COMMAND AND GENERAL STAFF COLLEGE FOUNDATION, INC

COL. ARTHUR D. SIMONS CENTER FOR THE STUDY OF INTERAGENCY COOPERATION

The Simons Center
Fort Leavenworth, Kansas

InterAgency Journal

The Journal of The Simons Center
Vol. 8, Issue 3 (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 3 (2017)

Arthur D. Simons Center
for Interagency Cooperation
The Lewis and Clark Center
100 Stimson Ave., Suite 1149
Fort Leavenworth, Kansas 66027
Ph: 913-682-7244 • Fax: 913-682-7247
Email: office@TheSimonsCenter.org
www.TheSimonsCenter.org

Features

Simons Center Editorial Board

From the Editor-in-Chief

This issue of the *InterAgency Journal* offers a variety of topics I hope you find interesting and informative. Our lead article is the 2017 Simons Center Interagency Writing Award winner from the School of Advanced Military Studies at the U.S. Army Command and General Staff College. Patricia Ladnier puts forth that a strategic review is needed to inform the realignment of federal statutory law to allow the Department of Homeland Security to implement various recommendations to achieve its national security goal of critical infrastructure protection.

Our world continues to be a dangerous place. The next three articles explore what might be done to address some of our challenges. Matthew Rautio argues that the key to successful counterproliferation is fostering interagency collaboration before a crisis emerges. He informs this conclusion with data from a formal collaboration process undertaken at a U.S. Embassy. Brendan Melley discusses the threat of nuclear terrorism. He offers that our best chance to stop nuclear terrorism is a combination of focused policies to restrict the materials needed to build nuclear bombs along with continuous efforts to deny potential terrorists the time and space to gather and assemble weapons. And Terrance Allen argues that the United States needs to take the lead for the international community and develop a treaty for international norms which set limits on offensive cyberspace operations. He also calls for the U.S. to develop and articulate a clear deterrence strategy for the cyber domain.

While the “whole-of-government” approach is often necessary to address the complex problems of national security, our system does not have a professional development path for interagency leaders. Rather, we develop folks inside our own organizations and when interagency leadership opportunities arise we often are not prepared for the challenge. Duane Blackburn shares his perspective and offers informed insight on successful interagency leadership garnered from years of service at the highest levels of the federal government.

The next two articles address shortcomings. Gus Otto takes to task the Department of Defense’s use of operational phases in their planning process and decries how their misuse has negatively affected other departments of the federal government. Michael Jones points out that the U.S. government faces many challenges when conducting civil information management around the world. And unfortunately one of them is an unnecessarily self-imposed problem – various departments use different information platforms which are not compatible or are redundant. He argues that our government must synchronize information systems to better facilitate information sharing.

Leaders make decisions. But do we take into account the biases and psychological traps that affect our decision making? Ted Thomas and Robert Rielly use a historical case study to illustrate the traps that await if one is not aware of their own psychological baggage.

And finally, John Breen provides a historical look at covert CIA actions to examine if they actually can be deemed as successful in advancing U.S. foreign policy goals.

Thank you for reading this issue of the *InterAgency Journal*. Our readership has crested over 11,000 and I thank you for helping us meet our mission of developing interagency leaders and adding to the body of interagency knowledge. I invite you to become an author and share your interagency observations and experiences. And as always, your feedback is most welcome. – **RMC**

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 COMMAND AND GENERAL STAFF COLLEGE FOUNDATION, INC.

In Partnership With

PEOPLE to PEOPLE
Greater Kansas City

Chamber of COMMERCE
LEAVENWORTH LANSING AREA
Operation International

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

Critical Infrastructure Protection

by Patricia Ladnier

Both the Department of Homeland Security (DHS) and the Department of Defense (DoD) work to secure and defend the U.S., including protecting and securing key resources and critical infrastructure (referred to collectively as critical infrastructure). The Constitution and federal statutory law establish national security goals. The Critical Infrastructures Protection Act of 2001 (CIPA) articulates as a national security goal the protection of critical infrastructure by a public-private partnership.[1] The Homeland Security Act of 2002 specifically tasks the DHS with preventing terrorism and protecting critical infrastructure.[2] Much of the nation's critical infrastructure is interdependent and interconnected and is not owned by the federal government.[3]

Critical infrastructure sustained damage in multiple post-9/11 disasters or emergencies. Reports about some of these catastrophes analyze lessons learned. Two key tasks for critical infrastructure protection emerge as crucial: (1) establishing standards and enforcing compliance with the standards; and (2) physically protecting and securing critical infrastructure routinely and in an emergency. Reviewing relevant existing federal statutory authority for the DHS and the DoD to perform these two key tasks reveals that authority is insufficient to achieve these tasks. A strategic review should realign federal statutory law to allow the DHS to implement recommendations to achieve its national security goal of critical infrastructure protection.

The statutory framework to implement constitutional authority historically authorized the DoD to defend the nation and support national defense policies. The CIPA linked national security and critical infrastructure protection. "Critical infrastructure" is an asset or a system that, if incapacitated or destroyed, "would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[4] After 9/11, the Homeland Security Act of 2002 created and authorized the DHS for the mission of homeland security to prevent terrorism, reduce vulnerability to terrorism, and prepare for and respond to terrorism and other disasters and emergencies. The DHS entities most concerned with critical infrastructure protection are the National

Patricia Ladnier is a management and program analyst with the U.S. Department of Homeland Security. She has earned a B.A. in Political Science/History and Economics from Graceland University, a Masters of Military Art and Science from the U.S. Army Command and General Staff College's School of Advanced Military Studies, and a JD from the University of Virginia School of Law.

Protection and Program Division's (NPPD) Federal Protective Service (FPS) and Office of Infrastructure Protection (OIP), the Federal Emergency Management Agency (FEMA), and the U.S. Coast Guard (USCG).

CIPA and Presidential Policy Directive-21 (PPD-21) designated specific infrastructures or sectors as critical. PPD-21 states that infrastructure owners are best suited to manage risks and to determine security strategies. PPD-21 assigned specific federal entities as responsible sector-specific agencies. The DHS is responsible for eight of the sixteen sectors and in conjunction with the General Services Administration (GSA) and the Department of Transportation (DOT) for another two. The CIPA and PPD-21 explicitly state, as national policy, reliance on a public-private partnership for critical infrastructure protection. Recent events, including physical attacks on the electric grid and the 2010 British Petroleum Deepwater Horizon oil well failure disaster, cast doubt on this reliance. This doubt is compounded when considering that non-federal infrastructure sectors, including foreign owners, own much of U.S. critical infrastructure. Multiple reports from some post-9/11 disasters and emergencies provide observations, conclusions, and recommendations about critical infrastructure protection. Key tasks for critical infrastructure protection discussed in these reports are to establish standards and enforce compliance and physically protect and secure the critical infrastructure routinely and in an emergency. These reports made many recommendations for protective measures.

...DHS regulatory authority to set standards is very limited and offers no mechanism for an integrated, strategic, regulatory framework for critical infrastructure protection.

This article focuses on these key tasks because they appear in multiple reports and illustrate basic protective measures. These key tasks are the basis for evaluating the existing federal statutory authority for the DHS and the DoD to protect critical infrastructure.

The CIPA and Homeland Security Act contain no new regulatory authority for critical infrastructure protection. The DHS has limited statutory authority to establish standards and enforce compliance and physically protect and secure critical infrastructure.

No statutory authority exists for the DoD to issue regulations to set standards for critical infrastructure protection, which is appropriate for a civilian government. The DoD's statutory authority would permit physically protecting and securing critical infrastructure, but only in certain emergency-type situations. Further, multiple challenges experienced by the DoD in executing its existing federal statutory authority could exacerbate or compromise its ability to protect critical infrastructure in a crisis.

As a result, the DHS regulatory authority to set standards is very limited and offers no mechanism for an integrated, strategic, regulatory framework for critical infrastructure protection. Second, the DHS and the DoD statutory authority to physically protect and secure critical infrastructure routinely and in emergencies is limited to specific sectors and circumstances. Third, no statute defines how the DHS and the DoD are to work together to achieve national security and, more specifically, critical infrastructure protection, even in an emergency or a crisis.

The Homeland Security Act makes clear that the DHS mission is separate from the DoD mission and reaffirms the DoD statutory authority. However, it offers no authority for an integrated response or single command authority.[5] These conclusions show a deficiency in the current federal statutory authority.

A strategic review of national security policy should examine policy assumptions and practicalities of critical infrastructure protection. Such a review should result, where warranted, in strategic, integrated policy revisions and realign statutory authority with mission accomplishment. The policy and assumptions in CIPA, PPD-21, and the Homeland Security Act rely on the public-private partnership to achieve critical infrastructure protection. Also, regulatory authority that may cover critical infrastructure is diffused among multiple separate DHS entities and federal agencies that historically have been concerned with safety issues, not national security. Almost sixteen years have passed since 9/11 and the passage of the CIPA. Multiple reports warn of gaps in critical infrastructure protection.[6] Statutory amendments could also address two other specific considerations identified in this article: repealing the statute that criminalizes *posse comitatus* and fixing the dual-command problem.

The DHS has made much progress toward a safer, more resilient nation as detailed in reports to Congress by the DHS and the General Accountability Office (GAO).[7] Now it needs the tools to move to the next level to ensure implementation of recommendations from assessments and studies.[8] This article surveys federal statutory authority most relevant to protecting the nation's critical infrastructure generally and as a whole and focuses on two aspects. First, the DHS entities studied (FPS, OIP, FEMA, and the USCG) are the ones concerned generally with working to protect all sectors of critical infrastructure. This article does not consider highly technical and specialized sectors, such as cyber, nuclear, and nuclear waste, or a DHS entity that is responsible for one specific function, such as the Transportation Security Administration. Second, the plain text of federal statutes is reviewed, without reference to interpretation through federal executive agency regulations or judicial case law. Reviewing more than the plain meaning of the statutes exceeds the scope of this article.

The challenge of critical infrastructure protection is highly relevant, not only because of terrorism, but also because of aging and decaying infrastructure and the looming need to invest heavily in it. These circumstances present an opportunity to adopt standards to compel compliance with the standards, through regulation if needed, and also to ensure clear authority for physical protection and security where an owner fails to adequately protect the infrastructure. Given the interdependent and networked nature of the nation's critical infrastructure, it is important to build on years of work by the DHS. The DHS has worked to assess the critical infrastructure and build partnerships and frameworks for public-private collaboration. The next logical step is to shepherd the nation through implementing recommendations from assessments and collaborative efforts to ensure that the critical infrastructure is protected and the nation is resilient in a crisis.

The DHS has made much progress toward a safer, more resilient nation...

National Security and Critical Infrastructure Protection

An understanding of the constitutional and statutory framework for national security and critical infrastructure protection is necessary before beginning the analysis of the DHS and the DoD federal statutory authority for protecting the nation's critical infrastructure. The U.S. Constitution's preamble highlights security as part of the purpose for establishing the Constitution: "to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of

Army	Air Force
"preserving the peace and security, and providing for the defense, of the United States; supporting the national policies; implementing the national objectives; and overcoming any nations responsible for aggressive acts that imperil the peace and security of the United States." 10 US Code, (2017), §3062(a).	"preserving the peace and security, and providing for the defense, of the United States; supporting the national policies; implementing the national objectives; and overcoming any nations responsible for aggressive acts that imperil the peace and security of the United States." 10 US Code, (2017), §8062(a).
Navy	**Marine Corps**
"for prompt and sustained combat incident to operations at sea. It is responsible for the preparation of naval forces necessary for the effective prosecution of war except as otherwise assigned." 10 US Code, (2017), §5062.	"to provide fleet marine forces of combined arms, together with supporting air components, for service with the fleet in the seizure or defense of advanced naval bases and for the conduct of such land operations as may be essential to the prosecution of a naval campaign. In addition, the Marine Corps … shall provide security detachments for the protection of naval property at naval stations and bases, and shall perform other duties as the President may direct." 10 US Code, (2017), §5063.
Source: **Author, created from identified sections of the US Code (2017), Title 10 (Armed Forces).**	

Table 1. Statutory Purpose for Army, Air Force, Navy, and Marine Corps

Liberty to ourselves and our Posterity." The Constitution grants to the federal government authority and responsibility for national security. Early federal statutes enabled the military to protect the nation. More recent statutory law authorizes the DHS to protect the homeland from terrorism. Recent national policy recognizes the priority of protecting critical infrastructure as vital to the nation's security and relies on a public-private partnership solution.[9]

DoD and DHS Missions for Homeland Defense and Homeland Security

Individual military services historically have implemented the constitutional mandates to protect the U.S., culminating in consolidating the Army, Navy and Marine Corps, and Air Force into the DoD after World War II.[10] Table 1 defines these functions.

The DoD is responsible for protecting the nation through homeland defense[11] and supporting national policies. DoD doctrine defines homeland defense as "the protection of US sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression, or other threats as directed by the President."[12]

The more recent Homeland Security Act of 2002 created the DHS. The DHS entities most directly responsible for physical critical infrastructure protection of multiple infrastructure sectors are the NPPD, FEMA, and USCG.[13] NPPD includes the FPS, which protects federal government property,[14] and the OIP, created by the Act to promote protection of critical infrastructure generally. FEMA previously was an independent federal agency focused on disaster and emergency preparedness and response and now also, according to statutory authority, is to work toward infrastructure protection and resilience. The USCG is a military service and a branch of the armed forces, transferred from the DOT. It may operate as part of the U.S. Navy upon a Congressional declaration of war or when the President directs.[15] The USCG's mission is to protect and defend U.S. ports, inland waterways, coastline, and territorial waters. Table 2 summarizes the major relevant responsibilities of the DHS and these DHS entities.

DHS	Coast Guard
The primary missions of the Department are to “prevent terrorist attacks within the United States; reduce the vulnerability of the United States to terrorism; minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States; carry out all functions of entities transferred to the Department, including by acting as a focal point regarding natural and manmade crises and emergency planning.” 6 US Code, (2017), §111(b).	““…enforce or assist in the enforcement of all applicable Federal laws on, under, and over the high seas and waters subject to the jurisdiction of the United States.” “…engage in maritime air surveillance or interdiction to enforce or assist in the enforcement of the laws of the United States.” “…administer laws and promulgate and enforce regulations for the promotion of safety of life and property on and under the high seas and waters subject to [U.S.] jurisdiction.” “…maintain … readiness to function as a specialized service in the Navy in time of war.” 14 US Code, (2017), §2
NPPD	
FPS (and designated DHS employees)	**OIP**
“shall protect the buildings, grounds, and property that are owned, occupied or secured by the Federal Government … and the persons on the property.” 40 US Code, (2017), §1315(a).	“To access, receive, and analyze law enforcement information, intelligence information, and other information to “identify and assess the nature and scope of terrorist threats to the homeland; detect and identify threats of terrorism against the United States.” “To carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructure.” “To integrate relevant information, analysis, and vulnerability assessments to “identify priorities for protective and support measures regarding terrorist and other threats to homeland security.” “To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States.” 6 US Code, (2017), §121(d).
Source: **Author, created from identified sections of the US Code (2017), Title 6 (Domestic Security) and Title 14 (Coast Guard).**	

Table 2. DHS and DHS Entities with Critical Infrastructure Protection Missions

The DHS has broad and specific statutory authority for homeland security[16] and critical infrastructure protection. Both the DoD and DHS have missions for securing the homeland and its critical infrastructure and for supporting national policies.

National Security Policy to Protect Critical Infrastructure

As articulated in the CIPA, national security policy identifies critical infrastructure protection as vital:

> A continuous national effort is required to ensure the reliable provision of cyber and physical infrastructure services critical to maintaining the national defense, continuity of government, economic prosperity, and quality of life…
>
> It is the policy of the United States—(1) that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and

CIPA	PPD-21
Function or Sector	**Sector and Federal Agency Designated as Sector Specific Agency**
Telecommunications	Chemical: DHS
Energy	Commercial facilities: DHS
Financial services	Communications: DHS
Water	Critical manufacturing: DHS
Transportation	Dams: DHS
National defense	Defense industrial base: DOD
Government continuity	Emergency services: DHS
Economic prosperity	Energy: Department of Energy
Quality of life	Financial services: Department of Treasury
	Food-agriculture: Departments of Agriculture and Health & Human Services
	Government facilities: DHS, GSA
	Healthcare-public health: Department of Health & Human Services
	Information Technology: DHS
	Nuclear: DHS
	Transportation: DHS, DOT
	Water, wastewater: Environmental Protection Agency

***Source:* Author, created from information in the CIPA and PPD-21.**

Table 3. Critical Infrastructure Sector Designations in the CIPA and PPD-21

> government services, and national security of the United States; [and] (2) that actions necessary to achieve the policy stated in paragraph (1) be carried out in a public-private partnership involving corporate and non-governmental organizations….[17]

The CIPA defined critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[18] The CIPA relies upon "a public-private partnership" for acting to protect critical infrastructure.

Public-Private Sectors as Partners to Protect Critical Infrastructure

CIPA's framing of critical infrastructure protection as a shared action of infrastructure owners and government may not result in protected critical infrastructure. This sharing assumes reaching consensus on protection measures and implementation. Studies of some disaster and emergency scenarios cast doubt on this assumption, as discussed below. The ownership of U.S. critical infrastructure magnifies this doubt, since private entities, non-federal public entities (such as state and local governments or utilities), and non-federal public-private entities own much of the critical infrastructure. These studies demonstrate this tension and make recommendations to improve critical infrastructure protection. Two key tasks for protecting critical infrastructure emerge from these recommendations: establishing standards and ensuring compliance and physically protecting and securing the infrastructure.

Public-Private sectors partnership

The CIPA assumes that the private and public sectors would reach consensus and act in partnership. PPD-21 takes this assumption a step further by stating: "Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient."[19] The CIPA highlighted certain infrastructure sectors and functional areas as critical. PPD-21 subsequently defined sixteen critical infrastructure sectors and assigned federal agencies to each sector as the responsible, sector-specific agency to each. Table 3 summarizes these CIPA and PPD-21 designations:

Recent physical attacks on the electric grid and the 2010 Deepwater Horizon oil well failure and oil spill, among other examples, cast doubt on the assumption underlying the CIPA and PPD-21.[20] Since non-federal entities and some foreign entities own much of critical infrastructure, this doubt is important.[21] As an example, buildings owned by foreign entities, including China, house some highly-secure government agencies. A recent GAO report concluded that these leasing arrangements pose security risks for this infrastructure sector.[22] Two key facts call into question whether critical infrastructure protection is satisfactory: (1) continued critical infrastructure vulnerabilities and (2) privately-owned infrastructure being outside the government's control.[23] Reports of recent critical infrastructure damage demonstrate how to measure the ability of the federal government to ensure that critical infrastructure truly is protected.

Lessons from some post-9/11 disasters and emergencies

Some specific post-9/11 disasters and emergencies illustrate threats and damage to critical infrastructure regardless of whether the crisis was from natural or human causes or whether unintentional or intentional. Reports about the Northwest U.S.-Canadian electric grid failure (2003), Hurricane Katrina (2005), Deepwater Horizon oil well failure and oil spill (2010), and physical attacks on the Metcalf, CA, electric substation (2013–14) recommend critical infrastructure protection measures and provide examples of protection shortfalls and gaps.

Establishing Standards and Enforcing Compliance

Multiple reports studying specific emergencies recommend that the government establish specific standards and enforce compliance. The 2003 U.S.-Canada task force recommended that U.S. and Canadian government agencies establish and enforce compliance with reliability standards "in the planning, design, and operation of North America's vast bulk power systems."[24] More recent reports continue to echo the need for greater electric grid regulation.[25] The Deepwater Horizon commission specifically concluded that a lack of government standards contributed to the disaster.[26] The question then becomes how to set standards. The 2008 Electromagnetic Pulse (EMP) commission report succinctly stated the allocation of responsibility between industry and government and why the government must set standards:

> Industry is responsible for assuring system reliability, efficiency, and cost effectiveness as a matter of meeting required service levels to be paid for by its customers. Government is responsible for protecting the society and its infrastructure, including the electric power system. Only government can deal

> with barriers to attack — interdiction before consequence. Only government can set the standards necessary to provide the appropriate level of protection against catastrophic damage from EMP for the civilian sector.[27]

Two main points are the allocation of responsibility between industry and government and the independence of government from industry.

The government's independence from the infrastructure owner is crucial. Both the U.S.-Canada and the Deepwater Horizon commissions criticized the government for relying too much on industry, to the detriment of both the public and workers at infrastructure facilities. The Deepwater Horizon Commission candidly stated that the government regulatory agency "had a built-in financial incentive [from charging expensive licensing and permitting fees] to promote offshore drilling that was in tension with its mandate to ensure safe drilling and environmental protection." Having the government set standards and enforce compliance gives infrastructure owners a common, independent guide to address security concerns.[28]

Having the government set standards and enforce compliance gives infrastructure owners a common, independent guide to address security concerns.

Physically Protecting and Securing Critical Infrastructure

The electric grid attacks and the aftermath of Hurricane Katrina establish the need for routine physical security. The U.S. electric power grid, historically concerned with deterring vandalism, now is "most vulnerable to intentional damage from malicious acts" to shut down an infrastructure or perpetrate a terrorist act. Despite voluntary guidelines, grid owners failed or declined to implement available security measures even at critical high-voltage substations, as evidenced by substation attacks in California, Arkansas, and Arizona and results from North American Electric Reliability Corporation grid exercises in 2011 and 2013. A Congressional Research Service (CRS) report noted continuing efforts of the Federal Energy Regulatory Commission to implement its physical security policy for the power grid and recommended that Congress examine "whether company-specific security initiatives appropriately reflect the risk profiles of their particular assets, and whether additional security measures across the grid uniformly reflect terrorism risk from a national perspective."[29] On-going routine physical security of critical infrastructure is required.

In the aftermath of Hurricane Katrina, the collapse of law and order illustrates the need for emergency protection of critical infrastructure. The total collapse of local law enforcement led to uncontrolled violence and civil unrest. Hurricane Katrina destroyed local government capabilities and incapacitated and overwhelmed state government, leading to calls for assistance from higher jurisdictional levels. The federal government had trouble protecting and restoring critical infrastructures after Katrina. Eventually, federal forces were decisive in helping the state National Guard to restore order in New Orleans.[30]

Existing Federal Statutory Authority for the DHS

The DHS's NPPD, FEMA, and USCG have limited federal statutory authority to establish standards and to physically protect and secure critical infrastructure when the owner fails to adequately do so. The DHS has some regulatory authority for standard-setting for federal government property, areas under the jurisdiction of the USCG, and certain parts of the chemical sector. The only statutory authority to physically protect and secure critical infrastructure covers federal government property and certain USCG authorities. The DHS has challenges in effectively exercising its authorities to perform the identified key tasks, including a lack of regulatory authority to effect an integrated response to protect critical infrastructure, especially where an owner fails to protect critical infrastructure.

Establishing Standards and Enforcing Compliance

The CIPA and Homeland Security Act contain no new regulatory authority for critical infrastructure protection. The Homeland Security Act provides that the DHS has existing regulatory authority under three specified statutes and from authority previously granted to agencies transferred to the DHS.[31] Current regulatory authority for the DHS to establish standards and enforce compliance only addresses property owned or occupied by the federal government and persons on the property; U.S. ports, waters, and coastline; and certain parts of the chemical sector.

Federal government property and persons on the property

The DHS has regulatory authority that would extend to setting and enforcing standards over facilities owned or occupied by the federal government and persons on such property. The plain language of 40 US Code §1315(b) directs prescribing regulations necessary for the protection and administration of property owned or occupied by the Federal Government and persons on the property." The statutory text specifies "occupied," which includes property owned by any private and non-federal entity. The statute penalizes regulation violations with a fine, imprisonment, or both.

Current regulatory authority for the DHS to establish standards and enforce compliance only addresses property owned or occupied by the federal government and persons on the property...

U.S. ports, waters, and coastline

U.S. ports, waters, and the coastline are the jurisdiction of the USCG. The USCG has the regulatory authority to establish standards and enforce compliance both for security and for safety. The authority to regulate for safety provides additional authority to the extent that safety issues also compromise security. The USCG can implement statutes related to port and maritime transportation security and to transportation and commercial shipping.[32] Second, statutory authority exists for regulation of vessels in U.S. territorial waters when either the president declares a national emergency or the U.S. Attorney General determines that an actual or anticipated mass migration of aliens en route to the U.S. requires an immediate federal response.[33] Further, the USCG may regulate to promote safety of life and property using two statutes. It seems reasonable that safety would encompass security since security affects safety of life and property. The first safety statute directs that the USCG "shall … promulgate and enforce regulations for the promotion of safety of life and property on and under the high seas and waters subject to the jurisdiction of the U.S., covering all matters not specifically delegated by law to some other executive department."[34] The second safety statute grants the USCG regulatory authority over vessels, including vessel "design, construction, alteration, repair and operation" and "the use of vessel stores and other supplies of a dangerous nature."[35] Finally, the USCG has regulatory authority for hazardous materials in commerce which also authorizes regulations related to transportation and pipelines.[36]

Chemical sector

Two laws amending the Homeland Security Act authorize the DHS to establish standards and to enforce compliance related to parts of the chemical sector. First, the Chemical Facilities Anti-Terrorist Standards (CFATS) Program regulates any facility that holds any specified chemical in a quantity at or above the minimum quantity for the chemical specified in the regulation. The statute directs the Secretary to "establish risk-based performance standards designed to address high levels of security risk at covered chemical facilities." The statute permits enforcement by civil enforcement and by emergency order in certain circumstances.[37] Second, the Secure Handling of Ammonium Nitrate statute grants regulatory authority for the "sale and transfer of ammonium nitrate" to "prevent the misappropriation or use of ammonium nitrate in an act of terrorism."[38] The statute focuses on registration and recording of transactions involving ammonium nitrate and does not mention physical security of facilities.

Physically Protecting and Securing Critical Infrastructure

The only sectors for which the Act authorizes the DHS to physically protect and secure critical infrastructure are: (1) federal government property and persons on such property, and (2) U.S. ports, waters, and coastline. Neither the authority granted to the OIP nor to the FEMA include physically protecting and securing critical infrastructure if the owner fails to adequately do so.

Federal government property and persons on the property

Statutory law mandates that the DHS "shall protect the buildings, grounds, and property that are owned, occupied, or secured by the Federal Government (including any agency, instrumentality, or wholly owned or mixed-ownership corporation thereof) and the persons on the property." The statute specifies that the DHS may designate employees of the DHS, including FPS personnel, for this purpose.[39]

U.S. ports, waters, and coastline

The statutory authority for the USCG does not mention specifically the physical protection of critical infrastructure so the analysis must rely upon reasonable inferences. The USCG has broad statutory authority to assist "any Federal agency, State, Territory, possession, or political subdivision thereof, or the District of Columbia, to perform any activity for which such personnel and facilities are especially qualified."[40] This statute requires a request for assistance from the proper authority as a precondition to action. This broad authority would include physically protecting and securing critical infrastructure either routinely or in an emergency, since the USCG has training and equipment for defense. The USCG has broad authority to routinely enforce laws related to U.S. ports, waters, and coastline, including maritime shipping and transportation. The USCG enforces laws, conducts maritime air surveillance, and makes "inquiries, examinations, inspections, searches, seizures, and arrests upon the high seas and waters over which the United States has jurisdiction, for the prevention, detection, and suppression of violations of US laws."[41] This authority enables the USCG, as part of its routine mission, to protect critical infrastructure to the extent laws prohibit behavior affecting security (as opposed, for example, to collecting revenue or policing for safety hazards). At certain specific times, statutory authority empowers USCG action that could include protecting and securing critical infrastructure. The USCG protects waterways and enforces regulations for anchorage and movement of vessels when the president declares a national emergency or when the U.S. Attorney General "determines that an actual or anticipated mass migration of aliens en route to, or arriving off the coast of, the United States" requires an immediate federal response.[42] Finally, the USCG is a military service that maintains readiness for war and that operates as part of the U.S. Navy when designated.[43] These authorities, while not specifically delineating critical infrastructure protection, enable the USCG to protect and secure critical infrastructure related to maritime transportation and related commercial facilities and shipping and other critical infrastructure when requested by the proper authority.

