences to CWMD process standards and reducing variations. This governance would shift competing processes to collaborating at the CWMD councils and offices levels. Through the PDCA cycle, the interagency CWMD decision-support process would continuously improve interagency effectiveness with respect to CWMD. Moreover, the system would integrate knowledge management into the PDCA cycle. Most importantly, interagency CWMD management system review would capture and record the CWMD leadership's evaluations and direction for the interagency CWMD way forward in national security strategy documents as courses of action, as well as institutional memory.

Of course, this proposed management system alone cannot altogether eliminate the fog of the interagency. Moreover, implementation and execution of complex systems, such as the one proposed in this article, has routinely proven disastrous in the absence of rigorous leadership commitment and participation, coupled with a reasonable tolerance for trial-and-error field testing. Nonetheless, interagency leadership requires optimism that surmounting this high bar is, in fact, possible. ***IAJ***

NOTES

1 Matthew Harrington and Deborah Mackin, *Survival of the Hive: 7 Leadership Lessons from a Beehive,* AuthorHouse, Bloomington, IN, 2013, p. 2.

2 Ibid., p. 24.

3 Ibid., p. 29.

4 Ibid., p. 51.

5 Ibid., p. 69.

6 H, Allen Irish, "A 'Peace Corps with Guns': Can the Military be a Tool of Development?" in Joseph R. Cerami and Jay W. Boggs (eds.), *The Interagency and Counterinsurgency Warfare: Aligning and Integrating Military and Civilian Roles in Stability, Security, Transition, and Reconstruction Operations*, U.S. Army War College Strategic Studies Institute, Carlisle Barracks, PA, pp. 53–95.

7 Counterproliferation Program Review Committee, "Report on Activities and for Countering Proliferation and NBC Terrorism," Vol. I, Executive Summary, Addendum to 2011 Report, 2013, p. 2.

8 Joint Publication 3-40, *Countering Weapons of Mass Destruction*, 2014, Ch. III, pp. 6–16.

9 Data from the ISO, <http://www.iso.org/iso/news.htm?refid=Ref1825>; ISO 9001:2015, *Quality Management Systems-Requirements,* <https://www.iso.org/obp/ui /#iso:std:iso:9001:ed-5:v1:en>, 2015, accessed on April 12. 2017.

10 Thomas H. Davenport, "Saving IT's Soul: Human Centered Information Management," *Harvard Business Review*, Vol. 72, No. 2, 1994, pp. 119–131.

11 Rene Tissen et al., *The Knowledge Dividend: Creating High-Performance Companies Through Value-Based Knowledge Management*, *Financial Times*, Prentice Hall, 2000, p. 47.

SAVE THE DATE!

Sept. 29, 2017 at 7 p.m.

A Celebration of International Friendship

Kauffman Center for the Performing Arts
1601 Broadway • Kansas City, Mo. 64108

Since 1895 international military officers from around the world have come to Fort Leavenworth to study military art and science at the U.S. Army's Command and General Staff College. Come help us celebrate and welcome the new class of officers in a black tie event at Kansas City's Kauffman Center for the Performing Arts.

The evening will begin at 7 p.m. with a reception followed by a program that will include the Introduction of the Command and General Staff College International Students, guest speaker remarks and a special performance by the U.S. Army Chorus.

Sponsorship opportunities are available. Ticket information will be published as we draw nearer to the event.

Hosted by *In Partnership With*

Greater Kansas City

Operation International

For more information contact the CGSC Foundation, Inc. – phone: 913-651-0624 email: office@cgscf.org

Concurrent Biological, Electromagnetic Pulse and Cyber-attacks: The Ultimate Interagency Response Challenge

by Patricia Rohrbeck

The Perfect Storm

The critical infrastructure components of an advanced society—telecommunications, transportation, banking and finance, petroleum and natural gas, food and water, public health and healthcare, and security—have at least one feature in common: All depend upon electrical and cyber power. Two well-known threats— electromagnetic pulse (EMP) and cyberattack—could, operating in tandem, disable not just a significant portion of the electrical grid and critical infrastructure, but also the network-centric military response to such an attack. If a high-altitude EMP attack were paired with both a large-scale cyberattack and a biological attack, the resulting challenge to the interagency could surpass anything the interagency is currently structured or equipped to respond to.

Current preparedness and response plans focus primarily on one weapons of mass destruction (WMD) attack mode at a time. However, an EMP and cyberattack would amplify the effects of a biological attack and vice-versa. The ramifications of such a combination of attacks are staggering:

- Detection of biological agents could be disabled after an EMP and cyberattack because electronic healthcare-surveillance systems would be no longer operational and could no longer process and exchange information among agencies.
- Laboratories would no longer receive or process suspected specimens to identify potentially hazardous biological agents. Without a timely response, the spread of disease in a population may not be contained during its early stages and could lead to outbreaks and epidemics. Without the ability to detect biological agents, public health officials cannot initiate timely treatment and preventive measures, which could result in higher than expected morbidity and mortality.

U.S. Air Force Lieutenant Colonel Patricia Rohrbeck serves at the 779th Medical Group, Joint Base Andrews, Maryland. She holds a Dr.P.H. degree in Public Health Practice and received a M.S. degree in WMD Studies as a National Defense University Countering WMD Graduate Fellow.

- With the breakdown of the entire transportation system in EMP-affected areas, sending laboratory specimens or distributing medical supplies may not be a priority as compared to food and water deliveries, which may disrupt how public health officials assess the ongoing health threat and how treatment is prioritized.

- Medical supplies and pharmaceuticals may not be delivered in the same dose and format requiring adjustments before administering. Thus, disruption of resource supply chains may cause a delay in patient treatment and care.

- The absence of telecommunication would severely disrupt interagency coordination efforts. For emergencies across state lines, support from federal agencies such as the Department of Homeland Security (DHS), Health and Human Services (HHS), and the Federal Emergency Management Agency (FEMA) is usually requested. Yet without the ability to communicate and travel, federal support may be delayed, leaving local agencies to lead the response. Local public health and healthcare personnel may lack the necessary training to coordinate a medical response to a biological agent. Thus, response efforts may be executed inefficiently.

These catastrophic attack combinations are not merely the stuff of science fiction. Adversaries of the U.S. certainly have the capability to execute EMP, cyber, and biological attacks. Some adversaries have the capability to execute them on a very large scale. In this latter case, the decision not to execute these large-scale attacks in tandem would be more reflective of the adversary's policy preference rather than the adversary's ability. Hence, failure to prepare against an attack combination cannot simply be dismissed as unthinkable. On the contrary, now is the time for the interagency to think about just such an eventuality.

One could argue that after EMP and cyberattacks, adversaries may not see the need for a biological attack because the lack of electricity, water, and food supplies alone will result in significant loss of lives. While that certainly is true, it is likewise the case that in order to recover from these attacks and to restore electricity and normal operation of systems, there need to be healthy people who can contribute to the recovery process. A biological attack in the wake of an EMP attack or cyberattack or both could render an effective response impossible and lead to societal collapse.

Understanding the Threat

The range of actors that might attempt EMP attacks against the U.S. is quite large and ranges from states with nuclear weapons, such as Russia and China, to rogue states with limited conventional and nuclear military capabilities, such as North Korea and terrorist groups that seek to inflict catastrophic damage on America.[1] Despite the reduction in the size of the Russian strategic nuclear force, Russia has optimized its strategic missile force to generate enhanced EMP effects.[2]

In a 2004 article, Russian Major General Vladimir Belous advocated an "asymmetric response" against deployed U.S. missile defense capabilities by detonating nuclear weapons prepositioned in orbit above the U.S.[3] China's interest in EMP goes back decades, and there is concern in Taiwan that China would use EMP weapons as part of a Chinese invasion of Taiwan.[4] An EMP attack would probably be very attractive to North Korea because its primitive economy would be less vulnerable to EMP than those of advanced industrial nations, while U.S. forces stationed on the Korean Peninsula would be extremely vulnerable.[5] Moreover the North Korean KN-08 missile, while inaccurate and possibly not able to reach a specific target in

the U.S., could be used to launch a high-altitude nuclear EMP attack.[6]

Even if a state was not disposed to launch a crippling EMP strike against the U.S. with no resulting fatalities, it may be willing to do so in combination with a biological attack.[7] Russia does not allow inspectors into all of its facilities capable of producing biological weapons.[8] The Department of State assesses that China, Iran, North Korea, Russia, and Syria continue to engage in dual-use activities with potential biological weapon applications.[9]

The most likely source of a bioterrorist attack is not governments, but radicalized groups or individuals, both within the U.S. or outside, that intend to utilize biological agents to cause mass casualties,[10] and it is not essential to assume that a combination EMP/cyber/biological attack must be perpetrated by the same actor. A state could execute an EMP or cyberattack or both, and a terrorist organization could seize the ensuing period of chaos to execute a biological attack. Terrorist organizations have expressed intent to use and show some capacity to develop biological weapons.[11]

Scientific expertise on acquiring biological resources and development of a biological weapon can be easily obtained through the internet. Additionally, small amounts of bacterial agents are sufficient to be cultured and grown into larger quantities in laboratories. Some agents, such as ricin, is readily available as a waste product of castor oil production, which is commonly used in the cosmetics industry.[12] Additionally, some laboratory leaders have paid insufficient attention to the details necessary to ensure laboratory biosafety and have inadvertently contributed to the biological threat.[13]

EMP, Cyber, and the State of Public Health Preparedness

Current issues with the public health response are multifaceted and start with a significant lack of understanding of the threat among public health professionals. Scientists and medical professionals are focused on their areas of expertise and may not appreciate the nature of the WMD threat. Many public health professionals may not even know what an EMP attack is and how it can impact infrastructure relevant to their work. Moreover, most response plans are written for one WMD and do not consider concurrent events to inflict mass casualties. Current education and training programs on EMP for emergency responders is limited and not readily available to the entire public health community response.