Challenges for the DHS in Exercising this Statutory Authority

Federal government property and persons on the property

In comparing two provisions of 40 US Code §1315, the statutory text differs. This difference could affect the regulatory scope since what is defined as subject to protection is greater than what is defined as subject to regulation. (See Table 4)

U.S. ports, waters, and coastline

The USCG's broad statutory authority to regulate for defense and law enforcement and to protect U.S. ports, waters, and coastline does not explicitly specify protecting critical infrastructure when an owner fails to adequately do so. Also, some of its authority can be exercised only in times of emergency or war or upon specific request. Finally, the broad authority in 6 US Code §141 is unclear as to whether it is limited to areas traditionally in the USCG jurisdiction (high seas and U.S. ports, waters, and coastline) or is broader. The USCG, as a military service, faces the confusion surrounding the doctrine of *posse comitatus* and laws limiting its use. For centuries, this doctrine permitted local sheriffs to assemble help in enforcing the law and restoring order. *Posse comitatus* is Latin for "power of the county" or "the force of the county." The practice dates to English law as early as 1411 and continued to be used throughout American history. In 1878, Southern Democrats angry about Reconstruction policies gained Congressional control. They enacted what became known as the *Posse Comitatus* Act which criminalized using the Army or Air Force to execute laws unless expressly permitted by the Constitution or statute. That act now is 18 US Code §1385, which causes much confusion among military services regarding its application.[44] Subsequently, 10 US Code §275 restricts members of the Navy from "direct participation … in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law."[45] The plain text of 10 US Code §275 is silent about whether it includes the USCG when it operates as part of the Navy.[46] Further, the more recent Homeland Security Act reaffirms "the continued importance of [18 US Code §1385] … in [restricting] any use of the Armed Forces as a posse comitatus to execute the laws."[47] This provision's broader use of "Armed Forces," rather than 18 US Code §1385's "the Army or

Protection authority	Regulatory authority
mandates protection of "the ***buildings***, *grounds*, and property that are owned, occupied, or ***secured***" by the federal government and "persons on the property." 40 US Code, (2017), §1315(a).	"may prescribe regulations necessary for the protection and administration of property owned or occupied" by the federal government and "persons on the property…" 40 US Code, (2017), §1315(c).
Source: **Author created. Emphasis added by underlining and by bolding/italicizing the text in (a) that is not in (c); the difference represents a gap in defined authority to protect and to regulate.**	

Table 4. Comparison of 40 US Code §1315(a) and (c).

the Air Force," further adds to the confusion for the USCG, since 14 US Code §1 defines the USCG as "a military service and a branch of the armed forces of the United States at all times." As previously detailed, the USCG is responsible for law enforcement and assisting in law enforcement. Additionally, one statute specifically authorizes the USCG to assist "any Federal agency, State, Territory, possession, or political subdivision thereof, or the District of Columbia, to perform any activity for which such personnel and facilities are especially qualified" when requested by the proper authority.[48] Thus, it seems logical that the USCG is exempted from the limits on the use of posse comitatus and on the military for direct participation in law enforcement. Otherwise, many statutorily authorized and mandated USCG missions are defeated.

The plain text of the statutes could cause confusion, especially in a crisis or multi-faceted, evolving operation. In at least one documented instance, a USCG judge advocate general believed the USCG violated the posse comitatus prohibition when called upon to assist in the DC sniper hunt that terrorized the metropolitan area of the nation's capital for months and resulted in multiple deaths.[49]

The Homeland Security Act offers limited authority for the DHS to establish protective standards or to physically protect and secure critical infrastructure where an owner fails to adequately protect it.

Chemical sector

The statutory authority for the CFATS Program expires in December 2018 unless reauthorized by law.[50] Also, it only covers establishing performance standards. One report questioned whether the program should augment its performance-based approach with prescriptive regulations.[51] Finally, the program, while making great strides in improving the security of chemical facilities, has problems with non-compliant facilities.[52] In the plant explosion in West, TX, in 2013, the facility failed to report its ammonium nitrate holdings to the CFATS Program. The final report investigating the explosion noted that if the facility "had complied with the CFATS [Program], a CFATS [Program] inspection or assistance visit might have noted the storage conditions … and prompted change."[53]

The Homeland Security Act offers limited authority for the DHS to establish protective standards or to physically protect and secure critical infrastructure where an owner fails to adequately protect it. For example, the GAO acknowledged the DHS has no authority to set standards for the electrical grid which affects every other critical infrastructure sector.[54] USCG authority related to critical infrastructure is not explicit and is limited in some areas to emergency or wartime. Also, the question of the *posse comitatus* limitation could cloud USCG operational effectiveness.

The DHS can exercise its statutory authority to influence the infrastructure owners and other government agencies with regulatory authority over infrastructure security;[55] to exercise its limited areas of regulatory and statutory authority to protect government property and ports, waters, and coastline; and to exercise its defined regulatory authority over certain chemical facilities and certain ammonium nitrate transactions. The DHS, however, has no statutory authority for strategic, integrated regulation of minimal standards or of physically protecting critical infrastructure where an owner fails to implement protective measures or inadequately protects the infrastructure.

Existing Federal Statutory Authority for the DoD

The DoD has no regulatory authority relevant to critical infrastructure protection. Its federal statutory authority for physical protection and security is limited. Title 32 authorizes the DoD to fund National Guard protection of critical infrastructure. Multiple authorities authorize the DoD, under specific, statutorily-defined circumstances, to act in support of civilian authorities. Like the DHS, the DoD has challenges in exercising its authority which could leave critical infrastructure unprotected and vulnerable, thereby compromising the DoD's ability to fulfill this national security goal.

The DoD has no statutory authority to establish standards to guide critical infrastructure protection. The authority for the DoD to physically protect and secure critical infrastructure either routinely or in an emergency derives from Titles 32, 10, 14, and 42. Title 32 provides the clearest authority by permitting DoD funding for the National Guard to perform homeland defense duties, specifically including critical infrastructure protection. Title 10 authorizes use of military forces for specific situations to restore law and order, to enforce federal authority, and to enforce federal and state law, including assisting the Department of Justice (DOJ). Title 14 USCG personnel are available. Finally, the DoD may assist in emergency situations if the president invokes Title 42 for disaster/emergency assistance.

National Guard, Title 32

The most explicit statutory authority is Title 32 funding authority for "homeland defense activity," which includes military protection of critical infrastructure. The DoD may fund state National Guard forces to perform "the military protection … of infrastructure or other assets of the United States determined by the Secretary of Defense as being critical to national security, from a threat or [an] aggression."[56] This authority would address routine and emergency protection and security.

Armed Forces and National Guard, Title 10

In addition, physically protecting and securing critical infrastructure could be part of restoring law and order, enforcing federal authority, or enforcing federal or state law.

One statute authorizes the President, upon request of the state's legislature or governor if the legislature cannot be convened, to call into federal service the militia of another state and "use such of the armed forces, as [the President] considers necessary to suppress the insurrection."[57]

The DoD has no statutory authority to establish standards to guide critical infrastructure protection.

Another statute authorizes the president to use militia of any state to enforce U.S. law or suppress rebellion where "unlawful obstructions, combinations, or assemblages, or rebellion against the authority of the United States, make it impractical to enforce the laws of the United States in any State by the ordinary course of judicial proceedings…."[58]

A third statute authorizes the President "by using the militia or the armed forces, or both, or by any other means shall take such measures as [the president] considers necessary to suppress, in a State, any insurrection, domestic violence, unlawful combination, or conspiracy." This statute applies where (1) violence or unlawful activity hinders the execution of state law or federal law within the state and deprives people of a "right, privilege, immunity, or protection named in the Constitution and secured by law" and (2) the state authorities "are unable, fail, or refuse" protection or the disturbance "opposes or obstructs the execution of federal law or impedes the course of justice under those laws."[59]

Finally, Reserve forces may be activated upon war, national emergency, national security requirements, and National Guard forces may be activated upon actual or danger of invasion or rebellion against U.S. authority and to execute U.S. law when the president "is unable with the regular force to execute the laws of the United States."[60] The president could order critical infrastructure to be physically protected and secured as a necessary action pursuant to these statutes.

...the President has authority in a natural disaster or an emergency to deploy any federal agency...

Also, the DoD has statutory authority to support DOJ activities to enforce laws related to bombings, biological and chemical weapons, and weapons of mass destruction (WMDs). The statute related to bombings authorizes the DoD to support the DOJ in enforcing the law that prohibits bombings of infrastructure facilities, public transportation systems, state or government facilities, and places of public use. The action must be necessary for "the immediate protection of human life and civilian law enforcement officials are not capable of taking the action."[61] The statutes related to biological and chemical weapons and WMDs authorize the DoD to assist the DOJ in emergency situations in enforcing laws that prohibit WMD.[62] Both statutes require the Attorney General to request DoD assistance and are limited to emergency situations. Physically protecting and securing critical infrastructure are not mentioned specifically in either statute.

Coast Guard, Title 14

The USCG at all times is a military service. It serves the DHS, except when it operates as a service to the U.S. Navy either upon a Congressional declaration of war or when the president directs.[63]

Disaster relief and emergency assistance, Title 42

Finally, the President has authority in a natural disaster or an emergency to deploy any federal agency, both with and without the request of a state governor. This authority could include directing the DoD to physically protect and secure critical infrastructure.

A state governor may request assistance in a major disaster or emergency.[64] The President may direct federal support of state and local assistance response or recovery efforts.[65] The President also may act without a request from the governor in a major disaster or emergency "where necessary to save lives, prevent human suffering, or mitigate severe damage"; where action is "essential to meeting immediate threats to life and property"; where it is necessary to provide emergency communication systems or emergency public transportation or fire management assistance; and where the federal government has primary responsibility for response because under the Constitution or federal statutory law the federal government exercises exclusive or preeminent responsibility and authority over the subject area.[66] It is reasonable to conclude that the President would deem physically protecting and securing critical infrastructure as mitigating severe damage or essential to meeting a threat to life or property.

Challenges for the DoD in Exercising This Statutory Authority

Whether Title 32, 10, 14, or 42 is invoked, or a combination thereof, the DoD has multiple challenges in unequivocally exercising its authority. These challenges could compromise the orderly and predictable physical protection and security of critical infrastructure.

National Guard, Title 32

First, the Title 32 statutory framework assumes that the state governor and the DoD will agree on the mission, threat assessment, and scope. It also assumes that the state governor will agree with the amount of DoD funding and proceed with the mission.[67] A second assumption is that the state National Guard has the capability and personnel available for the homeland defense activity identified by the DoD or requested by the governor, especially considering the duty is limited to one hundred and eighty days.[68] Finally, this authority requires the DoD to engage in additional recordkeeping, auditing, and compliance monitoring.[69]

Armed Forces and National Guard, Title 10

The most confusing challenge to exercising Title 10 authority may be the limitations placed upon the *posse comitatus* doctrine. Some Title 10 statutes specifically authorize military support to law enforcement related to WMD and bombings. Similar to the initial confusion on 9/11 as to the "cause" of the disaster/emergency/crisis, a circumstance may require military support even before determining whether the triggering event was a WMD or a bombing.[70] Further, some statutes have specific exceptions, such as "for the immediate protection of human life, and civilian law enforcement officials are not capable of taking the action."[71]

State National Guard units, except ones that are federalized, and the USCG, possibly except when operating as part of the Navy, are exempt from the bar against *posse comitatus* activity.[72] This situation may lead to not federalizing National Guard units to avoid the confusion at times when they need to be federalized for operational effectiveness. The military has multiple branches and engages in joint planning, training, and operations, including with the National Guard and the USCG. Navigating the statutory authorizations, prohibitions, limitations, and exceptions related to *posse comitatus* is like a maze.[73]

Coast Guard, Title 14

The USCG is a hybrid force: a military service and branch of the armed forces, as well as a law enforcement authority. As discussed previously, interpreting and applying posse comitatus limitations to the USCG presents a challenge, especially when the USCG may be transferred to the U.S. Navy where its operations may be changed to synchronize with Navy operations.[74]

Navigating the statutory authorizations, prohibitions, limitations, and exceptions related to *posse comitatus* is like a maze.

Disaster Relief and Emergency Assistance, Title 42

The statutory framework for disaster response and emergency assistance and recovery has at least two challenges. A most daunting challenge involves the dual-command problem where National Guard forces have a separate command chain than federal forces, including federalized National Guard forces, military active duty forces, and federal disaster response and law enforcement personnel, as illustrated by Figure 1 (page 20).

The governor of a state may mitigate the parallel command challenge by agreeing to appointment of a dual-status commander, as illustrated in Figure 2 (page 21). However, nothing in federal law requires the governor to agree to the appointment of a dual-status commander. In addition, arbitrary distinctions as to the cause of the emergency drive the types of action: (1) between "major disaster" and "emergency" and (2) between actions authorized after a governor requests assistance and actions authorized based upon a presidential

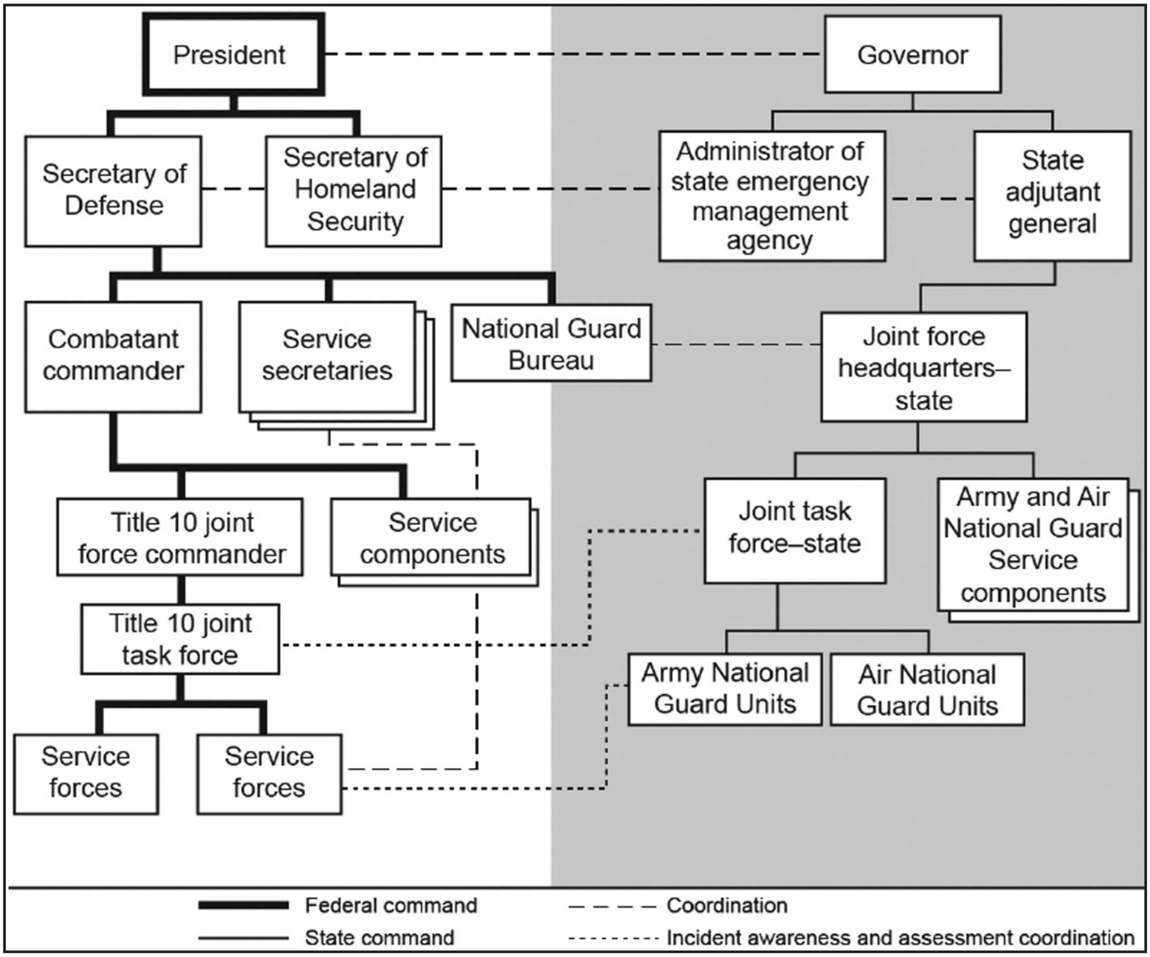

President
Governor
Secretary of Defense
Secretary of Homeland Security
Administrator of state emergency management agency
State adjutant general
Combatant commander
Service secretaries
National Guard Bureau
Joint force headquarters–state
Title 10 joint force commander
Service components
Joint task force–state
Army and Air National Guard Service components
Title 10 joint task force
Army National Guard Units
Air National Guard Units
Service forces
Service forces
Federal command
State command
Coordination
Incident awareness and assessment coordination

Figure 1. Dual/Parallel Command Structure with Federalized State National Guard.
Source: **U.S. DoD, Department of the Army, Headquarters, ADRP 3-28, Defense Support of Civil Authorities, p. 3-9 (Figure 3-5. Example of parallel command structure).**

determination. It seems that a catastrophe is an emergency regardless of whether caused by a brutal hurricane, raging fire, devastating explosion triggered by human error or an explosion or bomb detonated by a criminal or terrorist, or a nuclear or EMP attack. For example, if a governor requests assistance, the disaster relief assistance includes "precautionary evacuations and recovery" and "recovery activities, including disaster impact assessments and planning." However, emergency assistance without a governor's request does not include these actions.[75] An emergency response may require some precautionary evacuations (for example, clearing a bomb site or suspected bomb site locale) and recovery efforts. These statutorily-defined and overlapping categories, that seem arbitrary, may unnecessarily complicate operationalizing crisis planning and response, especially in joint environments and in major crises (the very ones that require swift, decisive response).[76]

No statutory authority authorizes the DoD to regulate to set standards for critical infrastructure protection. That lack of authority is appropriate for our civilian government, so that a purely civilian department exercises regulatory authority in such matters. The DoD has statutory authority which would encompass physically protecting and securing critical

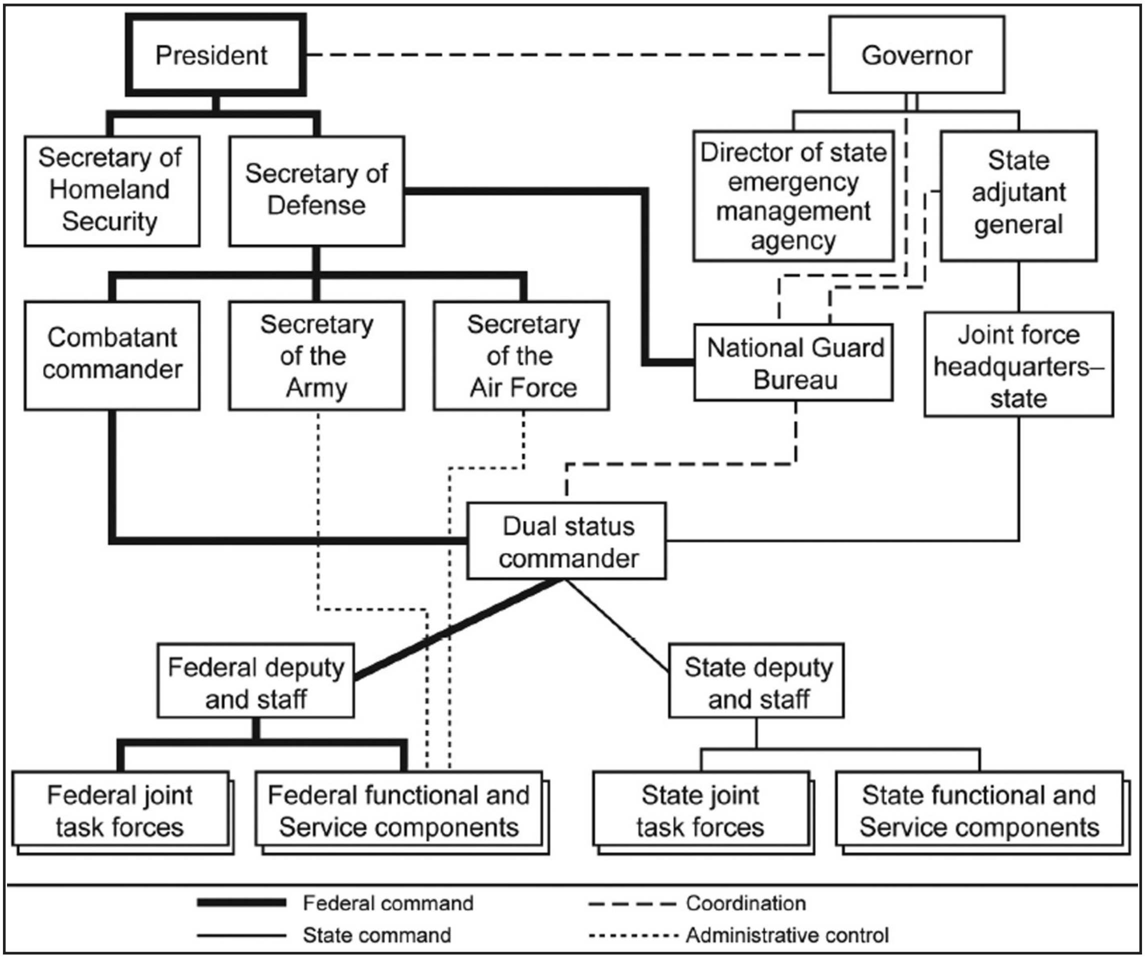


Figure 2. Dual Status Command Solution with Federalized State National Guard.
Source: **U.S. DoD, Department of the Army, Headquarters, ADRP 3-28, Defense Support of Civil Authorities, p. 3-10 (Figure 3-6. Example of dual-status command structure).**

infrastructure if an owner does not adequately do so. This authority applies only in certain circumstances. Challenges in exercising these authorities could exacerbate crisis response and could compromise the DoD's ability to perform this task as effectively as needed.

Implications for National Security and Critical Infrastructure Protection

Three conclusions are evident from the analysis of this survey of federal statutory law, including where an owner fails to adequately protect the infrastructure. These conclusions identify ways in which the federal statutory framework offers insufficient authority for the DHS or the DoD, acting separately or jointly, to achieve the national security goal of protecting critical infrastructure. This analysis demonstrates the need to strategically review previous policy assumptions about the public-private partnership model where the private sector implements action to yield protected critical infrastructure. In addition, two specific areas may be addressed by targeted statutory action to address the confusion around the *posse comitatus* doctrine and to remedy the dual-command problem. U.S. policy has long favored an integrated national security policy. It appears that critical infrastructure protection, even from this brief, targeted survey, is anything but integrated.

Strategic Analysis and Policy Considerations

Three conclusions are relevant to national strategic policy for protection of critical infrastructure, including as owned by private and non-federal government entities that fail to adequately protect it: (1) the DHS regulatory authority to set standards is very limited and the DHS has no integrated, strategic authority to set even minimal standards for critical infrastructure protection, even where another agency has no relevant authority or does not exercise its authority; (2) the DHS and the DoD federal statutory authority to physically protect and secure critical infrastructure routinely and in an emergency is limited and lacks integration; and (3) no statute defines how the DHS and the DoD are to work together to achieve the national security goal of critical infrastructure protection, even in an emergency or a crisis.

Neither [DHS or DoD] has federal statutory authority for an integrated plan or response to critical infrastructure protection.

Strategic Review for Integrated National Security and Critical Infrastructure Protection

These deficiencies and others suggested by this article present the need for a strategic review to integrate national security and critical infrastructure protection policy. The U.S. previously has moved to integrate national security policy. In 1947, Congress articulated the need for integrated, comprehensive, and strategic U.S. security; unified direction, authority, and control under civilian control; "more effective, efficient, and economical administration"; and elimination of "unnecessary duplication … particularly in the field of research and engineering."[77] The 1947 National Security Act consolidated the military and defense services into the DoD. In 1986, Congress reorganized and streamlined the DoD to establish clear authority, responsibility, and chain of command; to achieve integration and synthesis of the various capabilities of the military services; "to improve the military advice provided to the President"; "to increase attention to the formulation of strategy and to contingency planning"; and "to provide for more efficient use of defense resources."[78]

Today, the DHS has the homeland security mission to protect the nation from terrorism and to respond to disasters and emergencies, and the DoD has the homeland defense mission, terrorism fight, support for disasters and emergencies, and support to civilian law enforcement agencies. Neither department has federal statutory authority for an integrated plan or response to critical infrastructure protection. For example, neither department can effectuate a solution, such as for electric grid owners who fail to adopt available security measures or chemical facility owners who fail to avail themselves of available resources that may have prevented deadly and costly infrastructure catastrophes.[79] The DHS statutory authority authorizes studying, assessing, sharing information, and reporting to stakeholders and Congress about critical infrastructure protection needs and mandates building a national asset database.[80] A strategic review could work to resolve the limits to the DHS regulatory authority to set minimal standards for critical infrastructure protection as a guide so that owners who are not protecting infrastructure at least would be required to meet some minimal threshold. This measure is especially important for integrated and regional or nationwide critical infrastructure, such as the electric grid and emergency services, and especially where no federal agency has regulatory authority for security or does not exercise its authority. Also, a strategic review could address gaps in the ability of the DHS and/or the DoD to physically secure critical infrastructure where an owner fails to adequately do so. Finally, a strategic review could define how the DHS and the DoD work together, especially in a crisis, which would facilitate joint training and exercises.[81]

The limited authority of the DHS contrasts starkly with its broad statutory mission with grave national consequences to "prevent terrorist attacks," "reduce the vulnerability … to terrorism," and "minimize the damage … from terrorist attacks that do occur" within the U.S., and to protect critical infrastructure.[82] Yet the policy assumption in the CIPA and PPD-21 rests upon non-federal infrastructure owners acting in partnership with the federal government. As aptly noted with respect to the electric grid, the interconnected, networked nature of critical infrastructure that crosses over state and local jurisdictions may make this public-private partnership model—as the only framework—unrealistic for national security.[83] Second, the diffusion of regulatory authority among discrete DHS entities and among multiple federal departments and agencies hobbles an integrated approach. The DHS has no regulatory authority to set minimal national standards, to compel agencies with regulatory authority to issue protection standards, or to act in that agency's stead. Further, the DHS has no authority to compel that information be provided and updated for the national asset database and prioritized critical infrastructure list required by the Homeland Security Act.[84]

Physical protection is crucial with widespread disasters or in the face of credible threats of coordinated terrorist action against key critical infrastructure, such as water and dams or the electric grid. If state and local law enforcement authorities are overwhelmed or lack the capacity to physically protect and secure the infrastructure, the DHS and the DoD statutory framework must be clear as to authority and responsibilities, including unified command authority.[85]

How to accomplish a strategic review? Consider forming a commission to analyze and recommend strategic policy and tactical implementation options for protecting critical infrastructure, including how to address the reality of non-federal infrastructure owners who fail to adequately protect critical infrastructure. Primary considerations should be the representativeness and legitimacy of the commission. Members should be representative of the relevant issues and diverse in views with no vested interest, other than as dedicated, concerned Americans. Examples of members could include: retired members of the public, including state and local government officials; non-government entities; private owners; first responders; concerned citizens; retired members of the U.S. Congress, courts, military services, and federal government departments; and a limited number of retired military service members, including general and field officers and enlisted members. Champion legitimacy by having the fact-deciders and recommenders not have a profit, promotion, or reelection stake in the data collection, analysis, or recommendations. A second consideration is building or creating the political will to tackle the issues and recommendations rather than defaulting to the *status quo*. Congress must be committed to act on reasoned recommendations to secure our nation's critical infrastructure, rather than reacting to the next crisis.

Congress must be committed to act on reasoned recommendations to secure our nation's critical infrastructure, rather than reacting to the next crisis.