The most likely source of a bioterrorist attack is not governments, but radicalized groups or individuals...

One of the most challenging issues for public health in the present context is the ever-increasing reliance of public health on electronic and cyber technology. Incident communication networks, disease surveillance databases, and resource distribution tools have made a dramatic and positive difference in the overall preparation for and response to 9/11-like events and subsequent incidents.[14] Software automation tools are available to support the planning, coordination, and response of local governments and private sector organizations to potential emergencies and biological threats.[15] Management technologies may include functionality for event prediction, contingency planning, consequence coordination and response, post-event audit and documentation, recovery and remediation initiatives, as well as simulation and drill development.[16] During 2013, the Centers for Disease Control and Prevention (CDC) conducted two emergency notification drills with organizations that had received CDC funds for preparedness and response

capabilities.[17] The goal was to test whether CDC's Emergency Operation Center (EOC) laboratory staff and epidemiologists could contact each other regarding potential threats and disease outbreaks in a timely manner.[18] The target response time was 45 minutes for each drill, with 84 percent of participants meeting the target in the first drill and 94 percent meeting the target in the subsequent drill.[19]

Underneath these marvelous capabilities, however, lies a significant vulnerability. The problem is not the community's reliance on these communication and surveillance systems *per se*. The problem is that many of these systems are highly vulnerable to cyberattack; practically none of them are hardened against EMP-attack, and little has been done to train the public health community to function if these systems were suddenly to become non-operational. Local, state, and federal emergency management plans generally do not include back-up plans in case these electronic systems fail during an EMP and cyberattack. As a result, there is a false sense of security among public health agencies and responders that they are sufficiently prepared to respond to any threat.

...there is a false sense of security among public health agencies and responders that they are sufficiently prepared...

In 2013, the Secure High-voltage Infrastructure for Electricity from Lethal Damage Act (SHIELD Act; H.R. 2417) was introduced to Congress. The SHIELD Act assumes that the U.S. is currently ill-prepared to recovery after an EMP event and that the loss of electrical power systems will have catastrophic consequences to include potential casualties for more than 60 percent of the population. As a result, the SHIELD Act would authorize the Federal Energy Regulatory Commission (FERC) to propose standards and processes for industry and government alike to address vulnerabilities of the electric grid.[20] Congress has not passed the SHIELD Act, because it would require industry to harden and protect its electric infrastructure at a high cost. In addition, the Critical Infrastructure Protection Act (CIPA) was also introduced in 2013, which authorizes DHS to include EMP events in national planning scenarios and conduct outreach to educate owners and operators of critical infrastructure and emergency planners and responders on the threats by EMP events.[21] The CIPA Act passed the House in December 2014. Whereas some bills and plans have been established, little effort has been made so far to physically protect the electrical grid.

Education and Training

Education and training are crucial in ensuring that healthcare professionals can adequately recognize and respond to a biological attack as well as help maintain professional skills and expertise. The CDC's Office of Public Health Preparedness and Response (PHPR) conducts training and exercises to prepare state and local health departments to respond effectively during an emergency when Strategic National Stockpile assets are deployed, to ensure that vaccines and medications are received in a timely manner if local supplies have run out.[22] Yet, none of the exercises include scenarios in which the transportation and communication systems have failed. In 2014, the Assistant Secretary for Preparedness and the CDC together awarded more than $840 million in emergency preparedness and response fund to improve existing response measures.[23] Whereas the close alignment of the funding support improved efficiency in grant administration, no funding was allotted to evaluate the supported programs. It is therefore uncertain if funding has improved levels of preparedness within organizations and whether gaps in health security preparedness,

such as EMP, have been identified and addressed.

Another problem is that emergency preparedness training is often limited to federal, state, and local agencies and first responders and not routinely to primary care providers.[24] Affected individuals may not necessarily seek care in the emergency room, but rather consult with their primary care provider or their staff or support staff, so providing training to even the nonmedical personnel in a physician's office could aid in early detection.[25] Medical schools offer various courses on national disaster and emergencies, hazardous materials, and federal emergency response, but there is no recognized standard for training providers, and these courses are not widely utilized.[26]

Beyond training, practitioners still must seek opportunities to become familiar with local emergency medical series as well as local chain of command and their contact information.[27] In light of competing priorities for training and education, the amount of time a practitioner might actually devote to the difficult task of functioning successfully without electricity is questionable at best.

Many public and private organizations lack the comprehensive, emergency-response plan that defines the roles and responsibilities of trained personnel responding to an unexpected incident.[28] Additionally, most plans do not extensively describe how to work side-by-side with responders from other agencies.[29] Many organizations do not know where to turn for assistance regarding emergency preparedness, nor do they have the time to stop the daily task of operating a business or service.[30] If training is mandated, agencies participating in an emergency response are often not coordinated in their efforts.[31]

During the 2003 power outage in the Midwest and Northeast U.S., public health and emergency responders noted that there was a lack of preparations and resources for coping with public anxiety and behavioral issues, lack of training in dealing with power outage emergencies, and lack of planning for multiple-system failures across states when relying on aid from nearby communities.[32] In addition, the assumption is that healthcare staff trained in emergency response and disease surveillance will be in the right place at the right time to respond to a biological event after an EMP. Yet, with the collapse of the transportation infrastructure, trained staff may not be able to reach their hospital or public health facility in a timely manner or at all. Under normal circumstances, it may make sense to only train a selected few individuals as emergency essential personnel who can then direct the remaining staff, but after an EMP, this concept will not work; all will need to act under emergency conditions.

However, even if the entire public health community and all other public servants were adequately trained, a major public education effort would be required to condition American society—unaccustomed as it is to major, long-term inconveniences, to deal with privations that would render their circumstances more closely akin to those of the seventeenth century than of the twenty-first century.

Many public and private organizations lack the comprehensive, emergency-response plan that defines the roles and responsibilities of trained personnel...

Protecting and Recovering Critical Infrastructure

Incidents of biological threats, such as the so-called "Amerithrax" attack of 2001, have been well documented. Since that time, disease surveillance tools and rapid testing capabilities have been deployed and have, it may be argued, protected against attacks that

otherwise could have been more effective than they were or caused more panic than they did. What is underappreciated, however, is the total reliance of these technologies on electric and cyber power, as well as the fact that they are not hardened against EMP.

State and local governments have made sparse efforts to incorporate EMP preparedness and response measures into their response plans.

State and local governments have made sparse efforts to incorporate EMP preparedness and response measures into their response plans. Alaska and some New York municipal organizations include EMP preparedness measures in their response plans.[33] Whereas most of these plans address survivability measures, they do not include actual hardening of electricity-based infrastructure. The variability in how local and state governments address their needs for protective measures against an EMP attack is often due to lack of knowledge on the impact of an EMP on the electrical grid.

The DoD, on the other hand, has continuously prepared for an EMP over the past decade and continues to invest in hardening its military infrastructure. In 2012, the DoD spent $22.1 million to harden Minuteman missiles against EMP attacks.[34] The North American Aerospace Defense Command (NORAD) commander recently announced that NORAD headquarters, which provides early warning and command and control for the defense of the continental U.S. against nuclear attack, has been moved from Peterson Air Force Base in Colorado back into Cheyenne Mountain because going underground ensured protection against EMP.[35] In addition, the Pentagon awarded a $700 million contract to upgrade its electronics through 2020.[36] With that being said, most computers and electronic equipment in DoD is still vulnerable, such that an EMP attack could still severely degrade the ability of the armed forces to operate effectively.

If an EMP attack would occur, near-term recovery would prove impossible because of, (1) the nation's almost total dependence on the electrical grid[37] and (2) the interdependence of the critical infrastructures powered by the grid.[38] Restarting the grid, also known as a "black start," requires communication and energy transport, which both require electricity—causing an intractable "chicken or the egg" problem. Transformers and generators are not readily available for purchase and repairs may take months.[39] Thus, modernizing and hardening the electrical grid is as much a public health imperative as it is a defense or economic imperative.

Current grid protection measures require state legislator involvement since they have regulatory authority over the systems, so states can require power companies to install blocking devices and other technologies to protect against EMP or geomagnetic disturbances.[40] According to the National Governors Association, 70 percent of transmission lines and transformers are at least 25 years old, 60 percent of circuit breakers are at least 30 years old, and much of the infrastructure was designed in the 1950s making the entire grid vulnerable to EMP.[41] One of the major issues that limits grid modernization is that the current spending of $34 billion per year to maintain and partially upgrade the grid will have to be increased by $8 to $16 billion per year through 2030 to ensure a fully modernized grid.[42] A modern grid would address cyber security and EMP, as well as increased consumer demand, so governors have an important role in moving this agenda forward and making it a funding priority. Engineering approaches such as shielded enclosures, grounding techniques, current-limiting line filters, terminal-protection devices, and cable management are costly if added to an existing grid but relatively cost-

effective if integrated into the design phase of a new grid, but in either case, they are essential to the nation's security in a dangerous and uncertain world.

Conclusion

Perfect storm scenarios like the catastrophic convergence described herein are indeed the stuff of thriller novels and movies and, as a result, may seem simply too awful to be possible. However, it is precisely this "unthinkable" quality that demands the attention of thoughtful persons, intent upon securing the nation from those scenarios, which, even if unlikely, could prove the nation's undoing.