In the nearer term, two specific challenges could be addressed by new statutory law:

- *Posse comitatus* and criminal penalties. The doctrine of posse comitatus and attempts to limit it have created confusion and clouded the military's effective response to domestic emergencies, including in Katrina in 2005 and in the Los Angeles riots in 1992.[86] One of the reports from Katrina recommended revisiting this issue.[87] The statute enacted in a 2006 post-Katrina response was repealed shortly thereafter upon complaints from the Council of Governors about inadequate consultation.[88] The Katrina recommendation, therefore, remains unaddressed. More recent authors also have called for revisiting this issue.[89] The original 1878 Posse Comitatus Act, currently in 18 US Code §1385, should be repealed. The original 1878 Posse Comitatus Act, enacted to thwart federal post-Civil War reconstruction and integration efforts, was moved to the U.S. criminal code in 1956.[90] It is an unnecessary remedy that has stifled responses in the past, and that could stifle or chill authorized action in a crisis. The confusion could create cascading delays, for example, in light of more recent statutory law that specifically authorizes military support of law enforcement and in the hybrid nature of the USCG. The strategic review of national security policy then could address overarching policy considerations as to the authorized use of the military in the homeland. The strategic review also could consider whether any streamlining and clarity of statutory law is necessary or would be helpful to clarify the various statutes that bar the military from direct participation in law enforcement "unless otherwise authorized by law."[91]

- Dual-command problem and the need for unified command. The provision of federal assistance could be conditioned upon using the dual-status command model. Such a construct provides input from a state directly into the chain of command, while also preserving operational fidelity and the President's constitutional command authority over the U.S. military.

Conclusion

Conducting a strategic review is a much-needed opportunity to examine national security policy and critical infrastructure protection, as well as embedded policies about the functions of homeland security, homeland defense, and disaster/emergency preparedness and response. The Constitution is clear about the exclusive and preeminent authority and responsibility for national security and national defense being the province of the federal government where Congress is:

> … [to] provide for the common Defence and general Welfare of the United States;
>
> ... to provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions;
>
> … to provide for organizing, arming, and disciplining, the Militia, and for governing such Part of them as may be employed in the Service of the United States, reserving to the States respectively, the Appointment of the Officers, and the Authority of training the Militia according to the discipline prescribed by Congress.[92]

When the U.S. calls forth the militia (now the National Guard) to execute the laws of the Union, the militia should be in the service of the U.S.[93] In addition, the regular U.S. military forces (non-National Guard) are authorized by statutory law to act domestically in certain circumstances.[94] These circumstances can include physically protecting and securing critical infrastructure.

Americans in an emergency may not care so much about the color of the uniform the person is wearing when he or she protects a nearby major dam or electrical grid component or plucks them from the rooftops of their hopelessly flooded neighborhoods, secures them against wanton opportunistic or criminal violence, delivers life-saving clean water and emergency food, or takes them to a secure shelter. For all of the separate and overlapping statutes and policy discussions, it may not matter whether the person's uniform is the green, blue, tan, or white of the U.S. military or black, blue, green, gray, tan, red, or yellow of state or local law enforcement or emergency responders and whether the securer, defender, or responder acts under authority for homeland security, homeland defense, critical infrastructure protection, disaster/emergency assistance, and/or law enforcement. What likely matters is whether the nation is secure and defended; the individual is secure and safe; the government responds effectively, promptly, and affordably; and our civilian, representative government continues to operate to implement the Constitution and provide for the common defense.

A strategic review of national security policy and delivery of homeland security and defense services could promote integrated critical infrastructure protection, a defined national security goal. A strategic review, followed by statutory authorization, could take critical infrastructure protection beyond the stages of assess, study, inform, and report to a new stage of systematically and predictably implementing reasonable and necessary protective measures. These protective measures may include how to handle owners who do not adequately protect their critical infrastructure and how the DHS and the DoD will work together, especially in a crisis where it may be necessary to deploy American military forces on American soil to defend it, to restore order, to enforce federal authority, to enforce federal or state law, or a combination thereof. ***IAJ***

NOTES

[1] "Critical Infrastructures Protection Act of 2001," Public Law 107-56, 115 Stat 400, October 26, 2001, codified at 42 US Code, §5195c, <http://uscode.house.gov/browse.xhtml>, accessed on March 21, 2017.*

[2] "Homeland Security Act of 2002," Public Law 107-296, 116 Stat 2135, codified at 6 US Code, 2017, §§101 et seq., <http://uscode.house.gov/browse.xhtml>, accessed on March 21, 2017.

[3] ICF International, *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*, June 2016, pp. 88 and 91, <https://energy.gov/epsa/downloads /electric-grid-security-and-resilience-establishing-baseline-adversarial-threats>, accessed on March 22, 2017; James K. Hayes and Charles K. Ebinger, "The Private Sector and the Role of Risk and Responsibility in Securing the Nation's Infrastructure," *Journal of Homeland Security and Emergency Management*, Vol. 18, No. 1, March 2011, p. 2, <https://www.brookings.edu/wp-content/uploads/2016/06/04_critical _infrastructure_ebinger.pdf>, accessed on April 2, 2017.

[4] "Critical Infrastructures Protection Act of 2001," 42 US Code §5195c(e).

[5] "Homeland Security Act of 2002," 6 US Code §456; William C. Banks and Stephen Dycus, *Soldiers on the Home Front: The Domestic Role of the American Military*, Harvard University Press, Cambridge, 2016, p. 11; Shawn Reese, *Defining Homeland Security: Analysis and Congressional Considerations*, U.S. Congressional Research Service (CRS) report to Congress, Washington, DC, January 8, 2013, Summary,

<https://fas.org/sgp/crs/homesec /R42462.pdf>, accessed on April 2, 2017. This CRS report concludes that the U.S. government does not have a single definition for "homeland security," which may impede the development of a coherent national homeland security strategy and "may hamper the effectiveness of Congressional oversight."

6 Chris Currie, "Critical Infrastructure Protection: DHS Has Made Progress in Enhancing Critical Infrastructure Assessments, but Additional Improvements are Needed," testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives, GAO-15-692T, Washington, DC, July 12, 2016, <http://docs.house.gov/meetings/HM/HM08/20160712 /105169/HH"RG-114-HM08-Wstate-CurrieC-20160712.pdf>, accessed on April 2, 2017; Richard Campbell, *Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?*, written testimony before U.S. Congress, U.S. Government Printing Office, Washington, DC, April 2016, quoted in hearing before the Committee on Transportation and Infrastructure, 114th Cong., 2d sess., April 14, 2016, p. 65, <https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg99931/pdf/CHRG-114hhrg99931.pdf>, accessed on January 16, 2017; Ben Brinkman, et al., *Regulation of Physical Security for the Electric Distribution System*, California Public Utilities Commission, February 2015, pp. 3, 6, and 13, <https://pdfs.semanticscholar.org/e11b /21010c0fa 8e68d0958496bc3564c50524c63.pdf,> accessed on March 22, 2017; Thomas F. McLarty III and Thomas J. Ridge, *Securing the U.S. Electrical Grid: Understanding the Threats to the Most Critical of Critical Infrastructure, While Securing a Changing Grid*, Center for the Study of the Presidency and Congress (CSPC), Washington, DC, October 2014, <https://www.thepresidency.org/sites/default/files /Final%20 Grid%20Report_0.pdf>, accessed on January 5, 2017.

7 Caitlin Durkovich, NPPD Office of Infrastructure Protection Assistant Secretary and Andy Ozment, NPPD Office of Cybersecurity and Communications Assistant Secretary for a House Committee on Homeland Security, *"Value of DHS" Vulnerability Assessments in Protecting Our Nation's Critical Infrastructure*, written testimony of and subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies Hearing, Washington, DC, July 12, 2016, <https://www.dhs.gov/news/2016/07/12 /written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity>, accessed on April 2, 2017; *The 2014 Quadrennial Homeland Security Review*, U.S. Department of Homeland Security, Washington, DC, June 18, 2014, <www.dhs.gov /sites/default/files/publications/qhsr/2014-QHSR.pdf>, accessed on April 2, 2017.

8 Some thought-provoking articles relevant to issues in homeland security and defense that question the effectiveness of the status quo include: Steven Brill, "Is America Any Safer? 15 Years after 9/11," *The Atlantic*, September 2016, <http://www.theatlantic.com /magazine/archive/2016/09/are-we-any-safer/492761/>, accessed on April 4, 2017. Brill argues that much progress has been made in homeland security, but gaps remain; Barry Friedman, "We Spend $100 Billion on Policing. We have No Idea What Works. Police Are More Likely to Adopt New Technology Because Another Department Has It Than Because of Reasoned Cost-Benefit Analysis," *The Washington Post*, March 10, 2017, <https://www.washingtonpost.com/posteverything/wp/2017/03/10/we-spend-100-billion-on-policing-we-have-no-idea-what-works /?hpid=hp_no-name_opinion-card-b%3Ahomepage%2Fstory&utm_term= .e3f11d7fbd8c>, accessed on March 12, 2017. Friedman discusses the increasing cost of policing, including weapons and other systems, and questions the effectiveness of expensive new technology; Douglas Heaven, "The Uncertain Future of Democracy," BBC, March 30, 2017, http://www.bbc.com/future /story/20170330-the-uncertain-future-of-democracy>, accessed on March 30, 2017. Heaven discusses trends in democratic countries, including alarming moves in some countries toward the certainty and security offered by authoritarianism.

9 U.S. Constitution, Preamble; Article 1, Section 8; Article. 4, Section. 4. The Constitution states that the federal government is: "[to] provide for the common Defence and general Welfare of the United States"; "to provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions"; "to [guarantee] every State … a Republican Form of Government, and [to] protect … against Invasion and … against domestic Violence" [upon request of the state]; Banks and Dycus, pp. 43–46;

Stephen I. Vladeck, "Emergency Power and the Militia Acts," *Yale Law Journal*, Vol. 114, 2004, pp. 149–194, <http://www.yalelawjournal.org /pdf/427_pa9skxwv.pdf,> accessed on February 20, 2017. These sources provide a history of federal statutes authorizing the use of military force on the home front, enacted shortly after ratification of the Constitution and continuing to more modern times. "Critical Infrastructures Protection Act of 2001," 42 US Code §5195(c)(2); "Homeland Security Act of 2002," 6 US Code §121(d). These two statutes set forth national policy related to critical infrastructure protection and the public-private partnership. Thomson Reuters, *Guide to Homeland Security*, Thomson Reuters, Eagan, MN, 2016, pp. 1–5. This source gives background on the DHS.

10 "The National Security Act of 1947," Public Law 114-328, 61 Stat 496, July 26, 1947, codified at 50 US Code §3002, Chapter 343.

11 Joint Chiefs of Staff, Joint Publication 3-27*, Homeland Defense*, U.S. Department of Defense, Washington, DC, July 29, 2013, <http://www.dtic.mil/doctrine /new_pubs/jp3_27.pdf>, accessed on March 23, 2017; Joint Chiefs of Staff, Joint Publication 3-28*, Defense Support of Civil Authorities*, U.S. Department of Defense, Washington, DC, July 2012, June 2013, July 31, 2013, <http://dtic.mil/doctrine / new_pubs/jp3_28.pdf>, accessed on March 23, 2017.

12 Joint Publication 3-27*, Homeland Defense*, p, I-1.

13 "Organizational Chart," Department of Homeland Security, last modified February 1, 2017, pp. 1 and 21, <https://www.dhs.gov/organizational-chart>, accessed on March 25, 2017; "Information Analysis and Infrastructure Protection," 6 US Code, 2017, §121 and "Definitions" 6 US Code, 2017, §311 et seq. (FEMA); "Coast Guard and Maritime Transportation Act of 2012," Public Law 112-213, 126 Stat 1540, December 20, 2012, codified at 14 US Code §3, (Coast Guard).

14 It exceeds the scope of this article to parse overlaps in protective functions among FPS and other commonly-known, specific government personnel and buildings, such as the White House protected by the U.S. Secret Service and the U.S. Capitol protected by the U.S. Capitol Police. For this analysis, it is sufficient to focus on FPS as the responsible entity for protecting government property in general.

15 "Establishment of Coast Guard," 14 US Code, §1, and §3 (a) and (b).

16 "The Homeland Security Act of 2002." This act defines "American homeland" and "homeland" as "the United States" but contains no definition for homeland security. "Our Mission," DHS, <https://www.dhs.gov/our-mission," last modified May 11, 2016, accessed on April 4, 2017. "The vision of homeland security is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards." Christopher Bellavita, "Changing Homeland Security: What is Homeland Security?" *Homeland Security Affairs*, Vol. 4, June 2008, <https://www.hsaj.org/articles/118>, accessed on April 4, 2017.

17 "Critical Infrastructure Protection Act of 2001," 42 US Code, 2017, §5195c(b)(3) and (c)(1) and (2).

18 "Critical Infrastructure Protection Act of 2001," 42 US Code*,* 2017, §5195c(e).

19 Barack Obama, Presidential Policy Directive 21*,* "Directive on Critical Infrastructure Security and Resilience," February 12, 2013, Introduction, <https://obamawhitehouse .archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil," and <https://www.hsdl.org/?view&did=731087>, accessed on March 21, 2017.

20 ICF International, pp. 88 and 91. This report was prepared for the U.S. and Canadian governments. It demonstrates that most utilities are investor-owned, and that it is difficult to achieve results across the grid. Brinkman et al., pp. 3, 6, and 13. The 2011 and 2013 electric grid exercises revealed private owners had not implemented available security measures. National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, *Deepwater: The Gulf Oil Disaster and the Future of Offshore Drilling,* report to the President, U.S. Government Printing Office, Washington, DC, January 11, 2011, pp. 118–127,

<https://www.gpo.gov/fdsys/pkg/GPO-OILCOMMISSION/content-detail.html>, accessed on April 2, 2017. Problems with design and protective measures and with management practices and oversight by owner and subcontractors caused the disaster.

21 Hayes and Ebinger; Strategic Foresight Initiative, *Critical Infrastructure: Long-term Trends and Drivers and Their Implications for Emergency Management*, June 2011, <https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf>, accessed on April 2, 2017. This research and report was prepared for FEMA. U.S. Department of State, Under Secretary for Democracy and Global Affairs, "Critical Infrastructure Protection," August 2007, <https://2001-2009.state.gov/g/avianflu /91243.htm>, accessed on April 2, 2007. This article discusses how critical infrastructure is interconnected even outside the U.S., including in Canada and Mexico. Christopher Bellavita, "85% of What You Know about Homeland Security is Probably Wrong," *Homeland Security Watch*, March 16, 2009, <http://www.hlswatch.com/2009/03/16/85-percent-is-wrong/>, accessed on April 2, 2017. Bellavita critiques the commonly-used 85 percent figure used to describe private-sector ownership of critical infrastructure. U.S. Campbell (see Note 6 above) gives an example from the electric grid where only nine federal electric utilities are federally owned; 189 are investor-owned; 2,013 are publicly-owned by non-federal entities; and 887 are consumer-owned.

22 David Wise, "Federal Real Property: GSA Should Inform Tenant Agencies When Leasing High-Security Space from Foreign Owners," GAO-17-195, Washington, DC, January 2017, pp. 2, 13, and 20, <http://www.gao.gov/products/GAO-17-195>, accessed on April 2, 2017; Sophie Tatum and Pamela Brown, "First on CNN: Report Finds National Security Agencies at Risk in Foreign-Owned Buildings," CNN, January 30, 2017, <http://www.cnn.com/2017/01/30/politics/gao-report-foreign-ownership/>, accessed on February 1, 2017; James K. Jackson, *The Committee on Foreign Investment in the United States (CFIUS)*, U.S. CRS, RL33388, Washington, DC, February 19, 2016, pp. 30–31, <https://www.hsdl.org/?view&did=790777>, accessed on April 2, 2017.

23 William L. Painter, *Issues in Homeland Security Policy for the 113th Congress*, U.S. CRS R42985, Washington, DC, February 27, 2013, p. 3, <https://www.hsdl.org /?view&did=732600>, accessed on April 2, 2017. In addition, the report crystallizes a key point. Arguably, "homeland security, at its core, is about coordination because of the disparate stakeholders and risks .... Without a general consensus on the literal and philosophical definition of homeland security... some believe that there will continue to be the potential for disjointed and disparate approaches to securing the nation."

24 US-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," April 2004, p. 139, <https://energy.gov/oe/downloads/blackout-2003-final-report-august-14-2003-blackout-united-states-and-canada-causes-and>, accessed on January 16, 2017.

25 ICF International, pp. 88 and 91; Brinkman et al.; GAO-15-692T, pp. 6–7, 10, and 16–17; National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, pp. 118–127.

26 National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, pp. 118–127.

27 Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, "Critical National Infrastructures," report, April 2008, p. 53, <http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf>, accessed on January 29, 2017.

28 US-Canada Power System Outage Task Force, p. 21; National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, pp. 126–127 and 250–251. The National Commission stated that it is important to assure the "independence and integrity of government institutions charged with protecting the public interest." The government agency did not adopt pending regulations, opposed by industry, "that would have required companies to manage all of their activities and facilities, and those of their contractors, under a documented Safety and Environmental Management System (SEMS)" until after this

disaster. Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, pp. 53–54, 57, 59–60, 80–81, 104, 155, 157, and173. As another example, the EMP Commission suggested standards that the DHS either would set itself or work with other government agencies to set. Suggested standards include requiring gasoline and diesel fuel distribution facilities to have on-site power generation in the event of electrical grid failure, testing and installing electrical equipment, requiring incorporation of new technology in telecommunications infrastructure, and improving the hardening of oil and gas control systems to avoid damage from EMP effects.

29 Paul W. Parfomak, *Physical Security of the US Power Grid: High-Voltage Transformer Substations*, U.S. CRS R43604, Washington, DC, July 2, 2015, pp. 2, 30, and 32, <https://www.everycrsreport.com/files/20150702_R43604 _df43c1c3c34ecca8d6730fcca7cff108dbdd4a66.pdf>, accessed on February 1, 2017; Brinkman et al., pp. iii-iv, 3, 6, 13, and 29; ICF International, pp. 14–16, 88, and 91.

30 Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, "A Failure of Initiative," final report, 109th Cong., 2d sess., 2006, HR Rep. 109-377, pp. 1 and 3, <https://www.gpo.gov/fdsys/pkg/CRPT-109hrpt377/pdf/CRPT-109hrpt377.pdf>, accessed January on 15, 2017; The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, Washington, DC, February 23, 2006, pp. 40–43 and 61, <https://www.hsdl.org/?view&did=460536>, accessed on January 15, 2017.

31 6 US Code §457 mandates that: "Except as otherwise provided in sections 186(c) and 441(c) of [title 6] and section 1315 of title 40, this chapter vests no new regulatory authority [in the DHS] … and transfers … only such regulatory authority as exists on November 25, 2002, within any agency, program, or function transferred to the [DHS]… or that … is exercised by another official of the executive branch with respect to such agency, program, or function." The provisions of 6 US Code §186(c) and §441(c) are not relevant to this article, with §186(c) permitting the DHS to designate anti-terrorism technology for liability protection and §441(c) relating to research and development issues. "Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014," Public Law 113-254, 128 Stat 2898, codified at 6 US Code §621 et seq. and "Consolidated Appropriations Act," 2008, Subtitle J, Secure Handling of Ammonium Nitrate, Public Law 110-161 (Title V, Section 563), 121 Stat 2083, codified at 6 US Code §488 et seq. These laws amended the Homeland Security Act of 2002 and authorized new regulatory authority for these two specific programs directed only at the chemical sector.

32 "Coast Guard Authorization Act of 2010," Public Law 111-281, (Title VIII, §820[a]), 124 Stat 3001, codified at 46 US Code §70124 (Port Security). This section authorizes that "the Secretary may issue regulations necessary to implement this chapter" [Chapter 701 of Subtitle VII which includes port, vessel, and maritime transportation security issues]. 14 US Code §100 authorizes the USCG to enforce 46 US Code, Chapter 551, Coastwise Trade Laws. For an overview, see USCG, "Authorities," <http://www.overview.uscg.mil/Authorities/>, accessed on March 23, 2017.

33 50 US Code, (2017), §191. The statute specifies regulation by the Secretary of Transportation with presidential approval, but as explained in 6 US Code §457, this authority would be exercised by the DHS, with presidential approval, since the USCG was transferred from the DOT to the DHS. The statutory history and citations to the *US Statutes at Large* and public laws are set forth in the note to 50 US Code §191, beginning with the statute's origination and continuing with the two most recent amendments, "The Omnibus Consolidated Appropriations Act," Public Law 104-208, Div. C, Title VI, §649, 110 Stat 3009-711 and "Coast Guard and Maritime Transportation Act of 2004," Public Law 108-293, Title II, §223, 118 Stat 1040.

34 14 US Code §2(3). Another provision tasks the USCG to "enforce or assist in the enforcement of all applicable Federal laws on, under, and over the high seas and waters subject to [U.S.] jurisdiction." 14 US Code §2(1). If the Federal Aviation Administration (FAA) or the U.S. Air Force (USAF) do not regulate low-flying drones over U.S. territorial waters, then this security gap would be ripe to assign to the USCG, unless it fits in the regulatory scheme of the FAA or USAF.

[35] "Coast Guard Authorization Act of 2010," Public Law 111-281, Title VI, §612, 124 Stat 2970, codified at 46 US Code §1 and §3306.

[36] USCG, "Authorities," <http:www.overview.uscg.mil/Authorities>, accessed on March 23, 2017.

[37] 6 US Code §621 et seq., §622(a)(2)(C) risk-based performance standards; §624, civil enforcement; §624(c), emergency orders; §627, promulgation of regulations to implement the CFATS law.

[38] 6 US Code §488a(a). The proposed regulation for the Secure Handling of Ammonium Nitrate would establish the Ammonium Nitrate Security Program. A regulation has not been issued to implement the statute. DHS, "Ammonium Nitrate Security Program," October 7, 2016, <https://www.dhs.gov/ammonium-nitrate-security-program>, accessed on March 23, 2017.

[39] "Homeland Security Act of 2002," Public Law 107-296, Title XVII, §1706(b)(1), 116 Stat 2317, codified at 40 US Code §1315(b)(1).

[40] 14 US Code §141.

[41] 14 US Code §2(1), (2), law enforcement, maritime aerial surveillance; §89, law enforcement; §95(a)(1), (2) and §99, carrying firearms and making arrests; 14 US Code §100, authority to enforce chapter 551 of title 46, coastwise trade laws (shipping and transportation); 14 US Code §143. USCG officers "are deemed to be officers of the customs … subject to regulations issued by the Secretary of the Treasury governing officers of the customs." For additional information, see USCG, "Authorities."

[42] 50 US Code §191.

[43] 14 US Code §2(7), §1 and §3.

[44] Matt Matthews, *The Posse Comitatus Act and the United States Army: A Historical Perspective*, Combat Studies Institute Press, Fort Leavenworth, KS, 2006, pp. 1–46; Banks and Dycus, pp. 92–93 and 105–112; Charles Doyle and Jennifer K. Elsea, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law*, CRS R42659, Washington, DC, August 16, 2012, pp.19–20, <https://fas.org/sgp/crs/natsec/R42659.pdf>, accessed on February 5, 2017.

[45] "National Defense Authorization Act for Fiscal Year 2017," Public Law 114-328, Div. A., Title XII, §1241(a)(2), 130 Stat 2497, codified at 10 US Code §275 (renumbered from 50 US Code §375).

[46] Doyle and Elsea, p. 4. The USCG is not mentioned in the *posse comitatus* prohibitions, and "as a practical matter, however, the USCG is statutorily authorized to perform law enforcement functions." Banks and Dycus, p. 110. These authors take the view that the USCG "is subject to the *Posse Comitatus* Act only when it is called into service as part of" the U.S. Navy.

[47] 6 US Code §466.

[48] 14 US Code §141.

[49] Elaine M. Grossman, "Former JAG: Military Aid in DC Sniper Pursuit May Have Broken Law," *Inside the Pentagon*, Inside Washington Publishers, November 14, 2002, <https://fas.org/sgp/news/2002/11/itp111402.html>, accessed on April 4, 2017, quoted in Banks and Dycus, pp. 194–195.

[50] "Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014," Public Law 113-254, 128 Stat 2919, set forth in note following 6 US Code §621.

[51] Painter, p. 22.

[52] Caitlin Durkovich and David Wulf, statement for the record before the Committee on Homeland

Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, U.S. House of Representatives Washington, DC, February 27, 2014, <http://docs.house.gov/meetings/HM/HM08/20140227/101787 /HHRG-113-HM08-Wstate-DurkovichC-20140227.pdf>, accessed on March 23, 2017.

53 U.S. Chemical Safety and Hazard Investigation Board, "West Fertilizer Company Fire and Explosion (15 Fatalities, more than 260 Injured)," final investigation report, Washington, DC, January 2016, pp. 55 and175, <http://www.csb.gov/west-fertilizer-explosion-and-fire-/>, accessed on March 5, 2017. The fertilizer, blending, retail, and distribution facility was completely destroyed, with widespread damage to more than 150 offsite buildings, including residences, schools, and other structures. More than half of the damaged structures had to be demolished and reconstructed. Total loss was estimated at $230 million. Federal disaster assistance was estimated to exceed $16 million. The company was insured for one million dollars and declared bankruptcy.

54 Currie, p. 10.

55 6 US Code §121. The OIP has statutory authority to assess and make recommendations about critical infrastructure and to collect, analyze, and share information about critical infrastructure protection and threats.

56 "Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005," Public Law 108-375, Div. A, Title V, §512(a)(1), 118 Stat 1811, codified at 32 US Code §§901–908.

57 10 US Code §251.

58 10 US Code §252.

59 10 US Code §253.

60 10 US Code §§10102 and 12406.

61 10 US Code §283(a) and 18 US Code §2332f.

62 10 US Code §282. "The Secretary of Defense, upon the request of the Attorney General, may provide assistance in support of Department of Justice activities relating to enforcement of section 175, 229, or 2332a of title 18 during an emergency situation involving a weapon of mass destruction." 10 US Code §283(b). "Military explosive ordnance disposal units providing rendering-safe support to Department of Justice activities relating to the enforcement of section 175, 229, or 2332a of title18 in emergency situations involving weapons of mass destruction shall provide such support in a manner consistent with the provisions of section 328 of this title." 18 US Code §175, biological weapons; 18 US Code §229, chemical weapons; 18 US Code §2332a, weapon of mass destruction.

63 14 US Code §1 and §3.

64 "Robert T. Stafford Disaster Relief and Emergency Assistance Act," Public Law 100-707, 102 Stat 4696, codified at 42 US Code §5170(a), (b), major disaster; §5191(a), (c), emergency assistance. Both statutes also permit a request by an Indian tribal chief executive. 42 US Code §5122. A "major disaster" is a natural catastrophe (including hurricane, tornado, tsunami, snowstorm, drought, etc.) "or, regardless of cause, any fire, flood, or explosion" that the president determines "causes damage of sufficient severity and magnitude to warrant major disaster assistance…" An "emergency" means "any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States."

65 42 US Code §5170a, major disaster assistance; §5191(a), emergency assistance.

66 42 US Code §5170(a)(5) and §5191(b)(5), "where necessary to save lives, prevent human suffering, or mitigate severe damage." 42 US Code §5170b, "essential to meeting immediate threats to life and property"; §5185, emergency communications systems, including before disaster; §5186, emergency public transportation; §5187, fire management assistance. 42 US Code §5191(b), the federal government has primary responsibility for response because of exclusive or preeminent responsibility and authority pursuant to the Constitution or federal law.

67 32 US Code §905. The Secretary of the DoD provides funds "to that State in an amount that the Secretary determines is appropriate." This clarity, however, does not mean the State must accept the mission or the amount of funding determined by the DoD.

68 32 US Code §904(b). The statute limits this duty to 180 days. The time may be extended once for 90 days "to meet extraordinary circumstances."

69 32 US Code §906. The statute requires specific reporting to Congress. Also, a funding request initiated by the governor must contain a certification that homeland defense activities "are to be conducted at a time when the personnel involved are not in Federal service."