Operational planners have long noticed the vulnerabilities posed by bureaucratic gaps and seams. However, this convergence is not a problem of "gaps" and "seams." Rather, it is a problem of total systemic failure. EMP is real. Cyberattacks are real. Biological attacks are real. Adversaries of the U.S. who possess one or more of these capabilities are real. When the problem is considered in that light, it assumes a much more plausible form than it might when viewed on the Hollywood screen. Now is the time for the interagency to devote reasonable attention to the problem. ***IAJ***

NOTES

1 Jenna Baker McNeill and Richard Weitz, "Electromagnetic Pulse (EMP) Attack: A Preventable Homeland Security Catastrophe," The Heritage Center, October 20, 2008, <http://www.heritage.org/research/reports/2008/10/electromagnetic-pulse-emp-attack-a-preventable-homeland-security-catastrophe>, accessed on December 6, 2015.

2 Mark Schneider, "The Emerging EMP Threat to the United States," U.S. Nuclear Strategy Forum paper, National Institute Press, Fairfax, VA, November 2007, p. 3, <http://www.nipp.org/wp-content/uploads/2014/12/EMP-Paper-Final-November07.pdf>, accessed on December 6, 2015.

3 Ibid., p. 4.

4 Ibid., pp. 5–6.

5 Ibid., p. 10.

6 Ibid.

7 Clay Wilson, "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessment," Congressional Research Service Report to Congress, July 2008, p. 20, <https://www.fas.org/sgp/crs/natsec/RL32544.pdf>, accessed on November 3, 2015.

8 Ibid.

9 U.S. Department of State, "Adherence to and Compliance with Arms Control, Nonproliferation, Disarmament Agreements and Commitments," Bureau of Arms Control, Verification, and Compliance Report, <http://www.state.gov/t/avc/rls/rpt/2015/243224.htm>, accessed on June 5, 2015.

10 Oliver Grundmann, "The Current State of Bioterrorist Attack Surveillance and Preparedness in the U.S.," *Risk Management and Healthcare Policy*, October 2014, Vol. 7, pp. 177–187, <http://dx.doi.org/10.2147/RMHP.S56047>, accessed on December 15, 2015.

11 Hudson Institute, "A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts," Bipartisan Report of the Blue Ribbon Study Panel on Biodefense, October 2015, p. 4, <http://hudson.org/research/11824-a-national-blueprint-for-biodefense-leadership-and-major-reform-needed-to-optimize-efforts>, accessed on November 1, 2015.

12 Grundmann, p. 182.

13 Hudson Institute, p. 5.

14 Shawn D. Smith, "Inter-Agency Collaboration and Consequence Management: An All-Hazard Approach to Emergency Incident Response," EHS Today, May 16, 2006, <http://ehstoday.com/fire_emergencyresponse/ehs_imp_17938>, accessed on December 6, 2015.

15 Ibid.

16 Ibid.

17 Centers for Disease Control and Prevention, "National Snapshot of Public Health Preparedness," 2015, p. 11, <http://www.phe.gov/Preparedness/mcm/phemce /Pages/default.aspx>, accessed on February 7, 2016.

18 Ibid.

19 Ibid.

20 "H.R.2417, Secure High-voltage Infrastructure for Electricity from Lethal Damage Act," 113th Congress, June 18, 2013, <https://www.congress.gov/bill/113th-congress/house-bill/2417>, accessed on December 6, 2015.

21 "H.R.3410, Critical Infrastructure Protection Act," 113th Congress, October 30, 2013, <https://www.congress.gov/bill/113th-congress/house-bill/3410>, accessed on December 6, 2015.

22 Centers for Disease Control and Prevention.

23 Ibid., p. 27.

24 Gail Dudley and Robin B, McFee, "Preparedness for Biological Terrorism in the United States: Project BioShield and Beyond," *The Journal of the American Osteopathic Association,* 2005, Vol. 105, No. 9, p. 421.

25 Ibid.

26 Ibid.

27 Ibid., p. 422.

28 Smith.

29 Ibid.

30 Ibid.

31 Ibid.

32 James C. Kile et al., "Impact of 2003 Power Outages on Public Health and Emergency Response," *Prehospital and Disaster Medicine*, Vol. 20, No. 2, 2005, p. 96.

33 Baker Spring et al., "Before the Lights Go Out: A Survey of EMP Preparedness Reveals Significant Shortfalls," August 15, 2011, <http://www.heritage.org/research/reports /2011/08/before-the-lights-go-out-a-survey-of-emp-preparedness-reveals-significant-shortfalls>, accessed on December 6, 2015.

34 Ibid.

35 Henry F. Cooper and Peter Vincent Pry, "The Threat to Melt the Electric Grid," *The Wall Street*

Journal, April 30, 2015, <http://www.wsj.com/articles/the-threat-to-melt-the-electric-grid-1430436815>, accessed on December 6, 2015.

36 Ibid.

37 McNeill and Weitz.

38 Electric Power Research Institute, "Enhancing Distribution Resiliency: Opportunities for Applying Innovative Technologies," January 2013, p. 3, <http://www.epri.com/abstracts/Pages /ProductAbstract.aspx ?ProductId=000000000001026889&Mode=download>, accessed on December 6, 2015.

39 J. S. Foster et al., "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures," April 2008, p. 50, <http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf>, accessed on December 6, 2015.

40 Jenna Bergal, "States Work to Protect Electric Grid," February 27, 2015, <http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2015/2/27/states-work-to-protect-electric-grid>, accessed on January 15, 2016.

41 National Governors Association, "Governors' Guide to Modernizing the Electric Power Grid," March 2014, p.1, <http://www.nga.org/files/live/sites/NGA/files/pdf /2014/1403GovernorsGuideModernizingElectricPowerGrid.pdf>, accessed on January 15, 2016.

42 Ibid., p. 2.

Kinetic Energy Weapons
The Beginning of an Interagency Challenge

by Daniel C. Sproull

In 1948, the UN Commission for Conventional Armaments defined weapons of mass destruction (WMD) as "…atomic explosive weapons, radioactive material weapons, lethal chemical and biological weapons, and any weapons developed in the future which have characteristics comparable in destructive effect to those of the atomic bomb or other weapons mentioned above."[1] This widely-embraced definition of WMD acknowledges the possibility of unforeseen and, indeed, unforeseeable technological advances that could lead to the development of weapon types which, for all practical purposes, constitute WMD. One such possible weapon type—the result of rapid advances in hypersonic technology—is the so-called "kinetic energy weapon" (KEW).

KEW: An Overview

A KEW travels at hypersonic velocities and converts part or all of its mass into energy on impact. The kinetic effect of objects impacting at hypersonic speeds is easy to demonstrate in nature. Hundreds of craters, the result of impacting asteroids—some small, others extraordinarily large—can be found all over the earth.[2] The U.S. has contemplated artificially creating this phenomenon ever since the RAND Corporation first proposed placing tungsten rods on intercontinental ballistic missiles (ICBMs) in the 1950s.[3] In 2002, the RAND Corporation issued a report detailing what a possible rod-based KEW weapon system would look like.[4] In 2003, the U.S. Air Force detailed the development of hypervelocity rod bundles as a future weapon system goal. The concept contemplates that a KEW would enable the U.S. to strike ground systems anywhere in the world from space, as well as work to mitigate any anti-access environment that would restrict the operation of conventional forces.[5] The propulsion science for this type of weapon is currently under development by multiple countries, with the only limitation being sufficiently advanced materials science to withstand the enormous heat

Mr. Daniel C. Sproull is an Advanced Concept Weapons analyst for the U.S. Air Force, where he evaluates impact of developing and conceptual weapon systems at the campaign level. He received a M.S. Degree in WMD Studies as a National Defense University Countering WMD Graduate Fellow.

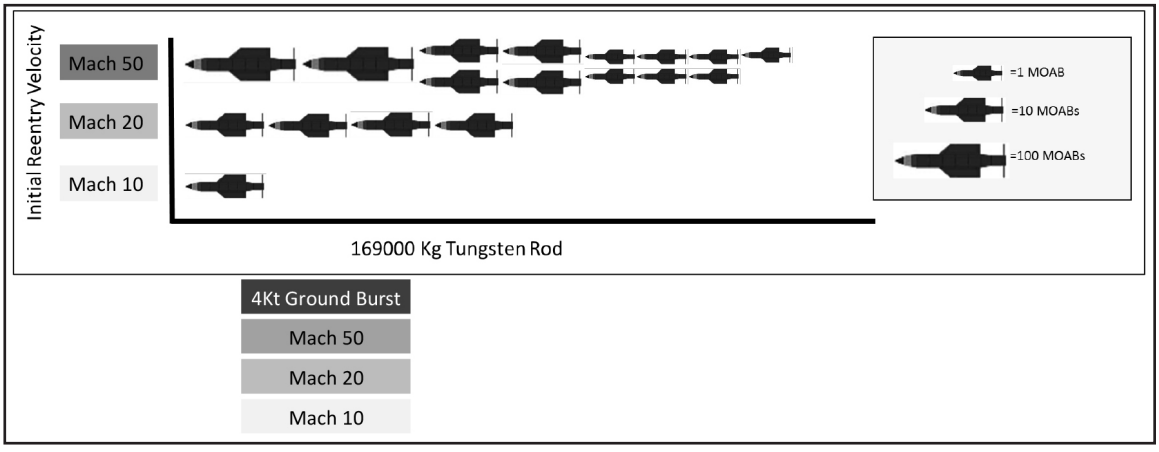


Figure 1. Tungsten Rod KEW vs. MOAB

and stress generated at hypersonic speeds. Once the materials science allows reliable hypersonic speeds to be attained, there is little to stop the development of a viable, large-scale, weapon system.