70 Also, consider the case of an EMP burst, which studies predict would result in widespread devastation and chaos that likely will completely overwhelm state and local first responders. Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack; Sirius Bontea, "America's Achilles Heel: Defense Against High-Altitude Electromagnetic Pulse: Policy v. Practice," master's thesis, U.S. Army Command and General Staff College, 2014, <http://www.dtic.mil/docs /citations/ADA613532>, accessed on March 5, 2017.

71 10 US Code §274, §275, §282, and §283.

72 10 US Code §275 specifies "Army, Navy, Air Force, or Marine Corps" and 18 US Code §1385 specifies "Army or Air Force."

73 Doyle and Elsea, p. 30. This report lists twenty-two statutory exceptions to the *Posse Comitatus* Act. This list does not include, however, 10 US Code §§271–284, some of which contain additional exceptions to the posse comitatus prohibition. Banks and Dycus, pp. 103 and 193–195.

74 14 US Code §3(b).

75 10 US Code §5170(a)(2), "including precautionary evacuations and recovery," and §5170a(3)(F), "recovery activities, including disaster impact assessments and planning," compared with §5191(b)(2) and (3).

76 DHS, USCG, "Incident Specific Preparedness Review (ISPR) Deepwater Horizon Oil *Spill,"* final report, Washington, DC, January 2011, p. 9, <http://www.uscg.mil/foia/docs /DWH/BPDWH.pdf>, accessed on January 21, 2017. The USCG report on the 2010 Deepwater Horizon disaster noted confusion by state and local authorities. State and local authorities were familiar with the National Response Framework (NRF) used for hurricanes and similar disasters. An oil well explosion and massive oil spill, however, is not one of the NRF planning scenarios, so response proceeded instead under the National Contingency Plan.

77 "The National Security Act of 1947," Public Law 114-328, Chapter 343, §2, 61 Stat 496, subsequently amended and codified at 50 US Code §3002.

78 "Goldwater-Nichols Department of Defense Reorganization Act of 1986," Public Law 99-433, 100 Stat 992 et seq. and 993-994 (policy), codified at 10 US Code §101 et seq., and policy set forth at 10 US Code §111 note.

[79] See earlier discussion of attacks on the electric grid in Metcalf, CA, and the explosion in West, TX.

[80] 6 US Code §121(d) and §124l.

[81] 6 US Code §456. Reese, Summary. This report cautions that "the US government does not have a single definition for 'homeland security'… [which] may impede the development of a coherent national homeland security strategy and may hamper the effectiveness of Congressional oversight." Banks and Dycus, pp. 11, 265, and 274–275. These authors conclude: "Civilian agencies, chiefly the Department of Homeland Security, should harmonize their emergency response plans with those of the Defense Department, including the establishment of a single line of command authority." Painter, pp. 1 and 3. This report states that several homeland security functions remain with "their original executive branch agencies and departments, including the Departments of Justice, State, Defense, and Transportation." The report cautions: "Without a general consensus on the literal and philosophical definition of homeland security, achieved through a strategic process, some believe that there will continue to be the potential for disjointed and disparate approaches to securing the nation."

[82] 6 US Code §§111(b)(1), 121(d).

[83] Hayes and Ebinger, pp. 1–2 and 19–20. Study results indicate that the private sector is focused on day-to-day vandalism and theft threats and believes that "the government will step in to cover losses in the event of a catastrophe." ICF International, p. 88.

[84] 6 US Code §124, national asset database and prioritized list. Stephen L. Caldwell and Gregory C. Wilshusen, "Critical Infrastructure Protection: Observations on Key Factors in DHS's Implementation of Its Partnership Approach," testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate, GAO-14-464T, Washington, DC, March 26, 2014, p. 6, <http://www.gao.gov/assets/670/661945.pdf>, accessed on March 12, 2017. This report notes that industry does not want to share information with the federal government and opines that the government needs to collect information about why facilities did not make security-related improvements.

[85] Examples are in this article, in addition to the DHS, USCG, "Incident Specific Preparedness Review (ISPR) Deepwater Horizon Oil Spill," final report, p. 9.

[86] Banks and Dycus, pp. 91–92 and 105–106.

[87] The White House, pp. 54–55.

[88] Banks and Dycus, pp. 107–108; Doyle and Elsea, p. 1.

[89] Banks and Dycus, p. 275. The way the *posse comitatus* doctrine has evolved in the U.S. should be reexamined and "possibly adjusted to enable a practical, response flexible response to future black swans and other crises." Deborah L. Geiger, "*Posse Comitatus*, the Army, and Homeland Security: What is the Proper Balance?" strategy research project, U.S. Army War College, 2006, <https://www.hsdl.org/?view&did=469535>, accessed on April 2, 2017. Geiger reviews the history of *posse comitatus* and proposes allowing trained military police personnel to assist more actively civilian law enforcement personnel in response to domestic emergencies.

[90] 18 US Code §1385, previously was in Title 10 but was moved to Title 18 (Crimes) in 1956. 70A Stat 626.

[91] 10 US Code §275 (DoD); 6 US Code §466 (DHS); Doyle and Elsea, p. 30; Banks and Dycus, pp. 103 and 193–195; see Table 5.

[92] U.S. Constitution, Preamble and Art. 1, Sec 8.

93 10 US Code §12406. The National Guard may be activated to federal service where invasion or danger of invasion; rebellion or danger of rebellion against U.S. authority; or "the President is unable with the regular forces to execute the laws of the United States." Doyle and Elsea, p. 30. This report lists this statute as a statutory exception to the Posse Comitatus Act.

94 10 US Code §§251–255, to suppress insurrections and rebellions and to enforce federal authority and federal and state laws; §§271–284, military support for civilian law enforcement agencies, including with WMD and bombings of public places, and Title 42 disaster/emergency assistance; and other lesser-known statutory authorizations detailed in Doyle and Elsea, p. 30 (for example, to protect Yellowstone National Park upon request by the Secretary of the Interior).

* All references to the US Code were accessed from this website as of March 21–25, 2017; any statutory changes since March 21–25, 2017 are not reflected in this survey of federal statutory law.

Fostering Interagency Collaboration for Upstream *Counterproliferation*

by Matthew D. Rautio

The proliferation of emerging and disruptive technologies, such as additive manufacturing and gene editing, is changing the way we think about national security. Such trends in science and technology inevitably increase the likelihood of hostile nations or non-state actors acquiring weapons of mass destruction (WMD). These emerging, novel threats have proved particularly vexing for the existing landscape of U.S. security bureaucracies. Absent major restructuring of the government to protect against future threats, significantly higher levels of proactive interagency collaboration will be required to successfully respond to the challenges posed by new technologies. Given these three premises—the threat of massively destructive (or disruptive) weapons, the lowering of the proliferation threshold, and the mismatch between these threats and the Cold War-legacy structure of U.S. government bureaucracies—the key to successful counter proliferation lies in fostering interagency collaboration before crises emerge.

Derek W. Lothringer, Matthew S. McGraw, Leif H.K. Thaxton, and I developed and tested a concept of collaboration aimed at increasing transparency, sharing resources, and fostering interdependence across the full range of interagency actors.[1] Our definition of effective collaboration requires extensive sharing of information, assets, responsibilities, and consequences, both good and bad. While this requirement may appear to be an obvious formula for maximizing organizational efficiency, it is not always the norm within the U.S. national security bureaucracy, where budgets, authorities, jurisdictions, and personalities too often work against whole-of-government efforts to achieve common policy objectives.

We used a formal collaborative methodology called "opportunity analysis (OA)" to examine the dynamics of interagency collaboration at a major U.S. Embassy in Asia. The embassy team participated in a scenario-based, table-top exercise (TTX) to elicit multiagency approaches to counter a proliferation network smuggling sensitive nuclear technology. We used the formal collaborative

Lieutenant Matthew D. Rautio recently earned an MBA from the Graduate School of Business and Public Policy as well as a M.S. in Irregular Warfare at the Naval Postgraduate School (NPS). Rautio was part of an interdisciplinary capstone team whose efforts helped develop the Counter Proliferation Center and a Counter Proliferation educational track within the Defense Analysis Department at NPS.

process to facilitate and expand collaboration among the agencies represented in the country team. Our research, while not exhaustive, highlights effective methods to encourage collaboration and demonstrates the benefits of expanded collaboration in counterproliferation (CP) policy and operations.

The proliferation threat is poised to grow as new technologies create new ways to make WMD.

Weapons of Mass Destruction are the Only Existential Threat

Weapons of mass destruction represent one of the few existential threats to national sovereignty. It is for this reason that countering the spread and use of nuclear, chemical, and biological weapons has been a consistent priority for U.S. policy since Manhattan Project scientists warned policymakers that the proliferation of nuclear technology was inevitable.[2] Since the invention of the atomic bomb in the 1940s, the U.S. government has used a mix of policy tools, including treaties, alliances, technology controls, and sanctions, to limit the number of nations possessing such capabilities.

The U.S., along with international partners, has been largely successful in blunting the proliferation of WMD. This argument is supported by the fact that there are only ten nations with declared nuclear weapons programs, despite the technology's 70-year history.[3] Nonetheless, several countries have covertly developed WMD capabilities, often with the aid of illicit procurement networks designed to evade national and international nonproliferation efforts. The best example is the A.Q. Khan proliferation network, which procured goods and services on behalf of Pakistan's nuclear program and then sought new customers by offering to supply Iran, North Korea, Libya, and others.[4]

The proliferation threat is poised to grow as new technologies create new ways to make WMD. For example, the nuclear fuel cycle necessary to produce nuclear weapons traditionally involves large industrial facilities that have a significant footprint. Nuclear reactors and enrichment and reprocessing plants are easily identified and provide important clues to a nation's intentions. Iran's Natanz enrichment facility, for example, became the focus of international nonproliferation concern. Advancements, such as additive manufacturing, commonly known as "AM" or "3D printing," could make it possible for illicit suppliers and nations harboring covert programs to evade international controls and conceal their activities.[5] In the biological realm, new gene-editing techniques, such as clustered, regularly-interspaced, short-palindromic repeats (CRISPR), might lower the bar for scientific skills required to enable countries and even nongovernmental organizations (NGOs) to explore biological-weapon concepts. Many powerful new technologies are not controlled by governments, which makes WMD acquisition easier and harder to detect.[6]

The U.S. government relies on the combined efforts of the executive branch agencies to implement and enforce U.S. policies, laws, and treaties. In practice, this combined policy body is referred to as the interagency (IA). The participants in the IA process may change depending on the issues, but for national security matters, the group normally reflects the members of the President's National Security Council (NSC).[7] The President and chief White House advisors empower the executive agencies to formulate and implement policy directives and priorities. This formula for national security policy is essentially unchanged since the National Security Act of 1947 created the current government organization.[8] For nonproliferation and CP policy, the IA normally includes representatives from the full range of diplomatic (State Department), military (Defense), intelligence community (Central Intelligence Agency [CIA], Director of National Intelligence [DNI], Defense intelligence Agency [DIA]), law enforcement (Justice, Federal Bureau of Investigation [FBI] , Homeland Security, Commerce) and financial (Treasury, Commerce) agencies. The interagency process determines how the different authorities and capabilities that exist throughout the government can be combined to form effective nonproliferation and CP strategy.[9]

The fall of the Soviet Union inspired new thinking in the form of Cooperative Threat Reduction programs to address the threat of "loose nukes" but did not create an immediate need for departmental reorganization to counter or combat emerging CP threats.[10] As a result, there are gaps among departments organized to counter Cold War-style, peer-competitor threats and new threats emanating from a radically-changed, global security environment.[11] Since 2001, the Global War On Terrorism, in particular, required the IA to adopt new strategies and explore new approaches. Not surprisingly, however, hostile nations and terror groups have adapted to assertive U.S. military actions and learned to exploit what General Joseph L. Votel, then commander of U.S. Special Operations Command, described as a gray zone. just below the U.S. response threshold.[12] Operating in the gray zone enables U.S. adversaries to exploit bureaucratic boundaries within the IA. These gaps also exist for nonproliferation and CP and are exacerbated by the use of new technologies.

Old CP/WMD Bureaucratic Divisions of Labor No Longer Effective Against New Threats

The existing national security bureaucracies, designed in the immediate wake of World War II, were structured for a world that no longer exists.[13] Built at the apex of interstate diplomacy and industrialized warfare, they have been slow to react to—or even recognize—the new threat environment.[14] Today's adversaries actively exploit departmental seams across the range of U.S. government agencies.[15] Given the nature of this challenge, IA collaboration is increasingly essential to address dynamic threats, such as the proliferation of WMD.

Expansive and rapid technological innovation is outpacing the speed at which decisionmakers are able to react to crisis.[16] The U.S. government does not currently have the agility to effectively address the speed of exponential, technological advancements; it lacks the capacity and expertise to deeply analyze the diverse range of potential dangers. The complexity and scale represented by such a diverse spectrum of WMD threats constitute a "wicked problem," as no single agency or department in the U.S. government has the capacity or understanding to tackle them alone.[17] The problems are compounded in the steady state when no crisis is spurring the IA into action.

The existing national security bureaucracies, designed in the immediate wake of World War II, were structured for a world that no longer exists.

We argue that expanding collaboration between relatively autonomous U.S. government agencies in the steady state enables more layering of authorities, experience, and institutional knowledge to frame nuanced options and support comprehensive action and policy.[18] As Brigadier General Terence J. Hilder wrote, "The root issue of interagency woes is the absence of an effective interagency process to drive policy integration and synergy within the departments of the Executive Branch."[19] In light of the changing threats and status quo agencies. we see a need for enhanced IA collaboration prior to a crisis.

...one potential disruptive innovation is the emergence of additive manufacturing or 3D printing.

Changing Proliferation Threats: Modern Procurement Networks and DIY Technologies

As proliferation networks search for new ways to provide their customers with illicit access to controlled technologies, one potential disruptive innovation is the emergence of additive manufacturing or 3D printing. The leading industry guide, Wohlers Associates, describes additive manufacturing as, "the process of joining materials to make objects from three dimensional data, usually layer upon layer, as opposed to subtractive manufacturing methodologies."[20] 3D printing, a term used interchangeably with additive manufacturing, refers to the production of metal, plastic, and even biological objects from a single device driven by an electronic design file to fuse raw material inputs using a direct energy source (often a laser).[21] Many industries are in the midst of a revolution that is forcing them to adopt strategies to incorporate the disruptions in economies of scale, supply-chain management, and retail manufacturing brought about by 3D printing.[22] Rapid prototyping through additive manufacturing has already drastically lowered time and costs to achieve breakthroughs in biotech development, information technology, and materials engineering, just to name a few.[23]

Additive manufacturing is one example of an emerging technology that is outpacing Moore's Law, the computing term referring to the observation that the number of transistors in an integrated circuit has doubled approximately every two years.[24] To place this in context, if a 3D-printed toy takes four hours to print today, it will take just seven minutes and 30 seconds to print by 2025.[25] Government experts, such as Bruce Goodwin, contend that within five to ten years, the advancements in 3D printing of metal, when combined with high-speed computing, will lower the threshold barrier for making uranium enrichment centrifuges and, eventually, nuclear weapons.[26] The combination of the two—the ability to print centrifuges for enriching uranium and the ability to print weapon components—is potentially world changing.

The U.S. is not the leader in this technology—the UK and Germany are, with Asia poised to take over this industry in the future. Singapore, for example, is investing $400 million in a five-year, advanced-manufacturing project focused on 3D printing.[27] The Chinese government is pledging to invest $245 million over the next seven years to become the global additive-manufacturing leader.[28] While additive manufacturing is having positive effects on multiple industries in the global marketplace (shipping, manufacturing, and medical, to name a few), the potential threats to global security cannot be ignored. Actors like North Korea and Iran could easily circumvent national and international export controls to simply print their own parts. Proliferation networks might use 3D-printing technology to open new global markets for proliferation and facilitate new threats to world order.[29] With the diffusion of additive manufacturing, barriers to obtaining WMD would be drastically lowered, not only for states but for proxy and non-state entities for whom ideology may run deeper than rational deterrence can hope to reach.[30]

Opportunity Analysis as a Means to Expand Collaboration

Given that antiquated bureaucratic structures align poorly against emerging technology threats, inaction becomes the default position. As observed by David Kilcullen, political and defense leaders are simply too overwhelmed and overtasked to do anything more than manage current crises.[31] If current methods of ad hoc collaboration and interorganizational challenges are not overcome, the next crisis just might be the nightmare of the "nuclear 9/11." To address this lack of bureaucratic inertia, we explored how a formal collaboration tool could energize U.S. CP policy.[32]

Ad hoc collaboration, the present norm in the IA, suffers from limitations without the forcing function of crisis. There are instances of productive, ad hoc, IA collaboration; however, these efforts are difficult to reproduce or sustain. An effective collaboration process can overcome some aspects of organizational stove-piping. It can change attitudes toward cooperation and information sharing and introduce opportunities for the broader changes required across the CP community of practice.

We applied OA as a formal collaboration process that divides and analyzes complicated problems. It enables an interdisciplinary and multiorganizational team to analyze a problem set using unconstrained thinking, dialogue, and collaborative software. The process breaks down large, "wicked" problems into digestible pieces. OA uses common language to replace organization-specific jargon. It enables a diverse group to organize, communicate, and operate to discover opportunities. These opportunities could be missed when relying on ad hoc collaboration alone.[33] OA is grounded in the U.S. Special Operations Pathway Defeat (SOPD) methodology that was developed for planning the "upstream" defeat of WMD. This method accounts for the equities of each department or agency in the shared CP mission space. OA goes farther than SOPD by framing alternative futures and discovering opportunities to enable or prevent those futures. OA uses an alternative-futures pathway analysis with a nodal dissection technique to divide and analyze a problem (see Figure 1, page 40). Through the OA process, a team focuses on one alternative future at a time and looks for opportunities to create pathways for action.

The OA process enables enhanced collaboration by identifying each organization's RICCAAAPP "recap") components, described below, and aligning them against a particular problem:

- **Responsibility**. Having the specific charge to execute a particular action.

Ad hoc collaboration, the present norm in the IA, suffers from limitations without the forcing function of crisis.

- **Influence.** Ability to effect action through a third party to accomplish one or more of the above elements or to act independently to accomplish counter-WMD (CWMD) objectives.

- **Capability**. The explicit abilities of regional and global resources with CWMD-specific technical capabilities, training, equipment, and readiness.

- **Capacity.** The depth and sustainability of regional and global resources to provide a specific capability to support CWMD operations for the required time or cycles of operations.

- **Awareness**. Cognizance of an issue or opportunity, combined with the speed and agility to move the information required to coordinate and collaborate across an array of interagency, regional, or global partners to enable rapid planning and engagement.

- **Authority**. The existence of legal authorities to carry out the required actions.

- **Access**. Physical access to the point of action.

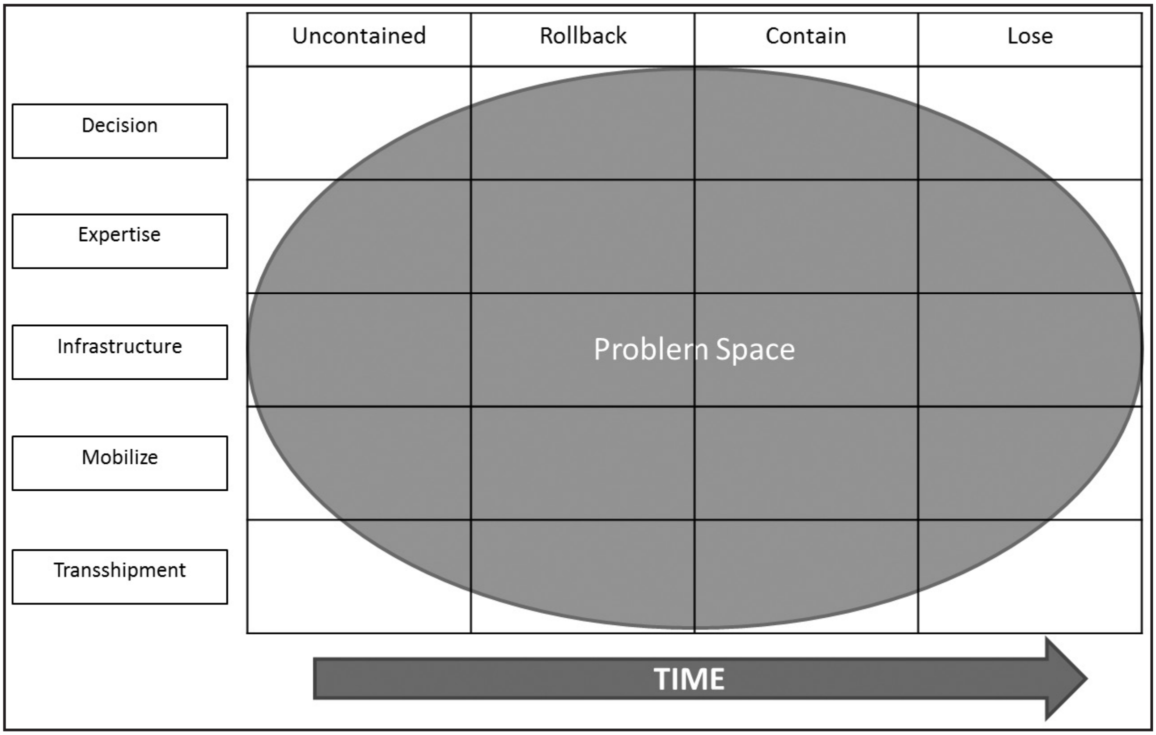


Figure 1. OA Nodal Dissection Technique at Macro Level

- **Placement**. Ability to achieve access through organizational position or nontraditional means.

- **Policy**. Department, national, or international strategies, guidelines, or norms that enable, or at least justify a CWMD action, including treaties, agreements, regimes, and the like.[34]

The agency RICCAAAPPs are collectively known as mission enablers. The OA process facilitates the identification of RICCAAAPPs and provides a structure for identifying collaborative opportunities to apply them to complex problems such as CP (see Figure 2).

By methodically considering the relevant attributes of the organizational contributors and matching them against the relevant aspects of the problem, collaboration opportunities emerge. The nature of the process itself is designed to increase the flow of information, as well as to erode cultural barriers among participants, providing additional, potential mechanisms toward increased collaboration.

Other factors also influence the potential for IA collaboration. In October of 2014, the OA methodology helped a cross-functional IA team in Washington, DC, develop a strategy in support of U.S. Central Command (USCENTCOM). Based on our observations of that exercise, we developed a hypothesis about possible limiting conditions. In this case, the OA occurred near the headquarters of the agency representatives, which had at least two effects. First, the participants were physically close to their bureaucratic headquarters, including their bosses and colleagues. It may be the case that the culture and pressures of their home organization could create a formidable challenge to collaboration, whereas physical distance from headquarters might lessen the dampening effect. Second, not all the participants in this OA exercise had a higher authority to authorize or facilitate, let alone enforce collaborative policies that might diverge from established policy. Those that did benefitted in tangible ways. Perhaps a venue that

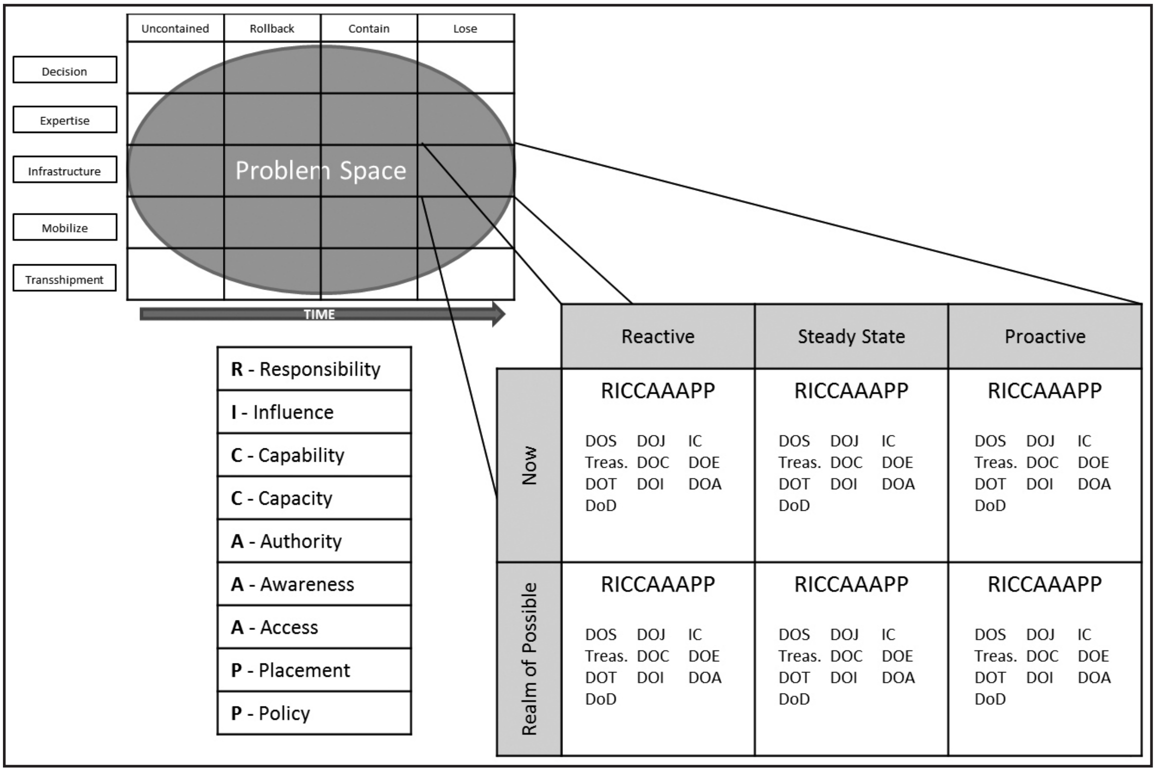


Figure 2. Dissection of CP Problem into Actor Attributes

included access to an entity possessing some attributes of a third-party authorizer and enforcer would allow for more innovative collaboration concepts. Finally, the participants in this exercise did not know one another personally. We wondered if pre-existing personal relationships might similarly result in higher levels of agency collaboration.

Based on these ruminations, the notion of an embassy team emerged as a venue to explore these arguments. Multiagency teams in embassies operate far from their organizations' headquarters; they function under the authority of the ambassador; and they work in close proximity to one another for extended periods. Some trade-offs, however, stemming from venue selection may be expected. For example, the dedication of organization resources to a common effort may be controlled above the level of authority normally found in an embassy; the same may go for committing an organization to a joint decision made in the field. Therefore, we expected the transparency dimension of collaboration to increase in an embassy venue and the resource sharing and interdependence dimensions to decline.

To explore these arguments regarding the use of formal collaborative processes and the venue of collaboration, we conducted an exploratory field study. Such field studies provide both limited deductive and inductive insights. In such studies "variables co-vary as expected but are at extremely high or low values [that] may help uncover causal mechanisms. Such cases may not allow [strong] inferences to wider populations … but limited inferences might be possible if causal mechanisms are identified."[35] This approach fit the needs of the OA study for many reasons. First, hypothesizing that the use of a formal process would increase collaboration among an interagency working group is intuitive. The potential interactive effects that such a process may produce in an already high-performing embassy team, however, might be significantly higher. The purpose, then, beyond recording the increase in collaboration (the causal "effect" of the study), was to search for the pathways by which such a set of conditions produces increased collaboration (the causal "mechanisms" of the study). Further, such mechanisms may emerge in unexpected ways, and the exploratory field study allowed for such inductive results. Though inferences and generalizations from such a study may be limited, its results provide the springboard for further studies and tool refinement.

The Singapore OA Exercise

We developed an embassy-level exercise to examine the application of the OA process by an IA team to a challenging, CP problem involving emerging technology. To execute the study, we first sought to establish a "baseline" of expected value of collaboration, grounded in the results of the earlier USCENTCOM exercise. We then developed a plan of qualitative data gathering to include an extensive set of interview questions to derive insights from our embassy collaboration scenario.

...the OA process encouraged discussion of the differences between agencies and departments and effectively drew out mutually-acceptable ideas...