The U.S. is not waiting for hypersonic engines to become viable before developing a hypersonic weapon. The U.S. Navy railgun project is a low-yield, tactical application of hypersonic technology. The railgun uses electromagnetic force to accelerate an inert steel projectile to hypersonic speeds, currently Mach 7, with a current range of 100 miles. Energy released upon impact is equivalent to 15.5 lbs. of TNT. While 15.5 lbs. of TNT does not equate to a WMD, an immediate kinetic effect of this magnitude clearly suggests the potential for a KEW of WMD proportions.

The Defense Advanced Research Projects Agency's (DARPA) hypersonic vehicle platform has similar potential. While tests conducted to date have only been able to achieve speeds around Mach 10, present goals call for a minimum speed of Mach 20.[6] If DARPA's vehicle was loaded with its maximum payload of 5500 kg and impacted on target at Mach 20, the energy released would approximate 31 tons of TNT.[7]

While this is still miniscule compared to the energy release of a nuclear weapon, it clearly shows the lethal potential inherent in a KEW. This is a yield which certainly exceeds the kinetic yields typically associated with conventional weapons. So, even if currently contemplated KEW does not produce effects of nuclear-weapon proportion, its effects still would far exceed present conventional capabilities.

KEW as WMD

WMD, as a class, have historically been understood to possess some extraordinary combination of four characteristics: high order of destruction, wide area of effect, lingering effect, and indiscriminate effect. Although not all WMD possess all of these characteristics in extraordinary degree, the case can be made that a KEW possesses all four:

High order of destruction

Figure 1 shows the comparison between a single, tungsten, rod-based KEW and the GBU-43/B Massive Ordnance Air Blast (MOAB), the largest precision-guided conventional munition in the U.S. Air Force inventory, with a blast radius of approximately 150 meters.[8] Given a tungsten-rod KEW with a mass of 169,000 kg, 90 percent the lift capacity of an Ares V rocket, note how the impact of one such rod compares with that of the MOAB at reentry velocities of Mach 10, 20, and 50, respectively.[9]

A single rod accelerated to Mach 10 releases the energy equivalent to 10 MOABs (300,000

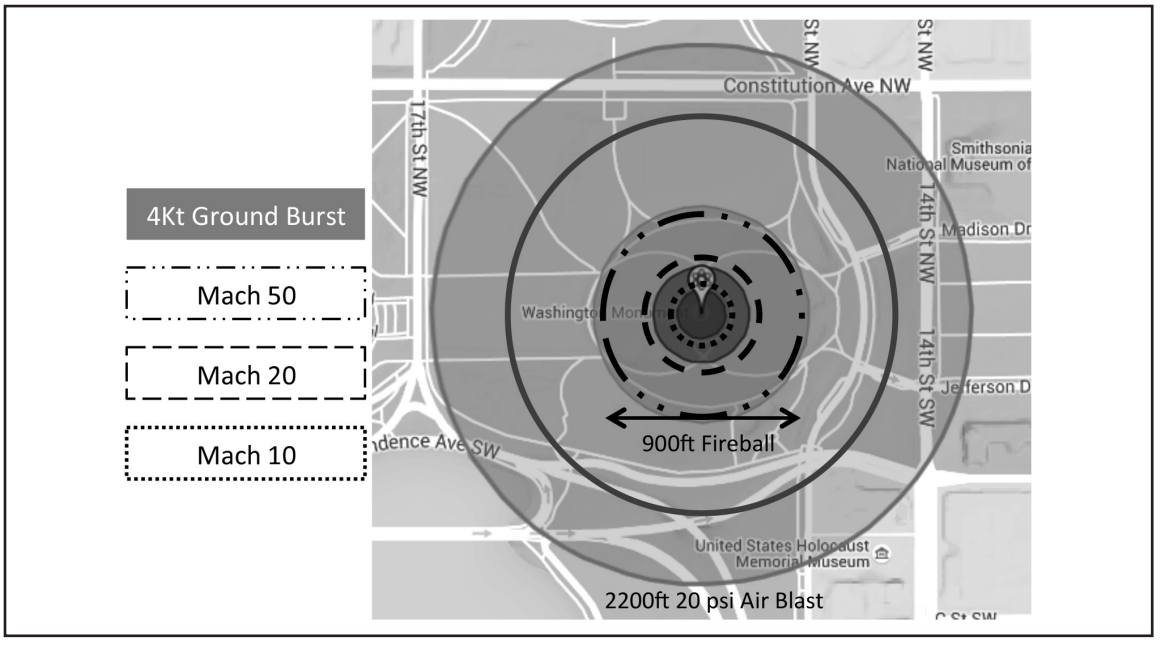


Figure 2. Comparison of Ground-Burst Effects

pounds of TNT) detonating at a single point. At Mach 50, the energy release is equivalent to 247 MOABs or approximately 4 kiloton (kT) of TNT at a single point. As the tungsten rod impacts, a significant portion of the rod vaporizes, leaving tungsten vapor or particulate to spontaneously combust at over 6,000 degrees Fahrenheit.[10] If this combustion occurs in an enclosed space, like a bunker, the resulting fireball would only add to the devastation caused by the impact.[11]

Wide area of effect

Figure 2 centers on the Washington Monument for scale and compares the immediate effects of a ground-burst 4 kT nuclear detonation (Circle 1) with those of a KEW, impacting at Mach 50 (Circle 3), Mach 20 (Circle 4), and Mach 10 (Circle 5).[12]

The Mach 10 and 20 rings either match or exceed the nuclear weapon crater. The Mach 50 ring almost meets the 4 kT nuclear fireball ring. However, a fireball is not the only nuclear weapon-like effect that the KEW illustrated above would produce. It would also produce lethal dynamic overpressure—20 pounds-per-square-inch (psi) in the case of a KEW delivered at Mach 50. Circles 1 and 2 are the 20 psi air blast ranges for the 4 kT nuclear detonation and the Mach 50 KEW impact respectively.13 At these distances, total destruction occurs simply from the air blast. Nearly equaling the Circle 1 is the 5-psi air blast range for the Mach 50 KEW. This also causes extensive damage to people as well as buildings. To place this degree of overpressure in perspective, Figure 3 summarizes the effect of dynamic overpressure on both buildings and on the human body.[13]

In terms of raw destructive capability, the Chelyabinsk meteor explosion over Russia in 2013 gives a real-world example of the possible wide area of effect of a KEW. Weighing in at over 12,000 metric tons and entering the atmosphere at around Mach 50, the meteor exploded 20–30 miles above ground. This event caused minor structural damage across six cities, with over a thousand injuries being reported. The explosion was estimated around 450 kT.[15] Had the meteor held together until impacting the ground, the area of effect would have been much smaller, but the damage done would have been significantly greater.

Peak Overpressure	Maximum Wind speed	Effect on Structures	Effect on the human body
1 psi	38 mph	Window glass shatters	Light injuries from fragments occur
2 psi	70 mph	Moderate damage to houses (windows and doors blown out and severe damage to roofs)	People injured by flying glass and debris
3 psi	102 mph	Residential structures collapse	Serious injuries are common, fatalities may occur
5 psi	163 mph	Most building collapse	Injuries are universal, fatalities are widespread
10 psi	294 mph	Reinforced concrete buildings are severely damaged or demolished	Most people are killed
20 psi	502 mph	Heavily built concrete buildings are severely damaged or demolished	Fatalities approach 100 percent

Figure 3. Effects of Dynamic Overpressure

Indiscriminate and Lingering Effect

Like WMD, KEWs possess the capacity to produce both indiscriminate and lingering effects. However, because of their cratering capability, KEWs could locally magnify these effects on subterranean infrastructure to a degree that exceeds that of WMD. Figure 4 compares the differences in cratering between the 20 kT "Fat Man" nuclear detonation over Nagasaki and Mach 10, 20 and 50 KEW impacts.

Even "Fat Man" caused unexpected subterranean damage over a wide area: the overpressure wave caused by the atomic detonation caused extensive damage to the city's subterranean public utilities, especially water mains, down to about 10 feet. In contrast, a Mach 10 KEW has the capability of cratering down to almost 100 feet. The Mach 50 depth is over 150 feet with a crater almost 800 feet wide. If a KEW attack were to take place near a large body of water, crater flooding would be catastrophic both in terms of lives lost and the time required to restore infrastructure. This effect is magnified if such flooding breached a subway system. Most modern, subterranean rail systems are not equipped to contain massive flooding. The magnitude of the problem becomes evident with today's society. Modern cities place much