The proliferation of WMD is a complex, global problem. Countering it effectively requires extensive sharing, delegation, communication, and understanding of other interests or, in our terminology, transparency. We devised a scenario that involved global proliferation networks, state sponsors, 3D printing, and a tangled mess of criminal and legitimate behavior. The OA took place at the U.S. Embassy in Singapore and involved representatives of the relevant law enforcement, defense, diplomacy, and other entities under the auspices of the ambassador.

The most significant features of the OA, as noted by TTX participants, were the use of a common language, the enabling of open and honest discussion, and the group consensus about which organization would take the lead in implementing agreed strategies. One participant in the Singapore OA TTX commented on the increased transparency enabled by the OA methodology: "…by listening [and understanding] various organization's perspectives, capabilities, and resources, we were able to better understand how we can support, which in turn created an atmosphere conducive towards proactive engagement."[36] Another OA TTX participant remarked on how highlighting one organization's weakness provided insight as to how another organization could step in to provide support:

> The construct of the exercise provided a setting for individual agencies to provide overviews of existing capabilities and weaknesses in a non-threatening way. By focusing discussion of weaknesses or gaps in an interagency context, it encouraged discussion of potential issues and problems between agencies and departments.[37]

We observed the utility of using common language, as opposed to organization-specific jargon and doctrine, to defuse biases and promote the sharing of ideas and information. The use of a common language helped agency representatives discuss their capabilities and weaknesses and avoid confusion. By focusing on information and capability gaps that exist within the seams of the IA partners, the OA process encouraged discussion of the differences between agencies and departments and effectively drew out mutually-acceptable ideas about how to address shortcomings. Due to the scenario focusing on steady-state initiatives (as opposed to crisis), the IA group identified which organization was best suited to take the lead or support as the scenario unfolded.

Of particular note was the extent to which the seasoned, IA group lacked understanding of RICCAAAPPs in the CP mission space. Dispensing with acronyms and with OA to facilitate dialog, the group found value in the CP role in the steady state. Many assumed DoD capabilities were limited to crisis operations. All parties gained new awareness of what each agency brings to the table in terms of RICCAAAPP. The structure of the process and user-friendly communication tools (we used SharePoint) facilitated real-time information-sharing that brought about transparency, which increased collaboration among the participants. Transparency proved to be the dimension of collaboration most significantly increased through OA. The exercise provided the opportunity for participants to uncover areas ripe for substantial joint benefit simply through the systematic revealing of their attributes and how they could be applied to a common problem. The venue greatly benefitted the OA process via the pre-existing, personal relationships among the embassy working group members, as well as the signal of approval from the Ambassador.

Resources provided by an organization and from outside sponsors are key elements affecting the commitment to a collaborative effort. Working from the collective understanding that collaboration is not possible without people, money, and time, participants noted what aspects of the OA most impact the sharing of resources. In this case, key factors included the personnel selected to support the collaborative effort, minimal funding requirements, and the connection of the OA exercise outcomes with managers and decisionmakers at agency headquarters. An OA TTX participant observed, "in the current budget environment, it is very difficult to increase program funding levels and I don't see this process as changing that, unless it was because another organization was willing to redirect its resources to the greater inter-organizational effort."[38] The pooling of scarce resources and reassurance that field representatives would not make unauthorized expenditures were important.

Allowing each agency to control its people and resources was crucial. We encouraged broad involvement from all relevant organizations and at multiple levels. Some organizations had representation from the strategic, operational, and tactical levels, helping to facilitate vertical collaboration and coordinate requests for resources. The fact that there was no need to increase funding to participate in the collaborative process was helpful. The main expense was the time commitment required.

We observed that resource-sharing showed a mild increase in the OA, relative to the other dimensions of collaboration. The sharing of significant resources by the Ambassador provided a clear signal to the participants of his support for the effort to expand collaboration, despite the limitations on personnel inherent at an embassy. The embassy venue, in this case, may have limited some aspects of collaboration, as opposed to locating collaboration efforts in Washington, where personnel and resources may be more abundant.

Resources provided by an organization and from outside sponsors are key elements affecting the commitment to a collaborative effort.

Another key variable for collaboration was interdependence. Understanding and trusting other agencies is necessary to achieve whole-of-government approaches. For our TTX, we included academic institutions, industry partners, and a variety of relevant governmental bodies in the scenario. Within this complex landscape, individual participants had to work with multiple agency representatives to identify collaborative courses of action. Taking directly from the response of one OA TTX participant on inter-organizational collaboration:

> The main reward of collaboration within our organization is opportunity. Interaction with other organizations and groups gives us the ability to build relationships that will provide the unit with additional information, access, and placement. The relationships we establish extend our network and provide us with more intelligence gathering and analysis opportunities.[39]

...personal relationships greatly enhanced collaborative efforts.

Increased transparency led to more positive attitudes toward interdependence throughout the process. Use of a common language, the shifting of lead roles between agencies and departments given the specific problem, and having representation from national, regional, and country-team levels all made it easier for participants to rely on other organizations. In the words of one participant, the OA "improved awareness and appreciation for policy and how academic alliances could be used as an instrument of national power to assist and solve seemingly intractable problems."[40] Representation from different levels within organizations improved awareness vertically, so that a broad span of stake holders could better understand the actions being considered in the field.

For some, the process highlighted their own limitations, especially with respect to the steady-state conditions before a crisis. The OA process showed them how it was in their interests to collaborate and let other agencies take the lead. Without the OA discovery process to illuminate mutually-beneficial outcomes, institutional bias greatly diminishes the willingness to admit deficiencies and lend resources to ensure a competitor's success. In Singapore, this tension was evident in the different approaches pursued by law enforcement, diplomacy, and defense. One participant summarized: "We were encouraged to piggyback off other organizations' comments and efforts; to use their actions as a springboard for other ideas."[41] The combined strategy developed by the group was affirmed by consensus to be greater than the sum of the individual parts.[42]

Finally, personal relationships greatly enhanced collaborative efforts. The OA process deepened preexisting professional relationships, which extended from the field reps to managers located in various home institutions.[43] The combination of horizontal and vertical collaboration, made possible by organizational representation from varying levels, led not only to the development of relationships but to greater interdependence, making more effective collaboration possible.[44] A participant commented on the value of organizational relationships:

> Relationship-building is a critical piece in this puzzle. And I'm not talking about team-building exercises. I'm talking about the kind of "around the table" discussions that have taken place in a professional manner, where each person could establish her/his credibility and potential contribution, followed by on-the-margin discussions, whether around a table or at a social event. People will still need to represent the equities of their respective organizations, but relationships can eliminate or at least lower barriers that exist due to pre-existing organizational culture.[45]

Over the course of the Singapore OA exercise, we observed increases in individual and organizational collaboration, measured in terms of transparency and interdependence. Over time, the participants developed more understanding of the other agencies RICCAAAPPs and collectively built integrated strategies to cope with the scenario. The fact that the scenario involved several challenging elements—unfamiliar technology being used in an innovative way by a sophisticated proliferation network—invited the country team members to consider new approaches based on an expanded understanding of their combined power.

New Collaborative Methods Are Needed to Enable U.S. Policy to Keep Pace with Rapidly Evolving Technology Threats

Weapons of mass destruction remain one of the few existential threats to U.S. national security and economic prosperity. Nation state and non-state threats echo a rhetoric indicating the possible use of WMD; although, the timeframe for such attacks remains unclear. The U.S. IA process is made up of stove-piped, hierarchical organizations. These departments and agencies, each with its own mission, goal, and culture, have evolved to value fiscal accountability, program support, and other bureaucratic priorities along with their missions.[46]Adversaries of the U.S. may have the ability to exploit vulnerable seams between interagency departments and their missions. As General Votel writes:

> The National Security Act of 1947 served us well, but in an era far removed from the Cold War, the United States needs a new construct for the 21st Century. There is widespread agreement that going forward, we will require an unprecedented level of Interagency (IA) coordination capable of synchronizing all elements of national power.[47]

We explored the use of OA to achieve the type of coordination called for by General Votel. Widespread diffusion of emerging and disruptive technology is lowering the barrier for countries and groups to acquire such high-leverage capabilities, some of which may meet the definition of WMD. For the most part, these emerging technologies will make positive contributions to human welfare. Old control techniques based on export control regulations and international agreements may not be applicable to the new global realities. Additive manufacturing printers, for example, are not being controlled in the way that nuclear-fuel-cycle equipment was restricted under the auspices of the Nonproliferation Treaty, the International Atomic Energy Agency, and the Nuclear Suppliers Guidelines.[48] Similarly, innovations in cyber warfare, genomics, or drones are not controlled by any international code. In this environment, the old institutions charged with safeguarding our security must adopt new methods to reenergize an old bureaucracy to defend against new threats.

...old institutions charged with safeguarding our security must adopt new methods to reenergize an old bureaucracy to defend against new threats.

A formal collaborative process, such as OA, can develop multiple, collective approaches to emerging technology issues. Of the nearly 170 steady-state (non-crisis or pre-crisis) CP approaches developed in Singapore, most centered around diplomatic and law enforcement outreach programs. These approaches sought to leverage industry engagement to establish norms and standards for the transfer of potentially dangerous goods. In time, such norms and standards could encourage a degree of self-regulation, which emerged as a goal for the Singapore-based additive manufacturing community. Without laws or treaties to restrict trade in these technologies, self-interested self-regulation arose as a possible bulwark against unfettered proliferation. Through the OA process, the embassy team devised a joint engagement strategy aimed at educating companies and partner nations to deter, detect, and stop illicit trade in emerging WMD-related technologies such as 3D printing. The strategy would employ stepped up communication, visits, and informational briefings for companies involved with 3D printing. One idea was to conduct an OA. including government and the private sector, to promote broader awareness of the potential proliferation problems associated with a broad range of merging technologies. The goal would be to encourage a high degree of self-regulation for technologies that are not subject to legal controls. We would expect to see the same types of expanded collaboration, transparency, and interdependence take root among self-interested companies as we saw among governmental actors, drawing the private sector into the collaborative interagency strategy and strengthening the coalition of law enforcement, defense, and intelligence partners in the CP enterprise.

We are aware of inherent "selection effects" in our research. The embassy working group was already a cohesive team prior to the OA exercise, and they had the explicit endorsement of the Ambassador to participate. The outcome of the process—in this case, 169 distinct concepts developed through the OA process—was no doubt influenced by existing relationships and the supportive environment. Nevertheless, we were encouraged by the measurable improvements in collaboration and would expect to see comparable results in other circumstances where multiple entities share a common mission. For further research, we would like to see OA performed by other embassies and among other parts of the U.S. government focused on other issues. For example, how might OA help promote more effective strategies toward counterterrorism issues, such as the fight against Islamic State of Iraq and the Levant (ISIL), human smuggling, or nuclear deterrence?

Finally, as members of the Special Operations Command (SOCOM) community, we learned important lessons about how we are perceived by other members of the CP community, including the DoD. As the result of a recent change in the Unified Command Plan that transfers DoD responsibilities for CP from Strategic Command to SOCOM,[50] SOCOM is deeply engaged in a process to enable them to execute this mission. Our OA research has direct relevance for this process, and the lessons we drew apply to SOCOM's role and participation with its IA partners. During both the October 2014 USCENTCOM exercise and the August 2015 Singapore exercise, a common perspective expressed by IA colleagues suggests a limited awareness of DoD and particularly Special Operations Forces (SOF) RICAAAPs. For that matter, SOCOM itself may not be fully aware of the extent of its own capabilities relevant to CP and how they complement those of other agencies.

We concluded that the OA process, which started over twenty years ago as a SOF method for identifying CP target nodes,[51] possesses significant potential for guiding both SOCOM and the U.S. government through the changes in technology and in global access to that technology that challenge our governmental structures. Innovative collaboration is necessary to adapt to innovations in technology, global business, and the ways they are changing WMD proliferation. ***IAJ***

NOTES

[1] Derek W. Lothringer et al., “Countering Weapons of Mass Destruction: A Preliminary Field Study in Improving Collaboration,” Naval Postgraduate School, March 2016.

[2] For a broad overview of U.S. nuclear nonproliferation efforts, see Henry Sokolski, *Underestimated: Our Not So Peaceful Nuclear Future*, Nonproliferation Education Center, 2016.

[3] Arms Control Association, “Nuclear Weapons: Who Has What at a Glance,” October 2015, <http://www.armscontrol.org/factsheets/Nuclearweaponswhohas>, accessed on September 21, 2016.

[4] David Albright, *Peddling Peril, How the Security Nuclear Trade Arms America’s Enemies*, Free Press, New York, 2010 and Gordon Carrera, *Shopping for Bombs: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the AQ Khan Network*, Oxford University Press, Oxford, UK, 2009.

[5] On such patterns of diffusion, see John Arquilla, “Patterns of Commercial Diffusion,” in Emily O. Goldman and Leslie C. Eliason (eds.), *Diffusion of Military Technology and Ideas*, Stanford University Press, Stanford, CA, 2003.

[6] On proliferation and new technologies, see Zachary Davis et al. (eds.), *Strategic Latency and World Power: How Technology is Changing Our Concepts of Security*, Lawrence Livermore National Laboratory, Livermore, CA, 2014.

[7] Colin Dueck, “Recommendations for the NSC Process,” Foreign Policy Research Institute, January 19, 2016.

[8] Significant exceptions are the establishment of the Department of Homeland Security and the Office of the Director of National Intelligence in the aftermath of 9/11.

[9] Zachary Davis, “Bombs Away,” *The American Interest*, January 1, 2009.

[10] Emily Goldman, *Power in Uncertain Times: Strategy in the Fog of Peace*, Stanford University Press, Stanford, CA, 2010.

[11] The National Commission of Terrorist Attacks on the United States, also known as the 9/11 Commission, confirmed the stove-piped nature of the U.S. government institutions; see 9/11 Commission Report at <http://www.9-11commission.gov/report/911Report.pdf>, accessed on November 12, 2016.

[12] General Joseph L. Votel, U.S. Army, Commander, United States Special Operations Command, statement before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, Washington, DC, U.S. House of Representatives, 2015, p. 7, <http://fas.org/irp/congress/2015_hr/031815votel.pdf>, accessed on October 21, 2016.

[13] U.S. Congress, “The National Security Act of 1947,” Public Law 253, July 26,1947.

[14] Douglas T. Stuart, *Creating the National Security State: A History of the Law That Transformed America*, Princeton University Press, Princeton, NJ, 2012.

[15] Amy Zegart, *Flawed by Design: The Evolution of the CIA, JCS, and NSC*, Stanford University Press, Stanford, CA, 2000.

[16] Marc Goodman, “From Crowdsourcing to Crime-Sourcing: The Rise of Distributed Criminality,” *Big Think*, 2011, <http://bigthink.com/future-crimes/from-crowdsourcing-to-crime-sourcing-the-rise-of-distributed-criminality>, accessed on August 4, 2016.

17 Horst W. J. Rittel and Melvin M. Webber, *Dilemmas in a General Theory of Planning*, Institute of Urban & Regional Development, University of California, Berkeley, CA, 1972 and H. Brenton Milward and Joerg Raab, "Dark Networks as Organizational Problems," 2003, <http://www.hks.harvard.edu/netgov/files/talks/docs/03_06_06_seminar_millward_dark_networks.pdf>, accessed on November 10, 2015; Jeffrey Conklin, *Dialogue Mapping: Building Shared Understanding of Wicked Problems*, John Wiley & Sons, Chichester, West Sussex, UK, 2005; and Kenneth J. Menkhaus, "State Fragility as a Wicked Problem," *PRISM*, Vol. 1, No. 2, 2010, pp. 85–100.

18 Douglas McGregor, "The Human Side of Enterprise," *Reflections*, Vol. 2, No. 1, 1966, pp. 6–15; E. L. Trist, "Collaboration in Work Settings: A Personal Perspective," *Journal of Applied Behavioral Sciences*, Vol. 13, 1977, pp. 68–278; Barbara Gray, *Collaborating: Finding Common Ground for Multiparty Problems*, Jossey-Bass, San Francisco, 1989; Barbara Gray and D. J. Wood, "Collaborative Alliances: Moving from Practice to Theory," *Journal of Applied Behavioral Science,* Vol. 27, No. 2, 1991, pp. 3–22; and Scott T. Allison et al., "Outcome Biases in Social Perception: Implications for Dispositional Inference, Attitude Change, Stereotyping, and Social Behavior," *Advances in Experimental Social Psychology*, Vol. 28, 1996, pp. 53–93.

19 Terence J. Hildner, *Interagency Reform: Changing Organizational Culture through Education and Assignment*, U.S. Army War College, Carlisle Barracks, PA, 2007.

20 Wohlers Associates, "What Is Additive Manufacturing," informational material, <https://www.wohlersassociates.com/additive-manufacturing.html>, accessed on December 10, 2015.

21 Had Lipson and Melba Kurian, *Fabricated: The New World of 3D Printing*, John Wiley & Sons, Indianapolis, IN, 2013 and Irene J. Petrich and Timothy W. Simpson, "Point of View: 3D Printing Disrupts Manufacturing: How Economies of One Create New Rules of Competition," *Research-Technology Management*, Vol. 56, No. 6, pp. 12–16.

22 Stephanie S. Shipp et al., *Emerging Global Trends in Advanced Manufacturing,* Institute for Defense Analysis, Alexandria, VA, 2012.

23 J.-P Kruth at al., "Progress in Additive Manufacturing and Rapid Prototyping." *CIRP Annals - Manufacturing Technology*, Vol. 47, Issue 2, 1998, pp. 525–540.

24 Radhakrishna Harmane, "From Moore's Law to Intel Innovation—Prediction to Reality," *Technology@Intel Magazine,* April 2005, pp. 1–9.

25 Brian Krassenstein, "Moore's Law of 3D Printing…Yes it Does Exist and Could Have Staggering Implications," Print.com, 2014, <http://3dprint.com/7543/3d-printing-moores-law/>, accessed on September 30, 2016.

26 Michael Lucibella, "Manufacturing Revolution May Mean Trouble for National Security," APS News, 2015, <http://www.aps.org/publications/apsnews/201504/revolution.cfm>, accessed on September 23, 2016.

27 Rose Brooke, "China Flexes Muscles in 3D Printing Race," *TCT Magazine*, 2013, <http://www.tctmagazine.com/3D-printing-news/china-flexes-muscles-in-3dp-race/>, accessed on November 12, 2016.

28 Wohler Associates, "Wohler Report 2015," <http://wohlersassociates.com2015report.htm>, accessed on February 2, 2017.

29 David Albright and Corey Hinderstein, "Unraveling the AQ Khan and Future Proliferation Networks," *Washington Quarterly*, Vol. 28, No. 2, 2005, pp. 109–128.

30 Robert Jervis, "Rational Deterrence: Theory and Evidence," *World Politics*, Vol. 41, No. 2, 1989, pp. 183–207 and Neil Gershenfeld, "How to Make Almost Anything," *Foreign Affairs*, Vol. 91, No. 6, 2012, pp. 43–57.

31 David Killcullen, "Psychological Warfare and Deception," lecture, Naval Postgraduate School, August 13, 2015; Michael R. Eastman, "Whole of Government Is Half an Answer," *InterAgency Journal*, Vol. 3, No. 3, Summer 2012, pp. 31–39; Sean M. Roche, "Is It Time for an Interagency Goldwater-Nichols Act?" *InterAgency Journal*, Vol. 4, No. 1, Winter 2013, p. 12; and Ralph O. Doughty and Ralph M. Erwin, "Building National Security through Interagency Cooperation: Opportunities and Challenges," in Linton Welles II et al. (eds.), *Changing Mindsets to Transform Security: Leader Development for Unpredictable and Complex World*, United States Institute for National Strategic Studies, 2013, pp. 249–262.

32 To operationalize the concept of collaboration for this study, we identified three dimensions with measurable indicators. These dimensions are transparency, resource-sharing, and interdependence. We argue that each is a necessary condition for true collaboration, and we build a rigorous operationalization of the concept to discipline our coding of collaborative efforts. See Lothringer, et al., Appendix A.

33 Michael Scott et al., *Opportunity Analysis for U.S. Embassy Singapore: Additive Manufacturing as a Disruptive Technology and its Implications for WMD Proliferation*, OASD CWMD Systems, Washington, DC, 2015.

34 It is important to note that the terms included in Figures 1 and 2 are notional and tailored to the specifics of one field study.

35 Scott et al.

36 Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences*, The MIT Press, Cambridge, MA, 2005, p. 75.

37 Lothringer, et al., p. 49.

38 Ibid., p. 49.

39 Ibid., p. 50.

40 Ibid., p. 51.

41 Ibid., p. 52.

42 Ibid., p. 52.

43 Ibid., p. 52.

44 Ibid., p. 52.

45 During and after the OA, we referred to collaboration across departments and agencies at the national or regional level as "horizontal collaboration" and the regional–national collaboration as "vertical collaboration."

46 Lothringer, et al., p. 53.

47 Valdis Krebs, "Organizational Hierarchy: Adapting Old Structures to New Challenges," Organette, 2008, <http://www.orgnet.comorgchart.html>, accessed on September 22, 2016.

[48] Joseph L. Votel, "The Grey Zone," United States Special Operations Command White Paper, September 9, 2015, p. 6.

[49] Matthew Korangi and Tristan Volpe, "3-D Printing the Bomb? The Nuclear Nonproliferation Challenge," *The Washington Quarterly*, Vol. 38, Fall 2015, pp. 7–19.

[50] Presidential Memorandum, "Delegation of Authority of Unified Command Plan Responsibilities," August 5, 2016, <https://www.whitehouse.gov/the-press-office/2016/08/05/presidential-memorandum-delegation-authority-unified-command-plan>, accessed on August 20, 2016.

[51] Interviews with former SOCOM operator and OA originator.

Join the CGSC Alumni Association!

The Alumni Association program allows graduates of the U.S. Army Command and General Staff College to stay connected and support the College through the CGSC Foundation.

Member dues are used as a base of support for the alumni mission including the website and our *Foundation News* magazine. Our benefits to the association members includes a subscription to the magazine and information updates.

For more information contact the CGSC Foundation:

ph: 913.651.0624

email: office@cgscf.org

or visit www.cgscfoundation.org

Nuclear Terrorism –

Imminent Threat?

by Brendan G. Melley

The 2015 National Security Strategy of the United States stated that "No threat poses as grave a danger to our security and well-being as the potential use of nuclear weapons and materials by irresponsible states or terrorists."[1] On March 25, 2014, in The Hague, President Obama stated, "I continue to be much more concerned when it comes to our security with the prospect of a nuclear weapon going off in Manhattan."[2] This is a sentiment he repeated throughout his presidency, and it has reference, of course, to the frequently alluded-to scenario of terrorists obtaining nuclear weapons or "weapons-usable" nuclear material (i.e., fissile material that could be used in a nuclear weapon, also known as weapons-grade material). Experts and senior officials frequently state that this scenario is a matter of "when," not "if."[3] This concern became even more urgent after it was learned that al Qaeda had sought access to nuclear material and technical knowledge associated with building a nuclear weapon, and it remains a concern with ISIS and other violent extremist organizations.

The fear of a nuclear apocalypse at the hands of terrorists has been amplified in the media, in movies and novels, and by political leaders' statements since 9/11. In some respects, a violent extremist organization like al Qaeda already can be presumed to be a terrorist nuclear power, for they have been able to terrorize Americans about a possible nuclear attack without necessarily having to prove that they possess an actual weapon.[4]

Yet, a terrorist nuclear attack has not occurred to date. Terrorism experts and analysts have debated this for years, and no consensus exists as to why the world has not seen terrorists succeed at perpetrating a nuclear attack. Despite the seeming inevitability of a terrorist attack with a nuclear weapon, terrorists may be substantially less likely to conduct such an attack than most analysts and policymakers expect, for two overarching reasons:

Brendan G. Melley is a senior research fellow at the National Defense University Center for the Study of Weapons of Mass Destruction. He received a master's in WMD Studies as a National Defense University Countering WMD graduate fellow.

1. Nuclear terrorism is difficult to accomplish, both technically and operationally.

2. There is no basis for a *prima facie* assumption that would-be nuclear terrorists cannot be disrupted, if not deterred, from conducting a nuclear attack.

Technical and Operational Difficulties

Technical Issues

Nuclear terrorism threats could take shape in three general pathways: the deliberate transfer of nuclear material from a state to a terrorist group or non-state actor; the sale of nuclear materials to a non-state actor on the black market, which may end up in the hands of a terrorist group; and, the theft or "leakage," or unintentional diversion of nuclear material from a state program.[5]

The question of whether terrorists would be able to steal an actual nuclear weapon from a nuclear-armed state, while conceivable, is highly problematic due to the extraordinary security afforded nuclear weapons. Attention usually is drawn to those nuclear states with perceived less-than-optimal security over their stockpiles and weapons; and many analysts point out that the spread of nuclear weapons to North Korea, and potentially Iran, increases the risk of terrorists getting access to nuclear material or weapons through collusion with regime officials, or lack of effective oversight or security. Allied to this is the fear that presently non-nuclear states will pursue a nuclear weapons program in Asia or the Middle East to counter North Korea's and Iran's (apparently suspended) nuclear weapons programs. This possibility would, of course, offer terrorists potentially more opportunities to acquire a weapon or the necessary material. However, the same reasons why existing nuclear states feel dis-incentivized to share nuclear weapons with terrorist would apply to these nuclear aspirants as well.

Several ongoing efforts take the form of addressing the supply problem, i.e., the international availability of fissile and other nuclear-related material. Four Nuclear Security Summits have been held since President Obama spoke in 2009 of "a new international effort to secure all vulnerable nuclear material around the world."[6] The fewer sources of fissile material that exist, the easier it will be to secure the remaining locations from theft or attack. It is precisely for this reason that the United States has made the lockdown of nuclear materials a national priority. Most of the international community ostensibly shares this objective.

The fewer sources of fissile material that exist, the easier it will be to secure the remaining locations from theft or attack.

The 2004 United Nations Security Council Resolution (UNSCR) 1540 directs states to refrain from "providing any form of support to non-[s]tate actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery." It also called for states to adopt and enforce "appropriate effective laws" and "establish domestic controls" to prevent the proliferation of WMD to non-state actors.[7] The aims of UNSCR 1540 have been institutionalized in efforts that include the legacy Cooperative Threat Reduction programs with the states of the former Soviet Union, the Russia- and U.S.-led Global Initiative to Combat Nuclear Terrorism, and the Proliferation Security Initiative, to which over 100 states have subscribed.

The "supply" side of nuclear weapons production likewise poses significant technical and operational challenges for terrorists pursuing a nuclear weapon from raw fissile materials. The simplest nuclear device to assemble would be a crude "gun-type" weapon with a quantity of highly enriched uranium (HEU).[8] The concept is simple enough: by means of high explosives, drive one mass of HEU into another one, causing the now super-critical mass of HEU to release its energy in a nuclear explosion.[9] Even so, substantial technical hurdles exist to getting the HEU into the right physical state, size, shape, and with the necessary chemical properties to be useful in a gun-type device.[10] A possessor of uranium would have to refine the ore to metallic form, understand any impurities within its composition, cast it, and then machine it to precise specifications of size and shape.[11]

Terrorists would need access to highly specialized machinery and equipment in order to manufacture the necessary HEU for a nuclear device.

Terrorists would need access to highly specialized machinery and equipment in order to manufacture the necessary HEU for a nuclear device. Much of the equipment necessary is specifically designed for the particular purpose of nuclear weapons production (such as numerous sensitive high-speed gas centrifuges configurable into cascades) and not generally available on the open market. Indeed, the infamous nuclear program supplier Abdul Qadeer Khan needed years to assemble the equipment necessary to manufacture centrifuge parts for the state nuclear programs to which he sold. A terrorist group that chooses to pursue a large centrifuge plant for enriching uranium as its path to acquire fissile material for a nuclear weapon would be taking on a very long timetable to achieve its aims. Even committed states spend years acquiring, manufacturing and testing centrifuge cascades. “The equipment is so specialized, and the suppliers so few, that a forest of red flags would go up.”[12] Customs and export licensing officials in most countries would take notice of the equipment and materials being transferred, ask questions, and possibly prevent the shipment from being sent or received.