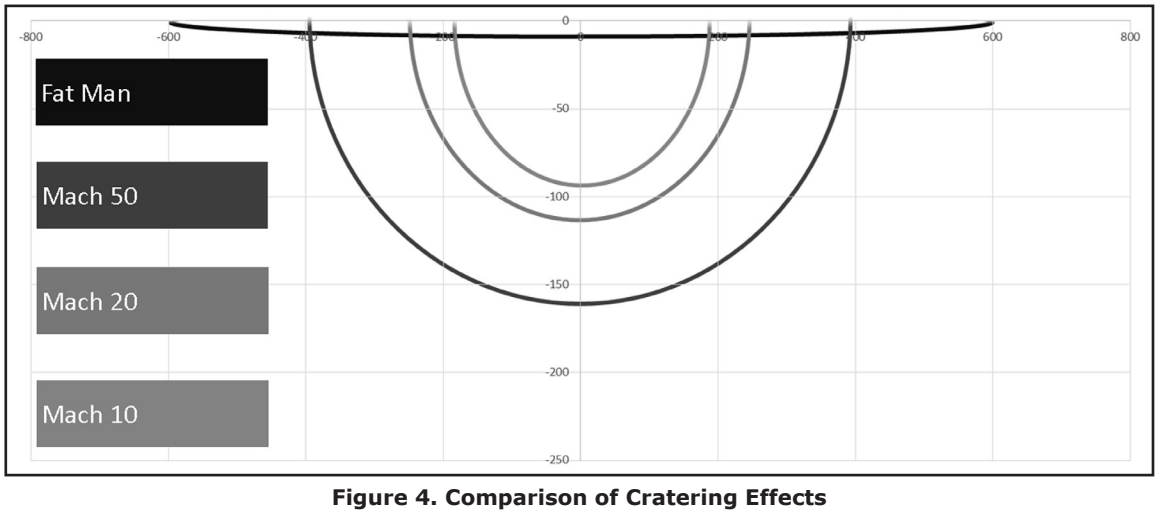


Figure 4. Comparison of Cratering Effects

of their infrastructure underground due to space and security constraints. At depths of less than 30 feet, cities typically have a labyrinth of power, water, steam and gas lines, and in some cities, a maze of subway tunnels and other structures beneath the utility lines. A KEW could easily cause catastrophic damage to this underground infrastructure.

Opportunities and Challenges for the Interagency

Hypersonic research promises a vast array of peaceful, commercial applications, such as hypersonic transportation systems. Moreover, peaceful applications of KEW-like devices for major public works projects, such as large earth-moving projects for cutting canals or creating mountain passes, can be imagined. In previous decades, this discussion was undertaken in earnest with respect to the peaceful use of nuclear weapons. KEW-like devices could conceivably accomplish the same peaceful tasks suggested for nuclear weapons use but without the inherent radiological hazards.

On the diplomatic front, a coordinated international effort will be necessary to achieve uniform understanding about the licit and illicit use of hypersonic technologies. That effort might, in fact, require the establishment of regulatory mechanisms similar to the Nuclear Nonproliferation Treaty (NPT) or the Chemical Weapons Convention (CWC). As the number of nations working to develop hypersonic flight capabilities or KEW expands, the need for such coordination will expand as well. Since the number of countries now focused on these kinds of advanced research efforts is small at present, now is the time to begin regulatory efforts. The NPT states that countries that voluntarily give up construction of KEWs could receive assistance with civilian applications enabled by new materials science. This has worked fairly well for the NPT, with many countries receiving access to technology they did not have to develop on their own.

Even so, both nuclear weapons and KEWs are, first and foremost, weapons, and the interagency must proceed with this reality foremost in mind. Looking at the history of kinetic impacts from meteors—from the older Morokweng and Sudbury impacts to the more recent Tunguska and Chelyabinsk—the unavoidable question becomes how might the U.S. be affected if an adversary were able to create similar effects with a KEW? Now is the time to begin a serious interagency exploration of the implications of hypersonic technology, particularly as that technology relates to KEW. The Department of Defense will be faced with some obvious operational questions such as: What yields will be acceptable for use on the conventional battlefield? What targets would be both viable and valid for attack using KEW? How will the U.S. detect orbital KEW systems? Can such a system be interdicted?

Diplomatic resources will be required to establish international understanding on the weaponized use of hypersonic technologies as well. The subclass of KEWs that can be used on the conventional battlefield must also be defined. Using either the BLU-82 "daisy cutter" or the GBU-43 MOAB would be an appropriate first start to establishing an acceptable conventional yield limit. Both these weapons rely on significant quantities of conventional explosive, 12,000 lbs. for the BLU-82 and 18,000 lbs. for the MOAB. However, the damage from these weapons is confined to a limited area. The BLU-82 has a maximum blast radius of approximately 900 ft., while the MOAB radius is slightly larger due to is greater explosive weight. These are the largest conventional weapons in the U.S. inventory, and both are used sparingly if at all.[16]

They must also decide on a minimum and maximum strategic yield of a KEW. For a time, the upper bound of a KEW yield will be limited by the lift capability of current rocket technology, as well as limitations in materials

science, yet these restrictions may not remain in effect forever. Fixing an upper bound on the size of an orbital KEW should be a necessity.

Additionally, countries must also decide how and on what targets KEWs can be used in conventional warfare. Current rules of engagement will suffice for most targets. However, greater care is needed when using a KEW around facilities that have the capability of causing secondary effects. For instance, dropping a 500-lb. bomb several hundred feet away from a nuclear facility might constitute a minimal risk.[17] Using a KEW near a nuclear facility runs the risk of catastrophic damage to the reactor and possibly spreading radioactive fallout. Chemical facilities are also of concern. The Bhopal India incident is a striking example of what can go wrong when dealing with toxic chemicals.[18]

The governing body will have to take decisive action on multiple issues. First, they will have to add large-scale KEWs to the existing UN WMD definition, or amend the Weaponization of Space Treaty to include whatever level of KEWs the group deems appropriate. Second, the group must tackle the issue of dual-use technology. Extensive military and commercial uses for the required high-strength materials as well as the propulsion technology will be found, and regulations must govern where, when, and to whom access to these materials and technology can be given. Finally, the governing body must decide whether or not countries that refuse to adhere to these regulations should be given access to the dual-use materials. Historically, this has been a reactionary measure when existing WMD conventions were violated. Hopefully, the lessons learned from the multiple, currently-existing, WMD regulatory bodies will be accounted for by the KEW governing body.

By and large, there is no one correct path to take concerning the future of KEW. Now is the time to be proactive. As these weapons become reality, ignoring the KEW issue could leave the U.S. and the UN in the weaker position of simply having to react once again. Hypersonic technology is not going away. The railgun is here now, and larger KEWs will follow steadily along in its wake. By declaring KEWs to be WMD, the door is kicked open to begin defining the regulations that will be required in the years to come. ***IAJ***

NOTES

1 United Nations Security Council, Commission for Conventional Armaments, August 24, 1948, Dag Hammarskjold Library, retrieved September 2015.

2 David Rajmon, "Impact Database," May 16, 2010, <http://impacts.rajmon.cz/index.html>, accessed on April 12, 2017.

3 Eric Adams, "Rods from God," Popular Science, June 1, 2004, <http://www.popsci.com/scitech/article/2004-06/rods-god>, accessed on April 12, 2017.

4 Bob Preston et al., Space Weapons, Earth Wars, RAND Corporation, Santa Monica, CA, 2002.

5 Headquarters, U.S. Air Force XPXC, "The U.S. Air Force Transition Flight Plan," <http://www.au.af.mil/au/awc/awcgate/af/af_trans_flightplan_nov03.pdf>, accessed on April 12, 2017.

6 "Hypersonic Missiles: Speed is the New Stealth," The Economist, <http://www .economist.com/news/technology-quarterly/21578522-hypersonic-weapons-building-vehicles-fly-five-times-speed-sound>, accessed on September 1, 2015.

7 Guy Norris, "Propulsion, Materials Test Successes Put Positive Spin on Falcon Prospects," Aviation Week and Space Technology, July 23, 2007, <http://aviationweek.com/awin/propulsion-materials-test-successes-put-positive-spin-falcon-prospects>, accessed on September 1, 2015.

8 John Pike, "GBU-43/B 'Mother Of All Bombs,'" Global Security, July 7, 2011, <http://www.globalsecurity.org/military/systems/munitions/moab.htm>, accessed on September 1, 2015.

9 A KEW yield is calculated in Joules, using the kinetic energy equation .5(Mass)(Velocity2). The corresponding energy release in Joules is then divided by the energy released by 1 pound of TNT. This conversion is required due to the most common measure of a nuclear weapon yield is in pounds of TNT. Converting the kinetic energy release into TNT equivalents makes grasping the comparison between KEW and nuclear weapons easier. See Physics Classroom, "Kinetic Energy," November 23, 2015, <http://www.physicsclassroom.com/class/energy/Lesson-1/Kinetic-Energy> and "Kilogram of TNT Conversion Chart," Convert-Me, <http://www.convert-me.com/en/convert/energy/tntkg.html>, accessed on September 1, 2015; Review of U.S. Human Spaceflight Plans Committee, 2009.

10 University of Pittsburgh, "Combustible Metals," 2013, <http://www.ehs.pitt.edu/assets/docs/combustible-metals.pdf>, accessed on April 12 2017.

11 Preston et al.

12 Alex Wellerstein, "Nukemap," Nuclear Secrecy, <http://www.nuclearsecrecy .com/nukemap/>, and Robert Marcus et al., "Earth Impact Effects Program," 2010, <http://impact.ese.ic.ac.uk/ImpactEffects/>, accessed on October 1, 2015.

13 Marcus et al.

14 E. Karl Zipf and Kenneth L. Cashdollar, "Explosions and Refuge Chambers," 2015, <http://www.cdc.gov/niosh/docket/archive/pdfs/NIOSH-125/125-ExplosionsandRefugeChambers.pdf>, accessed on April 12, 2017.

15 Kelly Beatty, "New Chelyabinsk Results Yield Surprises," November 7, 2013, Sky & Telescope, <http://www.skyandtelescope.com/astronomy-news/new-chelyabinsk-results-yield-surprises/>, accessed on April 12, 2017.