Plutonium, a by-product of uranium in nuclear power plant operations, is available in hundreds of reactors around the world.[13] Here again, however, the weaponization process is not a simple one. Weapons-ready plutonium must be chemically reprocessed in order to be suitable for an implosion-type device, in which exactly shaped high explosives rapidly compress a mass of plutonium into itself and create a nuclear explosion.[14] To accomplish this, terrorists would need “precision machine tools to build the parts, special furnaces to melt and cast the plutonium in a vacuum … and high-precision switches and capacitors for the firing circuit.”[15] Plutonium is harder to handle than HEU due to its high heat and radioactivity and requires more restrictive physical protective measures to prevent radioactive sickness or death. Terrorists would have to observe the “absolute need of foreseeing, preparing for, and observing all the necessary precautions” of working with plutonium.[16] If terrorists had access to a nuclear reactor that produced plutonium, they would need a “special, shielded chemical plant to chop up its radioactive fuel, dissolve it in acid, and then extract the plutonium from the acid.”[17]

Whether terrorist use HEU or plutonium, they still likely would also require “non-nuclear explosive testing” to develop a weapon with confidence that it would work.[18] This may involve very specialized testing devices of the implosion system, and the high-explosive “lenses” that would be triggered, to see if the plutonium would be compressed symmetrically and result in a suitable yield.[19] Without access to appropriate – and sensitive – diagnostic equipment, terrorists would have to resort to theoretical calculations, which would place a high premium on the caliber of the involved engineers for the operation.[20]

Operational Issues

Unless a state that was a nuclear power provided terrorists with an already manufactured warhead, terrorists would need time, a secure space, and a talented team of engineers, chemists, metallurgists, and physicists. Highly trained personnel such as these, ideally with experience in a state's nuclear weapons program, might be able to be identified as potential recruits to the terrorist organization, either for money or ideology. It is even quite possible that a few former weapons designers and engineers would be susceptible to being recruited by a terrorist group. However, it is far from certain that an entire weapons design and manufacturing team could be assembled securely by a terrorist group at one time.

In addition to the actual manufacturing of a device, operational security would be one of the terrorist groups' major challenges. The more people involved in what most likely would be a terrorist organization's most sensitive operation, the more the risk of detection and disruption by law enforcement or intelligence personnel. If the group is not adequately walled off or quarantined (for what likely would be an extended period of time), some might brag or even just hint at the importance of the project, and this might be detected.

Another operational consideration that terrorists would have to contend with is the physical movement of the device to its intended target, from the safe haven in which it was manufactured. Dozens of national and international programs have been created after the attacks on September 11, 2001, to monitor the trade routes that supply goods to markets around the world. Terrorists would have to conduct "complex international operations involving training, travel, visas, finances and secure communications" to be able to accomplish such an operation.[21] Even if mechanisms can be thwarted or bypassed, the mere perception of a concerted international effort to find nuclear weapons in the global commons might be expected give a terrorist group pause as they consider how best to move their weapon.

Finding a pathway to move a nuclear device potentially around the world is not without significant risk of losing physical control of the cargo, or having it detected and stopped. Using black market smuggling routes and facilitators could be one possible option, but terrorists would face the attendant risks of losing the shipment to criminal interlopers who might not know anything about the cargo other than it had high value to the shipper, and thus could be stolen from the terrorists.

...it is far from certain that an entire weapons design and manufacturing team could be assembled securely by a terrorist group at one time.

A related logistics question is whether the terrorist group would choose to accompany their cargo throughout the path to its destination. This would inevitably raise the profile of the shipment for the necessity of it being monitored. Accompanying the shipment will create risks for the terrorists themselves, as they could be identified in transit by law enforcement or intelligence agencies. Throughout the journey, anyone whom the terrorists might consider as "trusted" accomplices would create more vulnerabilities, as more people become aware of the importance of the cargo. Knowing these risks, if the terrorists decided to send the cargo without physical accompaniment, they would thus be putting their most valuable cargo into the international shipping system and hope that the system delivers the weapon to their designated far-end, witting, recipient for final preparations and movement to the intended target.

Assuming the worst case—that a terrorist group had the ability to acquire an adequate supply of appropriate fissile material, and had the time, space, and talent to manufacture a nuclear device—two key questions emerge: would it work, and how many would the terrorists want to produce?

...as proliferation of WMD programs continues, the risk grows that some state, friendly to terrorist groups, will permit or enable the transfer of WMD material to terrorists.

For the first question, without a testing program, the production of even a crude gun-type device may not produce a functioning device.[22] Terrorists want to be seen by their audience as being successful in executing a nuclear attack. Their sponsors' confidence would be eroded, and the confidence of the intended audience could be enhanced, by the production of a device that did not work. Without the involvement of skilled engineers and scientists throughout the process, a terrorist group could not be sure that whatever instructions they received were accurate, or even adequate to create a working nuclear device.

Regarding the second question, it is useful to consider that if terrorists only acquired the material for one bomb, "they would still lack an arsenal—and a single mistake in design could wreck the whole project."[23] Moreover, a terrorist group should certainly recognize that after exploding a nuclear weapon, the combined efforts of the world's law enforcement, intelligence, diplomatic and military resources would be deployed to find them and bring them to justice. If the terrorists claimed to have additional nuclear weapons, the hunt would be even more urgent and unrelenting until the terrorists and their weapons were found. While terrorists may employ suicide bombers, the terrorist leadership itself surely would want to live to guide the organization and likely would see the need to develop a good plan for staying hidden and alive for a lengthy period of time.

The security of terrorists' operations from leaks or the disruptive effect of counterterrorism missions, combined with the challenges of coordinating and executing secure shipment, add extra elements of risk and uncertainty to the major challenges terrorists face in trying to acquire the nuclear material itself.

The Commission on the Prevention of WMD Proliferation and Terrorism noted that as proliferation of WMD programs continues, the risk grows that some state, friendly to terrorist groups, will permit or enable the transfer of WMD material to terrorists.[24] On the other hand, states that possess nuclear material are not likely to transfer a weapon or weapons-usable material to a terrorist or non-state actor without a great deal of confidence that the transfer would go undetected, and attribution would remain undetermined. This would mean that "a state seeking to orchestrate a nuclear attack by proxy would be limited to collaboration with well-established terrorist organizations with which it had existing relationships, simplifying the task of connecting terrorist perpetrators to their state sponsors."[25] Moreover, "no state would be likely to give its nuclear weapons or materials to a terrorist organization with which it did not have a long record of cooperation and trust."[26]

"Few states trust their proxies," commented one analyst, "and indeed they often gravely weaken movements they support in order to control them."[27] A terrorist group "might use the weapons or materials in ways the state never intended, provoking retaliation that would destroy the regime."[28] For example, "Iran lacks deniability for the groups to which it might transfer more-advanced systems, but lacks the trust that would make it more likely to transfer advanced systems."[29]

Terrorists should expect intense retribution, whether they had a "return address" or not. A nuclear terrorist attack would prompt an immense, “unprecedented,”[30] international effort to determine the source of the material, and attribution efforts likely would continue for as long as it took for responsibility for the attack to be judged.

Simply, the risk of being held responsible would seem very high for a state that provides nuclear material to a terrorist group. Brian Jenkins notes, “It would require a government to take enormous risks. … [E]ven state sponsors of terrorism have become more cautious when engaging in larger-scale, higher-risk operations.”[31]

Deterring Attacks

While there have been very few nuclear terrorist attacks from which conclusions can be drawn, it also is not possible to rule out the extent to which terrorists are being deterred or disrupted from conducting a nuclear attack. Although deterrence has historically been associated with nation states, the organizations and aims that present themselves as factors in a comprehensive deterrence calculus are fundamentally the same for states and non-state actors.[32] Indeed, despite the popular belief (although not one held by many terrorism analysts[33]) that terrorist organizations and leaders are irrational and even suicidal, it may be that the United States and partner nations fighting terrorism are successfully deterring nuclear terrorism even now.

Key to this proposition is the decision-making framework, i.e., what influences them to make the decisions they take, within which terrorist organizations tend to operate. For example, the leadership itself, or the support structure components, might be capable of being influenced, while the operatives themselves may not be dissuaded from attacking a target. It is generally agreed by analysts that suicidal terrorists are difficult to deter, based on their beliefs in the rewards they will attain upon being “martyred.” Yet Jenkins notes that “[n]ot all terrorists welcome death,”[34] and even the most committed might be dissuaded by the idea of their “reward” being long-term confinement in a prison cell.[35] Similarly, it may be possible to influence a terrorist leader’s ability, or his perception of his ability, to achieve his political goals.

...the risk of being held responsible would seem very high for a state that provides nuclear material to a terrorist group.

In addition to the active international cooperative efforts to prevent access to nuclear materials, noted above, the disruptive effects of steady counterterrorist attacks on known terrorist bases and safe havens serve to highlight the risk of operational failure for terrorists. A failure to accomplish its mission of a devastating nuclear attack, either because of technical difficulties or the active measures to disrupt terrorist operations, would in turn undercut the stature or prestige of the group.[36] This need to successfully accomplish what would be the ultimate terrorist mission could drive terrorist leaders to not take some of the risks that may be acceptable at lower levels of violence.

The anticipated overwhelming retaliation for conducting an attack—a prime example of deterrence by punishment—could give some terrorists pause. As Jenkins notes, “An effective deterrent can reinforce existing self-imposed constraints by suggesting that any terrorist attack involving nuclear weapons will not only provoke retaliation but will leave the terrorist group isolated from its constituents, its hosts—those upon whom it depends for sanctuary and support”.[37]

Conclusion

The most simple, and resonant, counterargument to the present thesis is the claim that given the time, space, and necessary materials, terrorists will be able to employ a nuclear weapon successfully. The fear of nuclear terrorism arises from "the assumption that if terrorists *can* get nuclear weapons they *will* get them,"[38] that the only "prudent" response is for officials to assume that "acquisition equals employment," and that they therefore should use all necessary steps to prevent terrorist access to nuclear weapons.[39] Even if they were not able to make a sophisticated device, a successfully detonated nuclear device would still be destructive. "One [has] to assume at least a crude nuclear-weapons capability, and even crude weapons are weapons of mass destruction."[40] Former Vice President Dick Cheney was cited to have said in November 2001, "if there was even a [one] percent chance of terrorists getting a weapon of mass destruction — and there has been a small probability of such an occurrence for some time — the United States must now act as if it were a certainty."[41] If an actor *possibly* can attack successfully with nuclear weapons, this has been perceived as a near-certainty that he *will*.

The fear of nuclear terrorism arises from "the assumption that if terrorists *can* get nuclear weapons they *will* get them,"...

A second possible counterargument is that terrorists "bent on destruction for its own sake cannot be deterred."[42] Numerous statements from terrorist leaders support the view that terrorists will not stop until they are able to execute a devastating attack on a Western city. "The threat to retaliate can have little effect on those for whom mass destruction is an objective, not a fear."[43] And the situation is only getting more grim, as the "spread of nuclear weapons to new states in the Islamic world will place tools of indiscriminate destruction closer and closer to the hands of terrorists, who will use them without fear of retaliation."[44]

However, while these counterarguments are not uncommon in the popular press, they really are not arguments at all – they are counter*claims* that bring to bear no substantial evidence to support the counterargument. Of course, in principle, it is always possible that a nuclear terrorist could succeed. However, one who grants a *carte blanche* to the terrorist must at the same time ignore the mountain of obstacles that stand between terrorist aspirations and the realization of a nuclear terrorist attack.

Debate will continue on the technical and operational challenges associated with terrorists' acquiring the necessary nuclear-related components and material and employing a weapon successfully on a target. Certainly, if the fissile material were available to terrorists — despite the active programs and emphasis to secure remaining stocks of HEU and plutonium that are potentially vulnerable — *and* if enough time, space, and expertise were also available, terrorists would have a chance of making a workable nuclear device. However, the sheer number of conditions associated with this concession constitute significant obstacles to any terrorist's plans. Preventing fissile material and related equipment and expertise from being available to terrorists remains an active effort of the international community. Active efforts by U.S. and partner intelligence and law enforcement services attempt to address whether time and space are available for a terrorist group to make their plans and develop their weapon. Failure on the part of a terrorist organization to achieve success with respect to *any* of these concessions risks the derailing of *all* of the organization's nuclear plans. The more that terrorist leaders are convinced that the world would be turned upside down to hunt them down for a nuclear attack, the better the possibility that they might be deterred. The more that terrorist operatives and supporters understand that their future might not be martyrdom, but spending the rest of their life in a super-maximum security isolation unit, the better the chance that they might have second thoughts about supporting a WMD attack.

The issue of state sponsorship of a nuclear terrorist attack must be acknowledged as speculation, unless and until there is clear evidence of state support to a terrorist nuclear program. Until then, one could reasonably believe that the United States and its partners in the counterterrorism fight are applying enough pressure on actual terrorist plots so that states are taking notice and avoiding being linked to such plots.

The subject of deterring terrorists from employing nuclear weapons is not well understood, and thus is a good area for more debate and research. It is worth trying to understand the role that deterrence plays, and what policies may serve to support the goal of letting terrorist leaders rethink their commitment to conducting a nuclear attack. Of course, "[t]he risk is not zero."[45] This is undoubtedly true. The "one-percent doctrine" attributed to Dick Cheney asserts that if there is a small chance of a catastrophic event occurring to the United States, its friends or allies, including a nuclear terrorist attack, friendly governments must try to take all measures necessary to prevent that event from happening. Yet, this is unrealistic. It is, as Jenkins notes, as if al Qaeda has already become a nuclear power, as they are able to terrorize the world with the simple potential of being able to carry out an attack.[46] Indeed, the "one-percent argument" is applied by some to the nuclear terrorism problem even though it has only an extraordinarily small likelihood of ever occurring. This much, however, can be stated with confidence: Nuclear terrorism is not an existential threat to the United States.[47] An attack could certainly cause many thousands of casualties, disrupt the economy, prompt widespread panic, and spark more intensive security measures across the country. Some speculate that it could change the nature of the Constitutional protections to privacy afforded Americans. Nevertheless, such an attack would not destroy the United States as a nation-state in the way a massive nuclear exchange with the Soviet Union likely would have done. Meanwhile, the United States continues to take substantive measures to secure nuclear material around the globe, to strike terrorists when they can be identified and targeted, to infiltrate and arrest terrorists in their early stages of planning, to reinforce resiliency into the national character, and to deter terrorist leaders from conducting nuclear attacks. These efforts must, of course, be continued and enhanced.

In the end, precisely what combination and quantity of preventive measures will prevent a future nuclear terrorist attack is unknown. However, the wide range of policies against the supply and demand variables of terrorists' acquisition of nuclear weapons are not only justified, but essential. On the supply side, national and international efforts underway must continue. On the demand side, the ability to keep terrorists on the run, literally and figuratively, could cause them to be unable to assemble the materials and team in a secure place for enough time to complete their preparations. A strong combination of focused policies and actions remains the best chance to restrict nuclear terrorism to the realm of theoretical possibility. ***IAJ***

NOTES

[1] White House, *The National Security Strategy of the United States* (Washington, DC: White House, February 2015), p. 11.

[2] Michael D. Shear and Peter Baker, "Obama Answers Critics, Dismissing Russia as a 'Regional Power,'" *The New York Times*, March 25, 2014.

[3] Brian Michael Jenkins, *Will Terrorists Go Nuclear?* Amherst, NY: Prometheus Books, 2008, p. 204.

[4] Jenkins, p. 241.

[5] Daniel Bynam, "Do Counterproliferation and Counterterrorism Go Together?", *Political Science Quarterly* 122:1, 2007, pp. 26, 31.

[6] Barack Obama, Remarks, Prague, Czech Republic, April 5, 2009.

[7] United Nations Security Council, Resolution 1540, S/RES/1540 (2004).

[8] Gary Milhollin, "Can Terrorists Get the Bomb?" *Commentary Magazine*, The Wisconsin Project on Arms Control, February 2002, p. 47; Michael Levi, *On Nuclear Terrorism,* Cambridge: Harvard University Press, 2007, p. 37; J. Carson Mark, Theodore Taylor, Eugene Eyster, William Maraman, Jacob Wechsler, "Can Terrorists Build Nuclear Weapons?" In *Preventing Nuclear Terrorism: The Report and Papers of the International Task Force on Prevention of Nuclear Terrorism*, ed. Paul Leventhal and Yonah Alexander, Lexington, MA: Lexington Books, 1987, p. 55.

[9] Levi, p. 37.

[10] Mark et al, p. 59.

[11] Levi, p. 39; Milhollin, p. 48.

[12] Milhollin, p. 46.

[13] Ibid.

[14] Levi, p. 73.

[15] Milhollin p. 47.

[16] Mark et al, p. 59.

[17] Milhollin, p. 46.

[18] Levi, p. 73.

[19] Levi, pp. 75-76.

[20] Ibid, p. 76.

[21] Keir A. Lieber, and Daryl G. Press, "Why States Won't Give Nuclear Weapons to Terrorists," *International Security* 38:1, Summer 2013, p. 93.

[22] Mark et al, p. 64.

[23] Milhollin, p. 48.

[24] Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, *World at Risk: The Report of the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism*, New York: Vintage Books, 2008, pp. xix-xx.

[25] Lieber and Press, p. 93.

[26] Ibid, p. 96.

[27] Bynam p. 33.

[28] Lieber and Press, p. 85.

[29] Bynam p. 33.

[30] Lieber and Press, p. 91.

[31] Jenkins, pp. 142-3.

[32] Keith Payne, Thomas K. Scheber, Kurt R. Guthe, Cynthia L. Storer, *Deterrence and Al-Qa'ida*, National Institute for Public Policy, Fairfax, VA: National Institute Press, 2012, p. xi.

[33] Jenkins, p. 280.

[34] Ibid, p. 282.

[35] Payne et al, p. xii, xiv.

[36] Ibid, p. x.

[37] Jenkins, p. 283.

[38] Scott D. Sagan and Kenneth N. Waltz, *The Spread of Nuclear Weapons: A Debate Renewed*, New York: W.W. Norton & Company, Inc., 2003, p. 130.

[39] Lewis A. Dunn, "Can al Qaeda Be Deterred from Using Nuclear Weapons?", Occasional Paper, Center for the Study of Weapons of Mass Destruction, Washington DC: National Defense University Press, 2005, p. 2; Sagan and Waltz, pp. 161-2.

[40] Graham T. Allison, Owen R. Cote, Jr., Richard A. Falkenrath, Steven E. Miller, "Avoiding Nuclear Anarchy: Containing the Threat of Loose Russian Nuclear Weapons and Fissile Material." CSIA Studies in International Security, No. 12, Cambridge, MA: MIT Press, 1996, p. 58.

[41] Ron Susskind, "The One-Percent Solution," cited by Michiko Kakutani, "Personality, Ideology and Bush's Terror Wars," The New York Times, June 20, 2006, accessed March 29, 2014 at http://www.nytimes.com/2006/06/20/books/20kaku.html?pagewanted=all&_r=0.

[42] Sagan and Waltz, p. 130.

[43] Ibid, p. 161.

[44] Ibid, p. 166.

[45] Milhollin, p. 45.

[46] Jenkins, p. 241.

[47] Ibid, p. 26.

A Clear Deterrence Strategy
Required for Cyber

by Terrence S. Allen

With the press of a button, a nation goes to war. Much of that nation's livelihood will be destroyed with this button press. In the U.S. there is always an operator ready to hit their button, ensuring a devastating retaliatory attack. This was the scene during the Cold War, with the U.S. and Soviet Union both ready to ensure destruction of the other, should a nuclear launch ensue. Thankfully, that situation never occurred.

Today we live in a scenario very much like this, but with different weapons and participants. Instead of only a few countries with the capability to conduct nuclear warfare, strategic offensive cyberspace operations (OCO) can be conducted by anyone with a computer and network access. Just as the threat of nuclear war changed the conduct of warfare and threatened total war, strategic cyber weapons have the potential to do the same. Unfortunately there are no clear definitions for what is considered cyberwar versus cybercrime. A country's interpretation between the two might simply be based on what side of the attack they are on. The U.S. must take the lead by defining what cyberwar is, what cybercrime is, and formulate a clear strategy on how best to deter future attacks on American targets.

A Change in Warfare: Nuclear Weapons

After the U.S. used atomic bombs on Japan in WWII, it awoke the world to the real and devastating potential of nuclear weapons, changing the paradigm of warfare. This type of technological driven change is not new in the history of war. Technological advances such as the inventions of the longbow, gunpowder, machine guns, aircraft, and tanks all shifted the nature of war and forced paradigm changes. With two bombs, Nagasaki suffered 75,000 killed or wounded and 1/3 of the city devastated[1], while Hiroshima had 130,000 killed, injured or missing and 90% of the city was leveled.[2] Countries in the post-war period worked to obtain their own nuclear weapons. By the middle of the 20th century, many military experts and political leaders feared a proliferation

Major Terrence S. Allen is an Airborne Warning And Control System pilot currently assigned to School of Advanced Air and Space Studies at Maxwell Air Force Base. He earned his Masters in Military Operational Art and Science, and deployed multiple times in the U.S. Central Command area of operations.

of nuclear weapons throughout the world, with many countries crossing the threshold from nuclear research for peaceful purposes into military uses.[3] By the 1960s, twenty-one countries had already agreed to limit their pursuit of nuclear military weapons through the Treaty of Tlatelolco.[4] And to limit the spread of nuclear weapons throughout the world, the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) was initiated. At the time of the treaty, only five countries possessed nuclear weapons; the United States, Soviet Union, United Kingdom, France and China. It was clear to many at the time, that without a good framework to limit the pursuit of nuclear weapons, many other countries would cross the nuclear military threshold; a serious danger to the civilized world. The NPT continues through today with most countries adhering to the rules. A similar framework to what gained international agreement on the use and proliferation of nuclear weapons could work for an agreement on strategic OCO. Further, it is very much needed as soon as possible before individual nation states develop their own definitions and normalize OCO weapon use, allowing by default the cyber domain to become similar to the wild west of the U.S. during the 1800s.

A Change in Warfare: Strategic Offensive Cyberspace Operations

Cyber, like nuclear weapons, has changed the nature of war; but, the question is do individual countries as well as the international community view cyber as an emerging phenomenon, or do they recognize it is already here? The SysAdmin, Audit, Network and Security (SANS) Institute points out, "in this digital age warfare is no longer limited to military versus military engagements. In the cyber-world, a digital enemy can bypass our military and take down what is near and dear to us. Destroying critical national infrastructure such as automated power plants, stock markets, and transportation systems could disable this nation without firing a shot."[5] OCO has forced a new paradigm of warfare. Nations failing to develop cyber capabilities will find themselves strategically behind other countries. Future developments will shift how current military strategists envision the future use of cyber, and make no mistake, it will be used. Nations must invest the time and resources to develop thoughts on those future uses so as to create defensive strategic cyber weapons and strategies to deter attacks. The growing interconnectedness of civilian and military use of cyberspace makes this essential.

[Offensive Cyberspace Operations - OCO] has forced a new paradigm of warfare.

An article published by the SANS Institute in 2004 noted that due to the great advances in information and communications technology, there is an unprecedented impact of cyber on our society. Much of our civilian and military life is dependent upon the cyberspace realm. National infrastructure, transportation systems, government sectors, and many other private and public companies rely heavily on computers and networks systems.[6] Thirteen years after this article was published, nations are even more dependent on technology for everyday life. The necessity for technology is not slowing down, but growing faster. Now, with more devices being "connected" that make life easier for so many, the effects of a cyber-attack are more wide ranging. An attack on one part of the system would have a significant impact on the daily lives of many. For one example look at the targeting of a utility business. An attacker targets the power plant and shuts down integral components. If this plant is the only power source for an area, then this area is without power. If this situation continues, the effects begin to grow from inconvenience and loss of monetary transactions, to potential loss of life if the attack is not repealed. A clear and coherent strategy communicated to adversaries, both nation-states and criminal organizations, is vital to dissuading attacks where the second and third order effects are against non-combatants. This messaging is critical to a complete deterrence strategy implemented by nation states.

...discovering the true motivations ...and understanding if the attacks are state sponsored...are key to determining the appropriate response by the attacked nation.

Cheap Form of Attack

Though cyber warfare could disrupt a large portion of a community with the push of a button, it is different from nuclear weapons. Unlike the technological requirements to employ nuclear weapons, anyone with access to a computer and hacking tools can become a cyber attacker. If one does not possess the knowledge to conduct sophisticated cyber-attacks, they could look for disgruntled programmers who want to sell their abilities to another buyer.[7] Due to the relatively cheap nature of conducting an attack, this is an affordable way for various groups with different motivations and other non-state actors to wage "war" against a technologically dependent nation. This includes criminals seeking money, cyber terrorists who are fighting on behalf of religious or cultural ideals, corporate espionage, employees who are looking to embarrass their company, and hackers who are looking to simply test out new tools for hacking other entities.[8] While the results of cyberattacks are often similar, the motivations of the various attackers may vary greatly. Thus discovering the true motivations behind the attackers and understanding if the attacks are state sponsored, or even state conducted, are key to determining the appropriate response by the attacked nation.

Cybercrime vs. Cyberwar

Two examples demonstrate the difficulty in distinguishing between cybercrime and cyberwar. And the ease of the attacks increase the chance future attacks will be mischaracterized as enemy OCO, leading to unintended escalations. In 2013, the Associated Press (AP) Twitter account was hacked. A false narrative appeared which claimed there were two explosions at the White House and President Obama was injured. This sent stock markets spiraling and $136 million dollars were temporarily lost. The AP got control back of their twitter account within 30 minutes, but the damage was done. Eventually, the stock market made the money back.[9] Was this hack attack a cybercrime or was it cyberwar? The hack was eventually traced back to the "Syrian Electronic Army, which backs but is not officially sponsored by the Syrian government."[10] Real damage was done, though temporarily, so did this rise to the level of a state sponsored cyberwar and thus warrant a military response?

The second example closely aligns with espionage, but was conducted in concert with kinetic military actions - the Russian cyberwar against Ukraine. Attacks on Ukrainian networks targeted classified intelligence, to include the number of troops in reconnaissance battalions and types of equipment used. After the initial cyberattack, the same organization changed their code and got back into the Ukrainian systems. After a cease-fire of kinetic military operations was negotiated the cyberattacks stopped.[11] Does this mean the cyber organization within Russia considered their actions attacks, since they stopped after the government agreed cease-fire was negotiated? Also, since the cease-fire saw a stop to the cyberattacks, this seems to indicate there was control by Russia over the cyberattack groups, enough so that even if they were not government sanctioned, the government got them to stop at the same time as the cease-fire. Was this a cybercrime stealing information or was this cyberwar? These examples illustrate the difficulty in classifying future cyberattacks because there is no clearly articulated, commonly accepted, and internationally agreed to, definitions as to what defines a cybercrime versus cyberwar.

Proportionality, Indiscriminate Attacks, and Unintended Consequences

When nuclear weapons were first developed, they were not precision guided munitions. Today, the technology exists for kinetic weapons to accurately hit targets and reasonably limit collateral damage. However, cyber cannot be used like a precision guided munition. One cannot always correctly identify the effects of the weapon and see the collateral damage. As noted by Davis, "cyber war is not in the same league as a nuclear war or even kinetic war with precision weapons in so far as "assuring" anything, much less long-term incapacitation or distraction. Collateral effects and related confusion are likely."[12] This leads to a problem of determining if the cyber-attack crosses the line of an indiscriminate attack. For example, if a virus were used against a network, the virus would be coded to attack specific items. However, the virus could spread further than desired. The U.S. and other nations attempt to limit conventional military effects to combatants. When a weapon misses the target, the international community gets involved with discussions on the reasons non-combatants were affected. Is using a cyber weapon which unintentionally affects civilians considered the same as a kinetic weapon which misses the intended target or causes collateral damage? Does this make the US guilty of indiscriminate attacks? Due to the connected nature of many nations and individuals, it is difficult to conduct a large cyber-attack without affecting non-combatant civilians. The original target maybe hit but the second and third order effects may spread out further than intended. If a country retaliates via OCO weapons, proportionality must be considered. Proportionality looks at legally deciding if "attacks are prohibited if they cause incidental loss of civilian life, injury to civilians, or damage to civilian objects that is excessive in relation to the anticipated concrete and direct military advantage of the attack."[13] Cyber has unintended consequences when used in an offensive capacity. Like nuclear weapons, potential effects of strategic OCO weapons are not guaranteed to be limited to just military targets.