16 John Pike, "BLU-82B," FAS Military Analysis Network, March 24, 2004, <http://fas.org/man/dod-101/sys/dumb/blu-82.htm>, accessed on October 1, 2015; Pike, "GBU-43/B 'Mother Of All Bombs.'"

17 Ordtech, "MK82 500 Lbs Aircraft Bomb," 2015, <http://www.ordtech-industries.com/2products/Bomb_General/Mk82/Mk82.html>, accessed on April 12, 2015; Zipf and Cashdollar.

18 Edward Broughton, "The Bhopal Disaster and its Aftermath: A Review," National Center for Biotechnology Information, May 10, 2015, <http://www.ncbi.nlm.nih.gov /pmc/articles/PMC1142333/>, accessed on November 1, 2015.

Worth Noting

Ambassador Kennedy returns to Fort Leavenworth

Ambassador (Ret.) Laura Kennedy returned for a second visit to Fort Leavenworth in April, again serving as the DACOR visiting professor of diplomacy for the U.S. Army Command and General Staff College (CGSC) Class of 2017. Kennedy, who previously served as the Deputy Assistant Secretary of State for European and Eurasian Affairs among many other positions over a nearly 40 year diplomatic career, visited Fort Leavenworth April 4-6. She previously visited in December 2016.

On the first evening of her visit, Ambassador Kennedy attended the opening reception for the spring 2017 National Security Roundtable. At the reception, Kennedy spoke of about geopolitical issues around the world and the importance of diplomacy in today's contentious political climate.

From April 5-6, Kennedy attended student seminars at CGSC. On the morning of April 5, she visited with and spoke to students in "The Interagency and National Security" and "National Security Policy Formation" electives, where they discussed interagency operations overseas, the State Department, and the U.S. Agency for International Development. That afternoon she attended "Eurasia's Evolving Operational Environment," where the conversation focused on Ukraine and the conflict with Russia. On April 6, Kennedy visited "Statecraft and Diplomacy" and "Current Strategic Concepts". In these courses, Kennedy spoke about diplomatic tools and diplomatic power.

Ambassador Kennedy also visited with undergraduate students at the University of Saint Mary in Leavenworth, Kansas on April 6. At the University of Saint Mary, Kennedy spoke about her experiences during her diplomatic career, and encouraged the students to consider careers in the foreign or civil service. The Saint Mary students had a lot of questions for Kennedy, and relished the opportunity to meet a retired ambassador. Later that evening, Kennedy met with students from the University of Saint Mary's Lawrence D. Starr Center for Peace and Justice in our Global Society. Kennedy also received a private tour of the university's Abraham Lincoln collection during her visit.

Once again, Kennedy expressed her admiration of the students and faculty at CGSC, remarking that she greatly enjoyed the opportunity to be part of the DACOR program.

The CGSC Foundation administers this program in conjunction with the DACOR organization in Washington, D.C., and with generous support and involvement of the University of Saint Mary and its Lawrence D. Starr Center for Peace and Justice in our Global Society.

- ***Simons Center***

Dijkerman visits Fort Leavenworth

Career Minister Dr. Dirk Dijkerman recently visited Fort Leavenworth as part of a Simons Center special speakers program. Dijkerman is a retired U.S. Agency for International Development (USAID) Career Minister with a vast amount of experience in the agency, most notably serving as the Executive Coordinator for the U.S. Ebola Task Force in 2014-2015.

While at Fort Leavenworth, Dijkerman attended various elective courses at the U.S. Army Command and General Staff College, discussing the various interagency and international challenges

and the methods he used to successfully address them. He also spoke at Park University in Parkville, Missouri.

Dijkerman also attended one of the Simons Center's InterAgency Brown-Bag Lectures, where Mr. Patrick J. Wesner, the Command and General Staff College Distinguished Chair for Development Studies, led a discussion on the roles and missions of USAID. Dijkerman contributed to Wesner's presentation, speaking about his experience at USAID, particularly about his experience on the U.S. Ebola Task Force.

- Simons Center

Kelly calls for more cooperation, 'heavy artillery' in cyber

On April 18, Department of Homeland Security (DHS) Secretary John Kelly spoke at George Washington University Center for Cyber and Homeland Security. In his speech, titled "Home and Away: DHS and the Threats to America," Kelly discusses the importance of collaboration between DHS and other government agencies and warned against the "plodding pace of bureaucracy."

Kelly's remarks centered around threats facing the United States, including cybersecurity, terrorism, and criminal drug gangs. According to Kelly, U.S. cybersecurity needs "heavy artillery." Failing to develop cyber capabilities and defenses would be like "sending troops to take Fallujah armed with muskets and powdered wigs," said Kelly.

Kelly did not have an update on the long-delayed executive order on cybersecurity.

- Department of Homeland Security

Multidomain integration key to deterrence

Navy Vice Admiral Charles A. Richard, deputy commander of U.S. Strategic Command, spoke at a space security conference at the Center for Strategic and International Studies on March 22.

In his remarks, the admiral spoke of the importance of multidomain integration, noting the Joint Interagency Combined Space Operations Center (JICSpOC) in Colorado Springs, Colorado. According to Richard, JICSpOC facilitates integrated operations across joint forces by serving as a hub for collaboration and experimentation on new space system tactics, techniques and procedures. JICSpOC also increases DoD and intelligence community unity of effort.

Richard also spoke of integrating space operations on a global scale, saying "The idea is to promote the exchange of information with like-minded spacefaring nations to maintain and improve space-object databases, and to promote the responsible, peaceful and safe use of space and to strengthen cooperation in the global space community."

- Department of Defense

USAID the topic of InterAgency Brown-Bag Lecture

On April 6, Mr. Patrick J. Wesner, the U.S. Army Command and General Staff College Distinguished Chair for Development Studies, spoke about history and mission of the U.S. Agency for International Development (USAID). Three special guests were in the audience during Wesner's presentation on USAID – Ambassador (Ret.) David Lambertson, Ambassador (Ret.) Laura Kennedy, and Career Minister (Ret.) Dirk Dijkerman, Ph.D.

USAID is the lead U.S. government agency that works to end extreme global poverty and enable resilient, democratic societies to realize their potential. USAID carries out U.S. foreign policy by promoting broad-scale human progress at the same time it expands stable, free societies, creates

markets and trade partners for the U.S., and fosters good will abroad. Its efforts further America's interests while improving lives in the developing world.

Wesner's presentation was the seventh lecture in the new InterAgency Brown-Bag Lecture Series. Information on upcoming lectures in the series will be available on the Simons Center's website at a later date.

- Simons Center

DHS Secretary calls for greater cooperation

Department of Homeland Security (DHS) Secretary John F. Kelly testified to the Senate Committee on Homeland Security and Governmental Affairs on the subject of border security and public safety on April 5. Kelly remarked on DHS's border security mission and efforts.

In his testimony, Kelly called for greater interagency and international cooperation, saying "Interagency relationships and bilateral cooperation are critical to identifying, monitoring, and countering threats to U.S. national security and regional stability." Kelly went on to say that the challenges faced by DHS in confronting illegal immigration, transnational crime, human trafficking, and other threats to U.S. safety require an "integrated counter-network approach."

Kelly concluded his testimony by reiterating DHS's commitment to border security and his commitment to the committee.

- Department of Homeland Security

Interagency effort needed to combat illicit fentanyl

In February, officials from multiple government agencies met with the House Energy and Commerce Committee to discuss fentanyl, a synthetic opioid that is 50 times more potent than heroin and 100 times more potent than morphine.

Among those speaking were Matthew Allen, Assistant Director for U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations. Allen spoke about the dangers of fentanyl and of ICE's efforts to reduce the supply of heroin and fentanyl in the U.S.

The Heroin Availability Reduction Plan (HARP), developed by the Office of National Drug Control Policy in coordination with federal departments and agencies, reduces the supply of heroin and illicit fentanyl in the U.S. through various means, including supply chain disruption. According to Allen, ICE is targeting supply chain networks and collaborating with both domestic and international partners.

ICE is also part of the Drug Enforcement Agency's interagency Heroin and Fentanyl task force, which focuses on the collaborative authorities and efforts of each invested agency's resources, in order to better share and deconflict information. ICE and the task force are coordinating in several areas related to the combating fentanyl.

In his closing statement, Allen said that "ICE is committed to battling the U.S. heroin and illicit fentanyl crisis through the various efforts I have discussed today," and that "this problem set is an epidemic that demands urgent and immediate action across law enforcement interagency lines.

- Energy and Commerce Committee, House of Representatives

DoD officials discuss WMDs, new threats

On March 23, senior defense officials spoke before the House Committee on Armed Services on the subject of traditional weapons of mass destruction and the use of new synthetic biological tools.

Dr. Arthur T. Hopkins, acting assistant secretary for nuclear, chemical and biological defense programs, testified on the Department of Defense's (DoD) expanding responsibilities in countering WMD. While the focus used to be nuclear deterrence, programs now include chemical and biological defense, chemical demilitarization, and reducing the threat of improvised explosive devices.

According to Hopkins, synthetic biology, defined as using sophisticated techniques and tools to sequence, synthesize and manipulate genetic material, can be used for both adversarial and peaceful purposes. "The same tools of synthetic biology that we're concerned about as being capable of being used against us, we are also using in the laboratories to help develop countermeasures," said Hopkins. He went on to say that the department has asked the National Academy of Sciences to produce an interagency study of potential impacts on national security, including when potential threats might arise and how the DoD can react should there be a threat.

Also speaking were Peter Verga, performing the duties of the assistant secretary of defense for homeland defense and global security, who spoke on threats posed by North Korea and ISIS, and Shari Durand, acting director of the Defense Threat Reduction Agency, who testified on the need for an early-warning system for chemical and biological weapons.