Cyber has unintended consequences when used in an offensive capacity.

Deterrence

Paul K. Davis wrote "deterrence by itself is a fragile basis for strategic thinking."[14] He also stated that "hoping for a deterrent with today's reality would be like grasping for straws. Deterrent measures should definitely be part of a larger strategy, but the focus should be elsewhere."[15] Because cyber war is cheap to fund and can be conducted by many differently motivated groups, deterrence similar to MAD is not a viable option, as it was for nuclear weapons. Unlike nuclear weapons, the offensive capability of cyber is not limited to nation states. Any individual or group can go to a store, buy a computer, look on the internet for basic hacking tools, and begin practicing from any computer connected to the internet. Cyber deterrence is not just against another nation, but an entire spectrum to include criminal organizations, hackers, and state-sponsored groups. This is a major reason why a singular deterrent policy would suffer across the cyber spectrum. The technology exists to spoof one's actual location and make it seem you are somewhere else. This creates problems when trying to attribute blame for the attack.[16] If you cannot accurately figure out who did it and why, you struggle to fight against it. The enemy becomes ill defined. By the time countries figure out where the attack originated, the damage may be done and any action taken will be too late for effective or timely retaliation. A future deterrence policy must be flexible enough to deal with all actors and the varied motivations.

A future deterrence policy must be flexible enough to deal with all actors and the varied motivations.

U.S. Department of State

In March 2016, the State Department published their International Cyberspace Policy Strategy. This strategy is based on "implementing the President's International Strategy and reflects three themes: the applicability of international law; the importance of promoting confidence building measures; and, the significant progress the Department has made…to promote international norms of state behavior in cyberspace."[17] These themes are, and have been, worked into diplomatic discussions with foreign nations. In 2015, the U.S. State Department secured the "G20 Leaders' commitments to affirm the applicability of international law to state behavior in cyberspace."[18] This commitment also endorsed norms of behaviors states should abide by.[19] These same commitments are part of the ongoing effort by the State Department to gain trust and voluntary buy-in from nations across the globe on additional measures.[20] It must be noted these future commitments are voluntary with risk being pushed aside until the next large global event. Much like 9/11 changed the nature of U.S. military commitments, the next event could set in motion a chain of events which cause any agreements not formalized in treaty or law to easily be discarded and new rules established. Credit is due to the U.S. for beginning to lay the framework of cyber stability as risks are highlighted by states employing cyber capabilities.[21] However, there is still much work needed to gain formalized treaties and write new international law. These efforts must continue in earnest until such a time as the international community comes to an agreement with respect to the entire span of cyber actions and actors. Nations using loopholes and new ways of getting around the agreements and letter of the law must be anticipated and expected. Formalized agreements with clear language are the best way to hold nation states accountable within the international community for offensive acts conducted in the cyber domain. Such agreements will deter other nations from engaging in the cyber domain as punishments will be articulated and actors can weigh the cost-benefit of using OCO weapons.

Conclusion

Cyberwarfare was not introduced to the world like the nuclear bomb, rather it has been gradually tested and its usage increased by organizations seeking to gain advantage over their adversaries. Though the potential strategic destructive power (predominantly temporary in nature) is similar to nuclear weapons with respect to a large area affected instantaneously, a deterrence strategy like MAD will not work due to the wide range of entities capable of conducting cyber-attacks. The U.S. deterrence strategy needs to be flexible enough to detract criminal organizations through judicial punishments, as well as state actors through sanctions ranging from economic to military action. There needs to be a defined and clearly articulated response if the U.S. were attacked by a nation state, providing other states an expectation of the level of retaliation. Something akin to the escalation ladder concept used after World War II would work. This prevents an either/or situation, where if you don't act at all, your military credibility is damaged. A wide range of options allows a measured response to demonstrate the resolve to protect national interests, based on who and where the threat is coming from. The flexibility of an escalation ladder concept communicates to other nations they are on the ladder, on a path to larger conflict and gives them an opportunity to stop their actions before facing a greater response from the U.S. Additionally, any future treaty for cyberwar should use some principles of the proposal put forth by Richard A. Clark and Robert Knake, and include imposing a ban on first use cyber-attacks against civilian infrastructure. This ban would be in place only during times of peacetime operations. If two nations were to go to war, either a cyber war or a conventional shooting war, this ban would then be lifted.[22] The merits of this proposal lay a foundation for nations to have a common agreement pertaining to what is acceptable with the use of cyber-attacks against another nation, protects non-combatants, and prevents indiscriminate attacks, whether intentional or not.

Further, the international community needs to define what constitutes cybercrime and cyberwar in order for countries to develop clear strategies for OCO and deterrence. One cannot deter what is not defined! The definitions should start with the motivation of the group conducting the attack as well as the intended purpose of the attack, then build out from there. These definitions allow countries to seek appropriate justice within the international community rather than try and retaliate on their own. Pressure brought from the international community has the potential to do more to hold renegade actors in check and keep wars from beginning. These actions will allow the U.S. to more effectively deter cyberattacks and get ahead of nations who already employ cyber without regard to international norms. The U.S. must articulate a clear deterrence strategy in the cyber domain and lead the international community to an acceptable treaty signed by all nations limiting OCO against civilian targets. ***IAJ***

NOTES

[1] *The Columbia Encyclopedia*, 6th ed., s.v. "Nagasaki," http://www.encyclopedia.com/places/asia/japanese-political-geography/hiroshima#1E1Hiroshim (accessed 26 March 2017).

[2] *The Columbia Encyclopedia*, 6th ed., s.v. "Hiroshima," http://www.encyclopedia.com/places/asia/japanese-political-geography/hiroshima#1E1Hiroshim (accessed 26 March 2017).

[3] Nobel Media, "The Development and Proliferation of Nuclear Weapons," *Nobelprize.org* (2014). http://www.nobelprize.org/educational/peace/nuclear_weapons/readmore.html (Accessed 26 March 2017).

[4] Ibid.

[5] SANS Institute, "Information Warfare: Cyber Warfare Is the Future Warfare," *Global Information Assurance Certification Practical Repository* (2004). https://www.giac.org/paper/gsec/3873/information-warfare-cyber-warfare-future-warfare/106165 (accessed 26 March 2017).

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Max Fisher, "Syrian Hackers Claim Ap Hack That Tipped Stock Market by $136 Billion. Is It Terrorism?," The Washington Post, April 23, 2013, https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.7d6e08abb0aa (accessed 26 March 2017).

[10] Ibid.

[11] Aarti Shahani, "Report: To Aid Combat, Russia Wages Cyberwar Against Ukraine," NPR, April 28, 2015, http://www.npr.org/sections/alltechconsidered/2015/04/28/402678116/report-to-aid-combat-russia-wages-cyberwar-against-ukraine (accessed 26 March 2017).

[12] Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," *New York University Journal of International Law and Politics* 47, no. 2 (Winter 2014): 327-355. http://nyujilp.org/wp-content/uploads/2015/11/NYI203.pdf (accessed 26 March 2017).

[13] Horst Fischer, "Proportionality, Principle Of," Crimes of War, 2011, http://www.crimesofwar.org/a-z-guide/proportionality-principle-of/ (accessed 26 March 2017).

[14] Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," *New York University Journal of International Law and Politics* 47, no. 2 (Winter 2014): 327-355. http://nyujilp.org/wp-content/uploads/2015/11/NYI203.pdf (accessed 26 March 2017).

[15] Ibid.

[16] Ibid.

[17] U.S. Department of State, *International Cyberspace Policy Strategy*, 2016: 1-24. https://www.state.gov/documents/organization/255732.pdf

[18] Ibid.

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," *New York University Journal of International Law and Politics* 47, no. 2 (Winter 2014): 327-355. http://nyujilp.org/wp-content/uploads/2015/11/NYI203.pdf (accessed 26 March 2017).

Interagency Leadership

Many of the meaningful results that the federal government seeks to achieve, such as those related to protecting food and agriculture and providing homeland security, require the coordinated efforts of more than one federal agency, level of government, or sector.

— U.S. Government Accountability Office[1]

Editor's Note: This article is designed to provide an introduction and best practices in leading interagency groups, so that readers can benefit from the firsthand experiences of the author as he participated in and led such activities at the highest levels within the federal government.

by Duane M. Blackburn

After they have proven themselves within their own organizations and find themselves working on a priority topic, federal employees will likely lead an interagency team. Unfortunately, the behaviors and mindset that have made them and their team members successful within their agency are often quite different from what is required for success within an interagency setting. This article provides insights on leading interagency activities that will help lessen the learning curve for these individuals.

The federal government is a collection of stovepipes, formally created to focus attention on a group of activities that must be coordinated to meet a specific need. Each stovepipe has its own formal rules and informal processes that were developed to ensure that the stovepipe operates with little deviation and delivers consistent results. The stovepipe's stakeholders (e.g., parent agencies and departments, the White House, Congress, and impacted constituencies) value this consistency and often resist alternative approaches or activities that upset the status quo.

The need for interagency coordination occurs because these stovepipes are quite often stovepipes in practice but not in reality. Many operational issues are not constrained within the sole control of a single agency, and most science and technology initiatives benefit from leveraging multiple perspectives. Interagency activities are established when the need for coordination outweighs the

Duane M. Blackburn is a science and technology policy analyst with the MITRE Corporation. He served as the assistant director for Identity Management and Homeland Security in the White House Office of Science and Technology Policy from 2004-2011, where he led multiple subcommittees within the National Science and Technology Council and participated in numerous entities within the Homeland and National Security Councils.

inherent pain of implementing that coordination.

A natural conflict will quickly manifest among many individuals on a new interagency team, and the interagency leader must recognize this conflict. These members attained their senior status within their own organizations and gained the trust of their superiors largely because they ensured their stovepipes' consistency. They know the ins and outs of what they are supposed to do and how to get things done within their organizations. Upon joining an interagency team, these leaders are entering an unknown working environment, often with the task of redesigning their stovepipe's existing approach. Some may take this as an invigorating opportunity to be innovative. Many, however, will be shell-shocked because they are unsure of how to be successful on an interagency team that functions differently from others they have experienced in the past. Some may also be hostile to any concept that leads to a change in their stovepipe's existing processes or plans.

A natural conflict will quickly manifest among many individuals on a new interagency team, and the interagency leader must recognize this conflict.

The challenge for the interagency team leader is to understand these internal conflicts and overcome them. The leader must ensure that team members arrive at the same understanding—that each of their organization's best chance of future success is to follow the path developed by the interagency team. Team members must become champions of change within their own stovepipes to achieve an interagency-developed outcome. That is not an easy transition to make, and it can often take considerable time and effort to achieve. There is also no single "best practice" path to success, as each interagency endeavor is unique. Still, leveraging the following three concepts can provide a starting point:

1. Provide overall leadership of the team and encourage team members to lead aspects of the interagency activities themselves. This is not only a force multiplier, but also encourages individual team members to take ownership of the group's success.

2. Treat the interagency team as a change-management initiative. After all, the team was created to change existing approaches within the stovepipes. Using change-management methods can help consolidate the interagency team, as well as provide examples and experiences that individual team members can leverage within their own stovepipes.

3. Allow the interagency team to evolve over time. It is very rare for an interagency activity to devise and implement massive changes in one step. Meaningful change is usually an evolution that takes time. The interagency team must similarly evolve, in both its activities and its membership, to guide and support this evolution. Interagency leaders must have a dual focus of ensuring success on the team's current initiatives, while also looking ahead to what the team will need to do next, and bringing those experts on to the team in advance.

Interagency Leadership versus Interagency Management

The fundamental concept of leading an interagency team requires that the individual recognize that he or she is providing interagency leadership rather than interagency management. There are significant differences between management and leadership:

- Management involves directing people through existing processes to ensure they meet previously set expectations.

- Leadership involves inducing individuals to think outside their typical experiences about how to achieve greater successes in a different way.

Individuals who approach leading interagency teams with a management mindset fail for at least two reasons. First, a management mindset is a surefire way to kill the collective collegiality that is required for an interagency team to succeed. Team members come to an initiative with marching orders from their home organizations. Simply telling them to abandon those orders and do something else instead will be viewed by most as a non-starter. While this dynamic is rare in ad hoc interagency teams of peers, it has historically occurred too often in formal, White House-led activities in which politically-connected but inexperienced staffers misread their power and influence. Second, the management mindset can inhibit the creation of just the kind of innovative approaches that interagency teams require to accomplish their primary objectives. The management mindset practically creates a mandate for a pre-determined approach, with the manager ignoring the fact that the approach he or she has selected may not be optimal, or even possible, for the other team members.

Another key factor in leadership is recognizing that leadership can come from anyone on the team. While one individual is usually designated as the interagency team lead, teams usually achieve more when they encourage multiple members of the team to exert leadership. Interagency team leads should set the end-goal and define the boundaries of permissible activities to ensure the team is focused on reaching the same desired outcome. After that is established, the team lead can shift to a servant-leadership model in which the leader focuses on helping the team succeed, with multiple team members exerting thought-leadership and coordinating lower-level activities that advance the team toward the end-goal. This model not only inspires innovation, but also a sense of personal ownership of the team's success, both of which are required for the interagency team to succeed.

...the management mindset can inhibit the creation of just the kind of innovative approaches that interagency teams require...

Finally, the interagency team lead is responsible for taking and managing risks but in a different sense than the government norm. Within team members' individual stovepipes, risk management often involves issues such as cost, schedule, and communication—things that must be managed for a project to be successful. Risk in an interagency context is completely different. Here, the interagency team is investigating alternative approaches and trying to decide if adopting one is worth the risk to the team as a whole and to the individuals who may be upsetting their home agency's apple cart. The stovepipe agencies may feel the changes being proposed will increase their own risk. This pushback cannot be overcome by management fiat; rather, each team member must exert leadership to convince his or her agency of the benefits of the change. The interagency leader must be continuously mindful of this need by allowing feedback into interagency plans and activities, as well as doing whatever possible to support team members during moments of discord with their home stovepipes.

Interagency Leadership Is a Change-Management Initiative

The government creates an interagency team when it recognizes the existing individual approaches of agencies are not working well and a greater outcome could be achieved through collaboration. First, the mindset of interagency team members must be changed to think of the problem in a fundamentally new way, and they, in turn, must act to change their organizations' processes and plans to support the larger plans developed by the interagency team. That is a lot of change and why it is important to think of interagency team leadership as a change-management initiative.

...it is important to think of interagency team leadership as a change-management initiative.

John Kotter, a well-respected thought leader in the field of change management, provides eight steps to transform an organization:[2]

- Establish a sense of urgency.
- Create the guiding coalition.
- Develop a vision and strategy.
- Communicate the change vision.
- Empower employees for broad-based action.
- Generate short-term wins.
- Consolidate gains and producing more change.
- Anchor new approaches in the culture.

With a little creative adjustment of Kotter's message on each point (as his work focuses on changing a private-sector corporation), these steps constitute a good recipe for leading change within an interagency activity.

Establish a sense of urgency

Emphasize why the interagency team was created in the initial meeting invitation and reinforce it in the first few meetings: "What's the need? What's the justification for doing it now? What's the anticipated repercussions if we don't? What's the expected outcome from our collaborative work?" Interagency teams may be chartered to pursue efficiency, to achieve some overarching mission, or simply to afford individual agencies the opportunity to coordinate to ensure the success of all. The justification and goals for creating the team should be explained so that everyone understands the intended outcome and why it is important, both collectively and individually. Knowing the purpose ahead of time helps the individual organizations identify the proper representatives to send to the team, as well as to prioritize the effort properly within their own large list of demands.

Create the guiding coalition

An interagency team must have the proper membership to meet its goals. All directly-impacted agencies should have a seat at the table, of course, but it is also important to consider second- and third-order effects of potential decisions. How will the implemented changes impact other agencies, and should they be included in the team? If so, how do you deal with having primary and secondary team members? Similar questions arise when you consider the extent to which agency stakeholders, such as the Office of Management and Budget (OMB), should be involved. Once agency membership is determined, agencies will want to choose people who can properly represent their interests within the interagency group. The interagency team lead needs individuals who have enough clout within their home agencies to return to those agencies with the outcomes of the team's work and make the changes necessary to meet the new obligations. The interagency team lead also should analyze the backgrounds of the assigned team representatives and ensure that their collective backgrounds and experiences can properly support the team's work.

Develop a vision and strategy

The convener of the interagency team (and/or the interagency team lead) will have created the team with a desired outcome in mind, but that should be just a starting point for creating the team's vision. The team lead must ensure that each team member views the success of the interagency group as critical to his or her own stovepipe's success. The first step in achieving that state occurs as the group fine tunes its overall goal and decides how the group will work toward that goal. Sometimes this step takes a painfully long time to work out, but interagency teams will not succeed without reaching consensus.

Communicating the change vision

Once the interagency team develops a clear vision, the lead must consistently reinforce the message to keep the team on track. In addition, the vision must be effectively communicated outside the interagency team. The management of each member agency should understand the team's vision, how it impacts them, and how they will be expected to support it. This message should be individually tailored by each team member to take back to their agency to ensure that their management supports the vision. To some team members, this communication will come naturally, to others it may not, and a few will even be hesitant to stir the waters at home by sharing much of anything. The interagency team lead will need to reinforce the importance of this communication and ensure that it occurs.

Empower employees for broad-based action (or Empower others to act on the vision)

At this stage, the team begins to take action. Usually such action is a mixture of formally-planned activities combined with individual initiatives, though most interagency teams focus on the former. While formally-planned activities are often required to overcome the team's most complex hurdles, individual initiatives can also be beneficial as they support each team member's sense of ownership of the team's success, while simultaneously encouraging innovative ideas. As long as individual initiatives support the vision and do not negatively impact formally-planned activities, interagency teams should strongly encourage them.

> **The team lead must ensure that each team member views the success of the interagency group as critical to his or her own stovepipe's success.**

Generate short-term wins

Short-term wins are beneficial in most activities but are especially beneficial within interagency teams. Interagency work requires overcoming a daunting number of obstacles. Wins provide positive reinforcements that encourage team members to keep moving forward. They are important tools for the interagency team lead, who should constantly look for potential "wins" to highlight. These wins should be celebrated by the team, and the interagency team lead should recognize the leader's effort.

Consolidate gains and produce more change

While celebrating wins is important, it is even more important to use the momentum created by the short-term wins to take on bigger and more complex issues. Wins not only create a sense of excitement and accomplishment, but also help to overcome skeptics and to open everyone's eyes to potential outcomes that had previously seemed unattainable. Existing team members become more willing to invest their resources once they experience some successful outcomes. Outsiders may also want to join the team after witnessing its success. The interagency team lead should use these wins as prime opportunities to tell individual agencies, stakeholders, and third parties about the significance of the win, the nature of the next hurdle and the team's intended approach, and how the win and the next hurdle are steps toward fulfilling the team's ultimate vision.

Without nurturing, successful interagency outcomes are often short-lived, and the stove-piped organizations revert to their prior ways.

Anchor new approaches in the culture

The federal government and its processes are monolithic beasts— large, powerful, and intractable. Presidents and Congress, with all their available powers, have difficulty modifying federal government practices. Without nurturing, successful interagency outcomes are often short-lived, and the stove-piped organizations revert to their prior ways. Team members must therefore work to institutionalize the new approaches as their organizations' new normal culture. This institutionalization will be a long-term and laborious process for most team members, and the interagency team lead must keep the pressure on these individuals to persist in this uncomfortable undertaking while simultaneously driving the team to tackle its next hurdle. Successful institutionalization within each stovepipe should be celebrated and lessons-learned shared so that others may benefit from their experiences.

The Evolution of Interagency Teams

Occasionally an interagency team is created to overcome a simple hurdle; thus, it accomplishes its goal and then disbands. More often, however, interagency teams persist because the end state to which they aspire requires a significant amount of work to reach. In these cases, it is necessary to consider how interagency teams evolve over time, tackling increasingly difficult tasks on their way to their ultimate outcome. Using wins as a springboard to start working on harder tasks is a key part of continuing a team's work; however, there are times when a fundamental rethinking of the team's focus, structure, and messaging is required.

Consider, for example, the 10-year lifecycle of the National Science and Technology Council's Subcommittee on Biometrics and Identity Management. It grew organically out of multiple agencies providing guidance to the Federal Aviation Administration immediately after the 9/11 terrorist attacks, evolved into a formally-chartered, interagency team led by the White House, and survived an administration transition when the presidency changed political parties.

The size, membership, and activities of this Subcommittee changed considerably during its existence, but it maintained one overarching goal: to provide a foundation for the nation's screening capabilities through proper application of identity technologies, while protecting the privacy and civil liberties that make our nation strong.

Most interagency teams will not endure for as long as this Subcommittee has, and few will need to evolve in a similar manner. The common concept is that interagency teams that do not evolve will be unable to tackle more complex hurdles and are doomed to a stationary status with no chance of meeting their ultimate objective. Overcoming future, more complex hurdles often requires more formality within the interagency team as well.

The Subcommittee above, which originated as an ad hoc group but evolved into a formally-chartered organization. happened because the team and political leaders recognized that doing so was necessary for the team to meet its objectives. Once the team met those objectives that required White House-level support, its formality devolved back into an ad hoc nature. The group continues to meet and collaborate to this day, even though its stature and influence is significantly smaller than in its heyday.

There are many potential forms an interagency team can take on the path from isolated work to formal White House collaboration. What follows is a list of these potential states, from least to most formal. The list is presented within five distinct groups of pseudo-likeness for additional analysis. Interagency team leads can assess their current state and upcoming hurdles and use this list to help them plan their team's future.

Group 0, Single Agency Focus

Within this group of states, there is no interagency coordination taking place. Individual activities are so stovepiped, there is little recognition that anyone else is working on the issue at all. Only one agency focuses on the issue.

- Multiple agencies focus on the issue, but mistakenly believe they are the only ones doing so.
- Multiple agencies focus on the issue and are vaguely aware that others are doing so as well, but have no interest in information sharing or collaboration.

Group 1, Interagency Enlightenment

Within this group of activities, stovepipes realize they are not alone and begin talking with their peers. This is usually done on an ad hoc basis, but an occasional memorandum of understanding will formalize the data exchange.

- Two or more agencies exchange information and ideas irregularly.
- Two agencies decide to work on small projects in a bilateral fashion.
- One or two agencies realizes the need for and benefit of including other agencies in their developmental plans.
- Multiple agencies exchange information and ideas regularly.

There are many potential forms an interagency team can take on the path from isolated work to formal White House collaboration.

Group 2, Interagency Cooperation

Within this group of activities, organizations begin to shift from coordination to formal collaboration via jointly funded projects. Stovepipes begin to see beneficial outcomes from joint efforts and begin to question the wisdom of doing whatever they want without their peers' influence.

- One-time workshop (over one or more days) that results in a better understanding of the community's players; the effect is transient.
- Multiple agencies start collaborating on small, single-year projects sporadically with some management visibility; there is purposeful transience.
- Multiple agencies collaborate on small projects regularly with some management visibility.
- Multiple agencies recognize that a more difficult problem exists and determine how they can address it jointly.
- Multiple agencies separately work projects that are loosely tied together, with periodic interagency meetings to discuss individually and in aggregate.
- Multiple agencies collaborate on medium-sized, multi-year projects regularly with ongoing management visibility.

Group 3, Fertilization of Collaboration

Within this group of activities, an organization's activities and decisions are heavily influenced by the work and thinking of outsiders. That can be quite upsetting to individual stovepipes, which place a premium on self-control and consistency. The stovepipe's management will thus become much more interested and involved in external collaboration. Each organization begins to see impacts from joint work that outpaces what it can accomplish on its own, and the enhanced visibility of the work leads to greater management and policy-level oversight.

- Agency leadership (management) determines that more formal coordination and higher visibility is necessary to meet needs. Media or Congress may be fanning interest, and the group wants to seize that attention as an opportunity to advance capabilities.
- Multiple agencies routinely perform activities individually as components of a joint body that does not have the charter to press for genuine collaboration.
- Management within multiple agencies recognizes the existence of critical needs that cannot realistically be met by their agencies alone.
- Multiple agencies informally identify and prioritize needs so that plans to address them can be developed.

Group 4, Interagency Collaboration

Within this group of activities, an organization's activities are driven largely by interagency planning and consensus. Each stovepipe's leadership and stakeholders views its alignment with and support of interagency plans as critical to the its own success. The higher visibility and need can lead to enhanced appropriations funding, and activities at the interagency and individual stovepipe levels come under enhanced scrutiny by political leadership within agencies and the White House.

- Multiple agencies routinely work jointly with others.
- Formal agreements to work collaboratively are developed.
- The interagency group performs a formal analysis and prioritization of interagency needs.
- Multiple agencies identify best practices for overcoming the priority needs and work to address them collectively.

Group 5, Formal Interagency Collaboration

Within this group of activities, the administration views the work of the interagency team as critical to meeting its priority objectives and, as such, formally charters the group within the structure of an Executive Office of the President (EOP)-level interagency body. Funding and other resources necessary for the interagency team to succeed are much easier to obtain, but plans undergo significant scrutiny and must be approved by the EOP. Individual organizations are expected to fully support interagency activities and will see significant budget and authority restrictions if they fail to do so.

- An administration-wide strategy for prioritizing and overcoming the critical needs is produced.
- The strategy becomes a focus for OMB during an agency's budget preparation.
- OMB examiners begin to study the strategy and budget plans from an interagency perspective.
- A formal, staffed office is created to help

foster interagency planning, budgets, and activities.

- OMB performs a "cross-cut" analysis of agency budgets to ensure precise alignment with the strategy.

Conclusion

Establishing and leading an interagency team is one of the most complex and rewarding tasks that a federal employee could undertake throughout his or her career. Success depends on having a different mindset than is typically required for senior federal managers, along with a willingness to continuously evolve the team itself. In conclusion, the most important overarching principles to keep in mind to achieve success are:

- Lead the team and encourage others on the team to do so as well.
- Interagency teams often exist as change-management initiatives, so treat them as such.
- Teams must evolve to succeed. Use your "wins" as springboards and strategically plan future activities so that outcomes are achieved with as little extra pain as possible.
- For an interagency group to succeed, its members must take ownership of the group's success, perceiving it as necessary for each stovepipe's success. ***IAJ***

NOTES

[1] United States Government Accountability Office, GAO-14-220, "Managing for Results: Implementation Approaches Used to Enhance Collaboration in Interagency Groups," Washington, DC, February 14, 2014.

[2] John P. Kotter, *Leading Change*, Harvard Business Review Press, Boston, MA, 2012.

The End of Operational Phases at Last

by Gustav A. Otto

Operational phases are a way many in the military and Department of Defense (DoD) think about going to war. Joint Publication (JP) 3-0, *Joint Operations* describes phases zero through five (0-V) and calls them "notional operational plan phases."[1] JP 5-0, *Joint Operation Planning* further describes the phases and their notional application. These operational phases were originally intended to help frame or construct planning. Sadly, to the detriment of U.S. national security, they became the milestones by which entire organizations, from the tactical through the strategic, drove activities. After 25 years of planning, participating, and evaluating the operational phases of military effort in the U.S. government, military leadership is not meeting the needs of the decisionmakers who lead the Armed Forces. And worse, these phases are adopted by other agencies and departments who suffer severe outcomes because the phases are not used properly.

The well-intentioned concept was poorly understood in the first place, then it was poorly implemented, and eventually became a cookie-cutter for planning activities. In the process, the concept unintentionally neutered the deliberate art and science of planning, and it continues to undermine both creative and critical thought. Notional operational plan phases cannot address the layers and levels of complexity in any environment. The erosion of the operational level of war and a growing and inextricable direct link between the strategic and the tactical (or direct) levels are other reasons the phased approach fails. The operational level of war may quickly be coming to an end, and though this is not the primary point of this article, it is an important premise. The combined and linear fashion of the levels of war and operational phases result in a race to the lowest common denominator and the prettiest slide, rather than any good solutions.