- House Committee on Armed Services

Former DHS official calls for commisson on new roles, missions

In a recent Homeland Security Today article, a former Department of Homeland Security (DHS) official stated that DHS is in need of reauthorizing legislation that will reaffirm and update the department's organizations and functions. Daniel M. Gerstein, who was the undersecretary (acting) and deputy undersecretary in DHS's Science and Technology Directorate from 2011 to 2014, also said that such legislation should begin with a roles and missions commission for DHS.

In his article, Gerstein notes that "Such a review is not without precedent," citing the National Defense Authorization Act of 1994, which included a requirement that the Department of Defense "review … the appropriateness … of the current allocations of roles, missions and functions among the armed forces…" This type of review, says Gerstein, "is needed today for DHS."

DHS has seen some changes since it was established through the Homeland Security Act of 2002, but the department has not received a top-down assessment that a roles and missions review would provide. Gerstein lists several key areas that would benefit from a roles and missions commission, including cybersecurity, weapons of mass destruction, and critical infrastructure, as well as human factors that impact homeland security, such as the relationships between DHS, state and local authorities, the private sector, and others.

"A DHS roles and missions commission would be an ideal undertaking to ask fundamental questions about the functioning of the Homeland Security Enterprise as the 15 year anniversary of the Homeland Security Act of 2002 approaches." concludes Gerstein.

- Homeland Security Today

DHS releases first Declined Detainer Outcome Report

In March, the Department of Homeland Security (DHS) issued the first U.S. Immigration and Customs Enforcement (ICE) Declined Detainer Outcome Report (DDOR). The DDOR is mandated by the president's executive order "Enhancing Public Safety in the Interior of the United States," signed on January 25 of this year.

ICE places detainers on aliens who have been arrested on local criminal charges or who are in local custody and for whom ICE possesses probable cause to believe that they are removable from the United States, so that ICE can take custody of the alien when he or she is released from local custody. The DDOR is a weekly report that shows jurisdictions that choose not to cooperate with ICE detainers or requests for notification, and includes a list of sample crimes associated with those released individuals.

Acting ICE Director Thomas Homan spoke of the need for full law enforcement and ICE cooperation in fulfilling the executive order, saying "When law enforcement agencies fail to honor immigration detainers and release serious criminal offenders, it undermines ICE's ability to protect the public safety and carry out its mission." He went on to say that ICE's goal "is to build cooperative, respectful relationships with our law enforcement partners. We will continue collaborating with them to help ensure that illegal aliens who may pose a threat to our communities are not released onto the streets to potentially harm individuals living within our communities."

This DDOR reports on noncompliance that ICE is aware of, and future DDORs will likely reflect higher numbers of declined detainers as ICE plans to resume sending detainers to known uncooperative jurisdictions.

- Department of Homeland Security

Sixth InterAgency Brown-Bag Lecture focuses on intelligence

On March 15, Mr. Gustav A. Otto presented on the subject of the Defense Intelligence Agency (DIA) at the latest InterAgency Brown-Bag Lecture. The DIA is one of our nation's least understood intelligence organizations, and is the premier all-source military intelligence organization, providing authoritative assessments of foreign military intentions and capabilities.

Otto, who is the Defense Intelligence Chair and DIA Representative to the Combined Arms Center and Army University, spoke about the history and role of the DIA before inviting the audience's questions. From there, Otto discussed the training and education of DIA personnel and DIA's relationship with the intelligence community and other U.S. government entities. Audience members also asked about the intelligence community's relationship with the current administration, which has been a hot topic lately, and about the intelligence community's focus on counterterrorism instead of, and possibly to the detriment of, cybersecurity and other national security issues.

- Simons Center

Gary Sinise awarded AUSA's highest honor

On March 15, the Association of the United States Army (AUSA) announced that actor and humanitarian Gary Sinise had been selected as the 2017 recipient of the George Catlett Marshall Medal for his commitment to the men and women of our nation's armed forces. Sinise will receive the award, AUSA's highest award for distinguished public service, at the Marshall Dinner in October.

"I am honored to be invited to receive the George Catlett Marshall Medal from the Association of the United States Army," Sinise said. "It has been a great blessing to know there is something I can do to support the men and women in uniform who defend our nation and I will look forward to expressing my gratitude in person…"

Mr. Sinise has been a friend of the U.S. Army Command and General Staff College (CGSC) and the CGSC Foundation for many years, establishing the Lt. Col. Boyd McCanna "Mac" Harris Leadership Award at CGSC in 2014. The CGSC Foundation and the Simons Center congratulate Mr. Sinise and thank him for his dedication to the our military men and women and their families.

- Simons Center

State releases narcotics control report

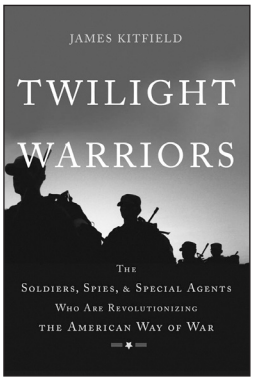
In March the Department of State released the 2017 International Narcotic Control Strategy Report (INCSR). In a teleconference on March 2, Assistant Secretary for International Narcotics and Law Enforcement Affairs William Brownfield introduced the INCSR, saying "This report… tells a picture of the international architecture that is now in place around the world to help us address this crisis in the United States."

According to Brownfield, the two volume report "lays out a good global architecture for more than 100 nations of the world to cooperate and work together to address the drug issue." Brownfield admitted that, while there are serious international drug problems to face, the U.S. is in a better position to address these problems than they have been in the past few decades.

Volume 1 of the INCSR focuses on drug and chemical control, while volume 2 focuses on money laundering and financial crimes. The report credits both international and interagency cooperation with successful endeavors to minimize drug problems and related criminal activity around the world.

- Department of State

Book Review



Twilight Warriors: The Soldiers, Spies, and Special Agents Who Are Revolutionizing the American Way of War

James Kitfield

Basic Books, 2016, 416 pp.

Reviewed by Col. Joseph Judge III, U.S. Army, Ret.
Assistant Professor
U.S. Army Command and General Staff College

In the years after 9/11, top U.S. military and political leaders were heavily engaged in how best to successfully defeat Al-Qaeda and Taliban terrorists in Iraq and Afghanistan. Despite the global launch of the war on terrorism, the passing of the U.S. Patriot Act, and the skyrocketing of budgets of all defense-related agencies, the terrorist insurgency networks still grew. Though there were initial counter terrorist victories, the insurgencies intensified as U.S. security agencies' synergy ebbed more than flowed. Chairman of the Joint Chiefs of Staff General Martin Dempsey had his "black swan moment" in 2004 as the then First Armored Division Commander exclaiming he would never forget his shock at a Shiite uprising and the collapse of the Iraqi units his forces had trained. We had relied too heavily on technology instead of anthropology and sociology to understand what was "on the Iraqi minds" in the street. One of his junior officers had foreshadowed to be wary of "false positives."

Reminiscent of a Ken Burns' historical movie documentary, James Kitfield in his latest work, *Twilight Warriors*, braids an intriguing chronological story that begins in 1998. He draws on years of firsthand experiences and senior defense leader associations. A rendering of a tight-knit group of interagency leaders who would ultimately break down age-old stovepipes resulting in an "unprecedented level of networked counterinsurgency (COIN) and intelligence cooperation between traditionally distrustful U.S. conventional and Special Operations Forces - and - between military, intelligence and law enforcement agencies." Kitfield centers his book on four key players, three military generals and an FBI special agent.

Kitfield portrays West Point classmates, Generals Martin Dempsey, Stanley McChrystal and David Petraeus as "preeminent leaders who would form the definitive narrative of a new revolution in the American style of war." This model relied on unprecedented civ-mil coordination, and modern COIN operations as the "fastest way to drain the extremism swamp." COIN lessons and doctrine had been expunged from military school curriculum and Dempsey lamented that the masters of maneuver warfare had created a generation of officers conditioned to go by the "doctrinal book" and not seek innovative solutions.

Kitfield describes Petraeus as a hero of the Iraq surge. From his doctoral thesis at Princeton on

COIN, to his leading of the rewriting of the Army COIN manual, he was steeped in COIN warfare. On his headquarters entry was, "Will this operation take more bad guys off the street than it creates by the way it is conducted?" He emphasized that insurgencies were for political power and any effective COIN campaign requires a tightly coordinated civil-mil partnership.

McChrystal, served as the Special Operations Forces Joint Special Operations Command Commander. His intelligence chief was Michael T. Flynn who would later become the Defense Intelligence Agency Director and President Trump's resigned National Security Agency director. Kitfield discusses how McChrystal and Flynn's network broke down the walls of traditionally separated intelligence agencies, analysts and operators. They created Task Force 714, a multiagency joint task force, and intelligence fusion centers which combined all the military, intelligence and law enforcement agencies that had a piece of the counter terrorist mission and drove them to "mind meld" as one coherent team, a level of centralized command and decentralized execution by multiple agencies that had not been accomplished before. The team learned that some agency sources were "triple and quadruple dipping" as well as providing contradictory information. It takes a network to defeat a network.

McChrystal and Flynn were pivotal in pioneering the emergence of drones, a superstar in the network of intelligence, surveillance and reconnaissance assets, whether it be as high value target strikes or following known or suspected terrorists.

Another integral visionary leader Kitfield revealed was the FBI's Brian McCauley, who led the network's suicide bomber tracking using serial-killer profile techniques. Despite the FBI and CIA's intense disagreements about interrogation, this led to the closest ever collaborations between the FBI, CIA and the military. McCauley, always seeking intelligence links to U.S. plots, was able to impact an extensive human source network overseas.

McChrystal dubbed the successful cyclic model against terrorist targets as F3EA or find, fix, finish, exploit, and analyze. Kitfield detailed how well it ultimately worked in Iraq and Afghanistan once the National Security Agency inserted its intelligence fusion system into the F3EA cycle. It was the "Amazon.com of counterterrorism." By 2008, insurgent attacks had fallen over 80%. An Air Force chief boasted recon missions in 1991 Desert Storm required days to deliver pictures of questionable accuracy - to thirty frames per second to anywhere on earth within seconds. That was the power of the network.

Kitfield then devoted one third of his book gauging the network's warfighting success against discrete global terrorist targets. Flynn had built on Joint Special Operations Command's network centers and "shook up" the Defense Intelligence Agency by creating five intelligence integration centers and growing its clandestine services. The National Counterterrorism Center (NCTC) maintained a clearinghouse of suspected terrorists and groups with numerous links between intelligence community databases. "Over 40% of NCTC personnel were from other civilian and military agencies borrowing many pages from the F3EA playbook." Terrorist plots quietly ended in arrests or kills. In 2013, Al Shabab terrorists enveloped an upscale Nairobi, Kenya mall. FBI's McCauley dispatched a rapid deployment team that was in place by day two. The dramatically compressed intelligence-gathering and decision making cycle in the F3EA model was evident two weeks after the mall attack as U.S. commandos conducted simultaneous raids in Somalia and Libya.

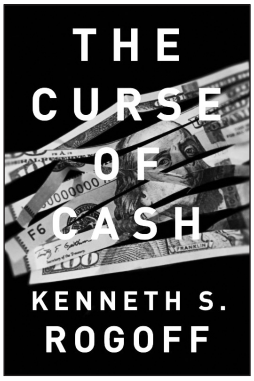
Kitfield lamented how the State Department resisted network partnerships with civilian corporations. But in 2014, terrorists hijacked a ConocoPhillips ship with over one million barrels of oil and the network "chatter" was an impending environmental disaster in the Mediterranean Sea.

The USS Roosevelt sent a "special" team which boarded and captured the three Libyan hijackers.

Will this model continue to keep the U.S safe? Can our counter terrorist network keep pace with the rapidly evolving threat? Working with counter terrorist partners on the front lines of the Global War on Terror after 9/11 proved invaluable to keep the terrorist threat from crippling the U.S. Though the network had begun linking with industry, Kitfield unfortunately omitted discussion of other nation's or NATO's links to the network. Select allies and partners would truly make this a unified action network. A globe-spanning network of significant lethality may be the only way to proceed in the future.

Kitfield asserts the tempo of F3EA must continue to keep pace with the "Hydra headed" terrorist networks. It will be expensive. We should be very concerned when each agency is competing for scarce resources. Stovepipes can quickly build in a time of budget cuts or political partisanship. Kitfield also placed significant emphasis on agency collaboration and the "personal" relations between interagency leaders who are essentially now out of the picture. Scarce agency resources coupled with scarce interagency bonds presages a repeat of past challenges. Be wary of false positives.

Twilight Warriors is more than just a great book on recent U.S. counterterrorism matters and the leaders who battled it. Kitfield's compelling accounting of the network and its global implications warrants it as a decidedly recommended reading for anyone, not just those interested in existing military, interagency, or civ-mil issues. ***IAJ***



The Curse of Cash

Kenneth S. Rogoff

Princeton University Press, 2016, 283 pp.

Reviewed by Dr. David A. Anderson
Professor
U.S. Army Command and General Staff College

Author Kenneth Rogoff is an Economics Professor at Harvard University. He is a world renowned academic scholar who has published a plethora of books and articles in the field of economics. In *The Curse of Cash*, Rogoff addresses whether advanced countries of the world, led by the U.S., should start phasing out the use of paper money (cash), except for small denominated bills and coins.

Rogoff's introduction immediately gains the attention of the reader painting an insightful and intriguing word picture. He reports that some 80% of the $1.34 trillion held outside of U.S. banks is denominated in $100 bills. The aggregate total of this cash is enough to provide every American $4,200, whereas the average American claims to carry less than $75 in their wallet. Meaning for that volume of paper money, most is in the hands of criminals for illicit use in the U.S., driving home the point of getting rid of it.

The premise of his examination lies in the inefficiencies and abuses with the inherent use of cash. He notes that the use of cash in conducting business transactions is often to avoid paying taxes. The U.S. government loses over $500 billion in tax revenue annually due to tax evasion. Cash lends itself to supporting criminal activity. It is also used by terrorists to finance their operations and corrupt officials in lining their pockets.

Eliminating cash in advanced economies would also afford central banks the option to offer negative interest rates, should it become necessary, to stimulate economic growth. Under a cash based system, countries have little monetary discretion to promote economic growth or in reducing inflation by lowering interest rates much below zero. The worry being, at some point below zero interest, investors would dump government denominated debt instruments for cash, and bank depositors would pull their cash to avoid the below zero interest penalty, then stashing their money in places not accessible for lending/investing.

The book is broken down into a three part journey as the author goes about persuasively waging his argument. In the first section he addresses the history of currency, backed and unbacked, including the history of the gold standard. He devotes other chapters in this section to the size and composition of global currency supplies, legal currency in the tax-paying economy, currency in the underground economy, monetary seigniorage and opportunity cost seigniorage, and his plan for phasing out most paper money.

Interesting facts and figures emerge throughout these chapters. Norway has the lowest cash to GDP ratio at 1.24 percent in the developed world, whereas Japan has the highest at 18.61 percent. The U.S. figure is 7.38 percent. Eighty-seven percent of China's currency is denominated in its

largest bank notes. The overwhelming majority of purchase transactions within the developed world are of value less than $20 U.S.

Forty-four percent of all U.S. paper money in circulation is held by foreigners. Most of this money is denominated in $100 dollar bills. The annual world drug market revenue is approximately $600 billion U.S. The illicit drug market conducts business in currency denotations of $100 U.S. or greater. Underground economies operate in cash and represent 7 percent (U.S.) to 29 percent (Turkey) of an advanced country's GDP. Corruption is largely conducted in cash. The global aggregated value of corruption is priced at $2 trillion U.S. The aforementioned figures help paint a fascinating word picture about currency and currency use around the world.

In the second section, Rogoff somewhat abruptly transitions to tackle the topic of negative interest rates and its implication on the use of paper currency. In doing so, he addresses paths and impacts of negative interest rates, the role of inflation targeting, nominal GDP, and fiscal policy effects. He notes that the history of negative rates is very limited.

During the 1990s, Japan used negative rates to spur economic growth. Over the past five years, a number of European countries have drifted to near or completely negative rates as a means to revitalize their economies from the aftermath of the Great Recession of the previous decade. Rogoff points out that negative rates are no panacea for a country's ills. It does come with risks. Negative rates may be seen as a direct tax on currency deposits and a violation of the depositor trust.

It may also be perceived as a coercive act waged by government forcing lenders to lend, or depositors to spend. This perception could lead to a run to cash by depositors--taking their money out of the banking system and sitting on it-- the opposite affect desired.

Negative rates can also lead to higher inflation than desired. The over stimulation of economic activity. Negative rates do help prevent credit contraction, whereas near zero rates may contract lending. This was the case in the U.S., post-2008. At the same time that interest rates were being lowered to encourage borrowers, U.S. banks were tightening their lending practices to avoid the risk of inflation eating away at their low yielding interest income on loans and borrower default.

In the final section, Rogoff speaks to the international dimensions of phasing out paper money the use of digital currencies, and gold's impact on a paperless system. He describes how U.S. domestic currency could not be practically replaced by foreign notes for illicit activities. He does ultimately see value in G-7 nations ridding themselves of paper money, particularly their large notes. Rogoff wages an argument that even emerging market countries could benefit for such a practice. However, he recognizes some of the problematic challenges that must be overcome in accommodating people such as the rural poor. The emergence of digital currency such as Bitcoin generate concerns but do not undermine the elimination of paper money. Finally, he asserts gold will always have its historical lure as a tangible safe haven against economic uncertainty, but will not rise again beyond backseat monetary status.

In *The Curse of Cash*, Rogoff wages a highly compelling, thought-provoking, and transformative proposition to rid or limit the use of paper currency. He provides a unique understanding into the function of paper money and its impact on such things as tax revenue, credit and institutional lending, monetary and fiscal policy, interest rates, and their collective effect on the macroeconomics of states. His objective approach to the subject and comprehensive analysis is rich in scope and scale, including insight from many of the sharpest minds in the field of business and economics. It is loaded with contributions from a "Who's Who" of academic scholars including those having worked in the U.S. Treasury, the U.S. Federal Reserve, and international financial institutions. Rogoff skillfully

leverages their research and opinions to not only support his own belief, but to also challenge his thought process--a refreshing but not so common practice these days.

The book is remarkable in its ease of readability and the number of supporting figures, tables, and diagrams. A broad array of readers will find this body of work a valuable read. However, it is best examined by those in U.S. government agencies involved in shaping monetary and fiscal policy, government revenue collection, combating criminal activities (including terrorist financing), and economic and trade policy. ***IAJ***

The ***InterAgency Journal (IAJ)*** is published 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 and/or which stem from lessons learned via personal experiences.

For additional information visit the Simons Center website at

www.TheSimonsCenter.org/publications

The Simons Center
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.