Gustav A. Otto was the first Defense Intelligence Agency representative to the Army Combined Arms Center, and Defense Intelligence Chair at the U.S. Army Command and General Staff College. A career human and counterintelligence officer, Otto instructed and advised faculty and students, emphasizing the importance of collaboration across government, industry, and academia.

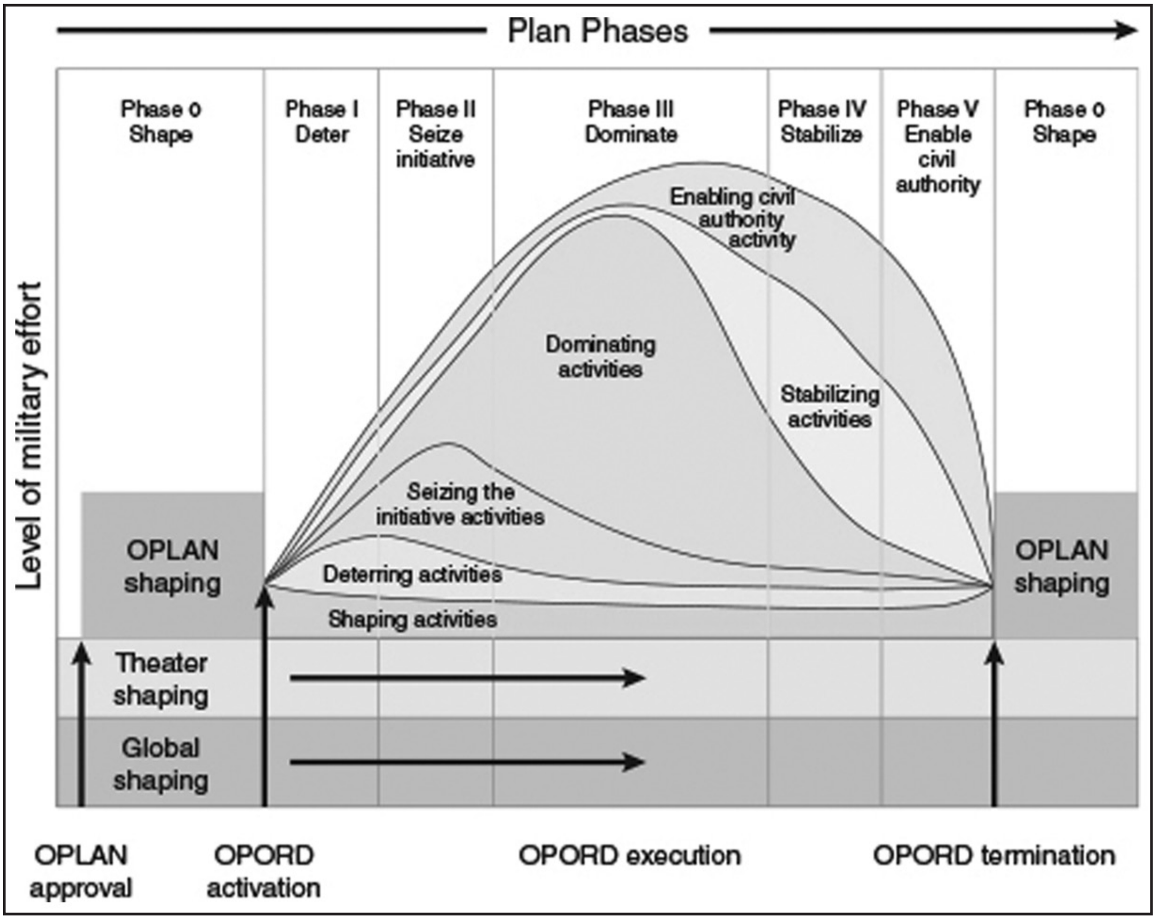


Figure 1. Phases of a notional operation plan versus level of military effort. OPLAN, operation plan; OPORD, operation order. *SOURCE: JCS (2011)*.

Figure 1 is included to orient the reader of the phases. Along the vertical axis is the level of military planning and execution of any specific or even notional plan. The horizontal axis suggests a degree of activity or work done by the military. This graphic is well-understood by staff officers across the DoD, and each phase and level of effort carries a correlated textual description, as well as notional outcomes, activities, and checklists. There are precious few, thoughtful measures of effectiveness, measures of success, or desired outcomes or results linked to these. A dyed-in-the-wool planner wedded to the phases will counter that a good plan will not have those until the plan is developed. These notional levels at best suggest a broad shift in the type of work to be done by the military during a particular phase. As a planning construct, particularly from a design-thinking perspective, this makes good sense. Design thinking is introduced to staff officers and leaders from the time they achieve mid-level status throughout the rest of their careers. Further, a good plan will start with a hearty discussion about the ways, ends, and means associated with the area or topic of discussion. Only when an end or set of ends or outcomes is established should planning begin. Only then, through deliberate design thinking, should it become an iterative approach between the ways, ends, and means.

The first shortcoming of this model is the gradual disappearance of the operational level of war. The explosive growth of communications and a globalized world finds even the youngest and most junior military person, U.S. government civilian, or even U.S. government contractor with the ability to affect global change at the lowest and most direct levels. This change was described by U.S. Marine General Krulak in 1999 when he introduced the concept of the "strategic corporal" and the "three-block war." This was the first of many bricks to pave over the increasingly-antiquated "tactical, operational, strategic" model.

...the "strategic corporal" is a seemingly, low-level person whose actions may shape large-scale events or have lasting repercussions.

Broadly, the "strategic corporal" is a seemingly, low-level person whose actions may shape large-scale events or have lasting repercussions. The negative version of this is easiest to see. For example, consider someone who seeks the intentional desecration of a holy text, mistreatment of a captive, or leaks secrets to the press. These low-level, tactical actions inordinately set back U.S. and international security by complicating already complex national security endeavors and impair international relations between established allies. These low-level actions also drive a massive shift in diplomacy, information activities, military affairs, and even the economy. Strategic leaders are put on the defensive because they are forced to react to an unplanned circumstance. Further, there is little discussion or relevancy of the operational level when these events occur, rather the tactical/direct event is so catastrophic it instantly transcends the operational and lands squarely in the laps of the strategic leaders. The "three-block war," Krulak cautioned, would find "U.S. Marines confronted by the entire spectrum of tactical challenges in the span of a few hours and within the space of three contiguous city blocks."[2] He goes on to warn: "The lines separating the levels of war, and distinguishing combatant from "non-combatant," will blur, and adversaries, confounded by our "conventional" superiority, will resort to asymmetrical means to redress the imbalance."[3]

A gifted future thinker, Krulak's predictions remain truer today and offer us much to consider for tomorrow. Yet the confusion of the operational phases and their purposes cloud thinking within the defense enterprise. For proof, look at any emerging or frozen conflict around the globe. From the Ukraine, to Syria, to Sudan, to Yemen, there is no shortage of fragile, failed, and failing states where a tactical event could catapult nations and other multinational actors into strategic engagements. Yet the military education system, policy, and doctrine-writing machines, along with their human resources systems for hiring, firing, retaining, and promoting remain woefully wedded to outdated models. It is for these reasons the "notional" is no longer present, and the less-than-discreet markers that exist between the levels of war and the phasing of operations are considered sacrosanct by so many in and out of uniform.

The military and DoD do some things incredibly well, especially grooming and growing leaders. Additionally, no one makes as deliberate, concerted, and well-developed approach to planning and leader development as the U.S. DoD. Service and DoD success is pursued by partners from around the globe, replicated by many across the U.S. government, and mimicked by select parts of the commercial world. However, the possible solutions are overshadowed or encumbered by this artificial phasing. For example, the phases and levels of effort are used in simulations, exercises, and scenarios across the departments. As a result, they are used like an anchor point diluting any real thought and hobbling any creative solutions. They serve as a milestone to nowhere or even the place you do not know how to leave (think Iraq).

They give a profound false sense of security both to lower echelons and to senior decisionmakers. Though I am not a fan of Clausewitz, even he recognizes the importance of the geometric challenges and complexity of warfare, the need for strategy to reflect "great spans of time and space [because] Armies do not burst from one theater of war into another; rather a projected strategic envelopment may easily take weeks and months to care out."[4]

Air-Land Doctrine may now be obsolete, and new and more accurate thinking for the contemporary age is emerging. Multi-Domain Battle (MDB) moves previous doctrines forward to better synchronize and integrate the many domains of a four-dimensional, "three-block war." The MDB approach recognizes the naturally-occurring chaos that may or will emerge and makes room for more complexity. Imagine how hard it is to apply the five phases of operational planning to the intricacies of a "three-block war." Now make it infinitely more complex by multiplying it by at least six domains. We quickly get to so many planning considerations that even in the most complex, analytic systems, human error will reign supreme. Trying to use the operational planning phases in this context risks over-simplification, at a minimum, and is counterproductive in many cases.

Worse, planners and operators are impaired by the notion that there will always be three options for a decisionmaker at any level. In these plans, the phases and levels are described in a narrative. Planners find and replace the old words with new words to describe the geographic area. The new magical solution lies in the new version. Then three probable courses of action are quickly developed; although, one is almost always deemed a "throw away." The distinction between the two remaining options is so vague or so minor the staff are content if either or a hybrid of the two remaining options are used. The lowest to the highest echelons remain within the restraints of these two linear models, usually with too few people who have or are practiced at deliberate planning or design thinking. A better than average leader will make marginal changes, whereas a great leader will send them back to the drawing board. Oversimplified? Maybe. It is not malicious on the part of the planners or decisionmakers. It is routinized. This is what most planners grew up with; it is what their mentors used, and they were told it worked. It got them promoted, and it got them to retirement. It was praised by seniors, so it must be right. Right? Fortunately, those same planners and decisionmakers are starting to emerge from their haze and delusion and realize they have had it wrong for some time, possibly since the end of the Cold War.

...planners and decisionmakers are starting to emerge from their haze and delusion and realize they have had it wrong for some time...

When learning to drive, did you always drive in a straight line and never turn, never stop, never parallel park? Of course not. This rudimentary example presents the same challenge as the use of operational phases. Their rigidity in conceptual thinking might offer ways to allow for synthesis, distillation, and reduction, if only these were encouraged and rewarded. As a cognitive approach to planning, it is and should be one of many ways to think about a problem. From a practical matter, you realize having a car without brakes, reverse gears, over-drive, and so much more may not be such a convenience. Likewise, the operational phases seek only to move forward in a largely monolithic fashion without finesse or elegance.

At some point, someone created the bell-like curves and colors to suggest many components of each phase are happening simultaneously.

They learned something from Krulak; yet, it is still layered, not integrated. It should be integrated and interdisciplinary. One looks at the macrocosm of a place such as Iraq or Afghanistan and says, "we're in Phase IV," when we are nowhere close. Even if we are in Phase III in both, they are different based on so many other factors. Clausewitz again teaches us: "The act of attack, particularly in strategy, is thus a constant alternation and combination of attack and defense." When operational phases are considered, they are broadly applied to a nation. Clausewitz cautions us that the "objective…need not be the whole country; it may be limited to a part—a province, a strip of territory, a fortress, and so forth."[5] This is an important point to make, and operational and strategic commanders and diplomats understand this. The challenge is encumbered by the antiquated and excessively-rigid planning process thanks to the routinized operational phases.

The use of operational phases for strategic-level planning clouds judgement and unnecessarily misrepresents a possible problem and set of solutions.

Defense planners around the globe use operational phases. Many of the planners looking at rogue nations, hard targets, or legacy adversaries develop a reflex for painting other countries and scenarios in their areas of responsibility with the same brushes used in operational phases. They look at a country or even a non-state actor and apply an inflexible mindset to a shifting and complex reality. This is especially true with emerging or simmering situations, often in fragile, failing, or failed countries. These judgements may be valid; yet, when overlaid with operational phases, there emerges only one clear answer: "We must move to Phase III and get boots on the ground because the other elements of government can't or aren't making it work." On the contrary, a fragile, failing, or failed state does not reflect a foreign policy failure by the U.S. or anyone else. It may reflect poor governance, rule of law, economy, or even natural resources. It could also mean a manmade or natural disaster, shouting for U.S. or the international community's intervention.

The operational phases inhibit the creative problem-solving the defense industry could provide. Their over-use and over-reliance drive military planning without allowing for sufficient development of rapport and collaboration among other U.S. agencies and departments. They assume there is a need for military intervention. The use of operational phases for strategic-level planning clouds judgement and unnecessarily misrepresents a possible problem and set of solutions. Often, when robustly and consistently consulted, the rest of government already had creative ideas and are implementing them in the field and around the world, which means there is always room for help and good ideas from DoD; however, there should be an awareness of mission creep toward Phase III. Just because a service member or defense civilian is tasked with developing a plan, does not mean operational phases are the right answers.

The following examples may help refine this point. In 2000, the status quo in Iraq between Saddam Hussein and the coalitions comprising military operation were largely static. The UN, several other intergovernmental organizations, several multinational corporations, and even many nongovernmental organizations were monitoring the activities in Iraq and were in some kind of dialogue with the Iraqi regime. In the year 2000, Iraq was Phase I and clearly not in Phase II. The 2008 Greek Recession, on the heels of the global recession, resulted in strained relations between Greece and its allies and trading partners in the West. Despite riots in the streets, use of domestic military force, and significant debt teetering on bankruptcy, this fragile (some argue failing) nation persists today. The U.S. never classified our foreign affairs in Greece during this period as anything but steady state (Phase 0). Since its independence from the United Kingdom in the early 1930s, Pakistan has struggled to maintain and advance its political sovereignty. Many scholars and politicians suggest it has teetered on the brink of being a fragile or failing state. Despite being a nuclear power, the sixth largest national population, and its strategic importance, the U.S. has never considered Pakistan as anything but a steady state, Phase 0 nation. To suggest moving to a Phase I or more active military situation in Pakistan would risk further unrest in the region. This kind of destabilization is not only unwanted, it would be unwise. The rise of Boko Haram in Nigeria and the terror this organization continues to afflict domestically and regionally has garnered the attention of the international media. Even after kidnapping hundreds of children, links to other global terrorism franchises, and continued mayhem, no Phase II emerged in Nigeria. Further, it does not currently represent an existential threat to the U.S., or even many (if any) of the countries in West Africa.

Critics of this position might argue this is because we are not at war in Greece or Nigeria; however, we were not at war in Iraq in 2000 either. If we are to commit to the operational phase notion, we should seek to remain perpetually in Phase 0. In fact, the State Department and most Ambassadors working for the U.S. and the President abroad would probably say they always prefer Phase 0 because it means we are successful.

The country team at any embassy is there before, during, and after most military actions and is often stuck holding the bag when the military moves on to Phase IV. This situation presents another challenge for the way the operational phases are used today. Phase IV should be the stabilizing phase. The military and the DoD have been pressed to carry much of this load, though neither are designed to do so. Further, Phase IV, like Phases I and II, is not practiced, planned, or simulated like Phase III. The only incentive to get to Phase IV, as seen again and again, is to send troops home. Unfortunately, there are too many examples where the precipitous departure of the military and insufficient planning, measures of effectiveness, and achieved outcomes create a vacuum and subsequent instability.

After repeated exercises, experiments, and scenarios, the military is comfortable in what many call the "race to Phase III."

After repeated exercises, experiments, and scenarios, the military is comfortable in what many call the "race to Phase III." There are myriad reasons for this. The first is the importance of the non-military, non-defense components of the U.S. government during Phase 0 and Phase I. The role of the military in relation to the whole-of-government, even the whole-of-society is minimal during the first phases. During the time of steady state and deterrence, there is little money to be spent on military equipment and, therefore, much more role for the rest of government and society. There is precious little opportunity to shoot tanks, artillery, mortars, or even train in small arms. This does not mean there is no role for the military during this period. The warrior ethos and the defense enterprise is not fully exercised, leaving it anxious for more sense of fulfillment. This fulfillment is found primarily during Phase III. The ideal might suggest moving away from or avoiding the notion of Phase III entirely and creating systems that allow for more peaceful solutions, with great emphasis on development and diplomacy. This means a systemic shift in how rewards are structured for promotions and profit. Instead of incentivizing Phase III by focusing so much on it, the U.S. government is well advised to focus on rewarding success during prior phases. It need not be combat; a rewarding military career could mean helping a nation, ministry of defense, or partner army be more professional, responsive to civilian control, and supportive to the needs of their domestic stakeholders.

The U.S. Army's idea of regionally-aligned forces (RAF) may illustrate a greater investment in Phase 0. The RAF concept allows the Army to leverage its leadership and management skills in conjunction with its technical expertise, such as engineering, information management, and medicine to help partner nations grow during Phase 0 or I and avoid any kind of escalation. It also allows the military to support the other areas of diplomacy and development. After all, the civil affairs, Guard and Reserve sister-state programs, and other legacy exchanges have been working effectively in foreign countries for decades. Further, the defense attaches, as the military component of the U.S. Embassy's Country Team serve with distinction in many a fragile or failing state with no recommendation for war or operational phases other than Phase 0.

The U.S. Army's idea of regionally-aligned forces (RAF) may illustrate a greater investment in Phase 0.

The DoD and the Services should not go to their colleagues at State and U.S. Agency for International Development, for example, and tell them what they are doing. Instead, through partnerships of equality, they should engage in a deliberate, patient, planning process that allows for better interorganizational alignment and greater synergistic effects over long periods. This might even allow those who believe the U.S. has a "grand strategy," to put their finger on it. It also creates additional barriers to what some say is the risk of "militarization of American foreign policy," which popularized Karl W. Eikenberry.

Another challenge facing the DoD and Services is the use of wrong metrics and objectives, where desired outcomes energize bureaucratic momentum and become too hard to stop. Think about the notion of a leading question. In a leading question, the interrogative drives the answer. If an investigator asks if someone still beats his pet, no matter the answer, the person responding is guilty of something—he either admits to having abused his pet or of not stopping the abuse. Oversimplified perhaps, yet a powerful point to illustrate the wrong emphasis developed in today's phased approach. In many of the exercises, because there is a desire to get to Phase III and test the military's war footing, the milestones and markers used to rationalize this progression are largely contrived. Some will argue these milestones are developed to test the scenario. Maybe, but this gets back to the linear test of a series of non-linear events. Of course, the military and DoD exist to wage wars in a classic sense; however, as the world grapples with the future definitions of war and additional expectations are placed on the best-funded instrument of power, they must also change the way they employ forces during times of peace and conflict.

There is no reverse gear for the phased approach, so if Phase II is successful, can you go back to Phase I? The simple answer is it has never been tried. The operational phases make it difficult for planners and decisionmakers to shake off the oppressive mindset they are accustomed to. I am not sure they could construct a scenario to test it because it is anathema to their culture. It does not show clear combat success; it does not rationalize more equipment; and it does not advance contracts and bonuses.

Lack of a concept I call "strategic patience" points to the system-of-system shortfalls for the MDB environment the U.S. faces now and in the future. Patience is hard for Americans, generally. Strategic patience is even harder. It is explicit in the 2015 U.S. National Security Strategy. Generally, strategic patience means putting actions into motion that exceed one's time of command, one's rotation in a unit, or one's term in office. It is the set of actions put into place only after deep deliberation and contemplation. It is looking two or three people down the road in the leadership position. Some will argue, accurately, that they are already doing this. It is not carte blanche maliciousness or narcissism of leaders in the DoD and military industrial complex driving these efforts. Most of these patriots and public servants are well-intentioned, moral people. Rather, the system rewards people for spending money, for engaging in combat and warfare, and for using equipment. Currently, as demonstrated above, there is not a time when we can reward people for avoiding these facts, especially at higher and higher echelons.

So, what to do? There is no easy way to answer this question. In an exacerbated tone, a senior colonel asked me, "How do we plan without phases?" The fix lies in the system's thinking and deliberate planning the military is already so good at. The DoD is well-advised to distance itself from the operational phases and think strategically about the hard problems it faces. There are other really good, deliberate planning models out there, and the way we train, educate, and develop our leaders is changing. For example, the deliberate planning put in to operational phases is good. The military decision-making process (MDMP), embraced by the U.S. Army, feeds the operational phases. Do not throw out MDMP. Rather embrace the true nature of design thinking it grew from. For example, instead of focusing on the operational phases of war as the primary backdrop for any scenario, at any school, embrace the notion that volatile, uncertain, complex, and ambiguous (VUCA) conditions will persist and grow. Looking at MDB through a VUCA lens encourages a more dynamic, less linear understanding of the process.[6] Taking a circular, even better, a spherical understanding would allow for better sense-making.

Keep words that have become common place like counterterrorism, irregular warfare, or counterinsurgency. They all have a place in a MDB, across a "three-block war," crisis, or natural disaster. Focus first on defining the problem. Focus on planning as President Eisenhower required. Do not restrict yourself so much to the operational phases that you get tunnel vision and lose the adaptability and agility to move in multiple directions. Synthesis of these points allows the U.S. government, the DoD, and the Services to focus on influence besides military force. Do not leave the military behind, but strive to better understand and utilize it. The flawed notion that a force, a unit, or a country controls or owns something is what mires thinking and adheres us (blindly) to the operational phases. Clausewitz directs us to his observation: "…intellectual activity leaves the field of the exact science of logic and mathematics. It then becomes an art in the broadest meaning of the term—the faculty of using judgement to detect the most important and decisive elements in the vast array of facts and situations."[7]

Operational phases are the albatross of military planning. They impede good judgement, they prevent holistic sense-making, and they retard critical and creative thinking. Keep the operational phases for analysis and evaluation, but de-couple them from synthesis in policy and doctrine. This bureaucratic dogma and its zealots slow our victories and cost us blood and treasure. We are running low on both. ***IAJ***

NOTES

1 Joint Publication 3-0, *Joint Operations*, Department of Defense, Joint Staff, 2001, <http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf>, accessed on July 8, 2017.

2 Charles C. Krulak, "The Strategic Corporal: Leadership in the Three Block War," *Marines Magazine,* Air University, U.S. Air Force, Montgomery, AL, 1994.

3 Ibid.

4 Michael Howard and Peter Paret, "Carl Von Clausewitz: On War," Princeton University Press, Princeton, NJ, 1984, p. 14.

5 Ibid.

6 VUCA was first introduced at the U.S. Army War College and has become a well-trod phrase to demonstrate complexity. It was first presented in a paper by James A. Lawrence (USDA Forest Service) and Lieutenant Colonel Earl N. Steck (US Army), "Overview of Management Theory," 1991, <http://www.dtic.mil/dtic/tr/fulltext/u2/a235762.pdf>, accessed on July 8, 2017.

7 Howard and Paret, p. 585.

A Call for Synchronization of Civil Information Management

by Michael L. Jones

Special operation forces (SOF) and interagency partners face unique challenges when conducting civil information management (CIM) within the joint interagency, intergovernmental, and multinational (JIIM) environments. Information management requires a streamlined technologic system that reduces redundant technological platforms for civil information sharing. Currently, there are more than ten platforms that exist between the military and interagency that are capable of synchronizing and distributing civil information. The lacking definitive definition of collaboration and the necessary technology solution that facilitates streamlined civil information sharing between the Department of Defense (DoD) and the interagency create problematic resistance barriers to streamlined information sharing.

Synchronizing CIM systems improves the sharing of civil information throughout the JIIM. SOF and the interagency community (IC) have successfully shared information, to include civil information and intelligence, foiling more than 60 terrorist attacks against the U.S.[1] Information sharing and deconfliction requires significant synchronization.[2] Successful CIM depends on streamlining organizational processes, synchronizing assets, and developing priorities.

Technology provides the necessary software and infrastructure solutions needed for collaborative analysis of civil information that can be leveraged by combatant commanders to inform and influence the decision-making cycle to achieve strategic success. Streamlining technological infrastructure enables organizations operating within the JIIM to maximize the use of civil information. Technology is the driving factor of synchronization.[3] The United States Special Operations Command (USSOCOM) has built one of the most network-centric organizations, with the capability to collaborate across military and civilian networks.[4] Utilizing a joint program of record for CIM,[5] capable of framing the civil domain by synchronizing civil information in the multilateral JIIM environment would increase efficiency and collaboration.

Major Michael L. Jones is a civil affairs officer assigned to the 96th Civil Affairs Battalion (Airborne) and is currently deployed in support of Operation Inherent Resolve. He received a master's in Global and Interagency Studies from Kansas University, and has multiple deployments to the U.S. Central Command area of responsibility.

Literature Review

SOF face multilateral challenges in maximizing civil information sharing. Multilateral challenges exist in two areas: lack of common policy that enables synchronization and collaboration of civil information between SOF and the interagency when conducting special warfare[6] and the resistance to streamlining organizational and technological systems for the goal of creating transparency. Concise definitions for the conduct of interagency collaboration are lacking and often overlap with other definitions necessary for collaboration within the JIIM; for example, a Congressional Research Service (CRS) search of Lexis-Nexis revealed 21 examples of interagency collaboration that lacked a definitive definition.[7] Multilaterally, these challenges exist for coalition forces and host nation partners.

The development of cohesive policy for the conduct of civil information sharing will shape future successes by streamlining mission command infrastructure technologies...

The multilateral approach to special warfare activities in the JIIM environment has seen successes that range from the Office of Strategic Services in World War II to Operation Enduring Freedom. Developing multilateral relationships among partnered nations, interagency organizations, and the military must focus more on operational efficiency and less on source protection.[8] The development of cohesive policy for the conduct of civil information sharing will shape future successes by streamlining mission command infrastructure technologies, while promoting efficiency and reducing organizational resistance to collaboration.

The CRS examined current agreements and activities to enhance joint efforts among federal agencies, shared responsibilities, and overlapping jurisdictions. Collaboration is defined as "any joint activity by two or more organizations that is intended to produce more public value than could be produced when the organizations act alone."[9] Precise definitions for conducting interagency collaboration are lacking and often overlap with other definitions that are necessary for JIIM collaboration. Lacking and overlapping collaboration policies create information-sharing resistance. The Government Accountability Office (GAO) loosely defines collaboration as two or more organizations contributing for greater gain and is generically considered to be cooperation. The GAO found that the generic interpretation of collaboration within the interagency community has created seven types of collaboration, 34 overlapping definitions, and 200 collaborative devices, many of which were determined to hinder matters of national security.[10]

Leaders within the interagency community identify the lack of authority and legislative policy as key elements that hinder collaboration, which are further complicated by a multitude of information technology solutions that do not easily facilitate information sharing. The CRS cites the changing nature of government organizations, politico-economic pressure, overlapping agency responsibilities and jurisdictions, and crisis response as rationales for definitive improvement in collaboration and coordination.[11] The CRS suggests that resolution begins with eliminating fragmented policymaking and implementing collaborative policies that mitigate redundancies and provide clear directives and jurisdictions for interagency collaboration.

In the conduct of special operations, literature trends associated with CIM indicate that information sharing is critical to operational success in a complex environment.[12] Dawes indicates the benefits of improved efficiency outweigh the associated risk of misuse of information and data management. Policymakers face significant challenges, such as organizational resistance, organizational discretion, and multiple networks, when developing clear procedures for information management and utilization across multiple agencies and systems.[13] Current data indicates that there is not a standardized system for synchronizing multiple CIM technology platforms. The value and impact of collaborative civil information sharing are not effectively measured. The literature reviewed does not reflect measurable effectiveness statistically; rather, effectiveness is reflected through opinion polls of nongovernmental organizations (NGOs). Although NGO input is valuable, it does not accurately depict the effectiveness of information sharing given the differing nature of NGO humanitarian operations when compared to special operations conducted by USSOCOM. Civil information sharing provides a unique representation of the human domain that when shared among different agencies and organizations increases productivity and improves policymaking.[14] The associated cost of network infrastructure development and management is a limiting factor for synchronizing civil information.[15] The cost of network system development and management warrants further research to determine the impact with the associated cost, creation, implementation, and management of information sharing. USSOCOM has approved the capabilities and production document enabling United States Army Special Operations Command (USASOC) to secure fiscal year 2017 funding for the transition of the Civil Information Management Data Processing System (CIMDPS) to the Joint Civil Information Management System (JCIMS).

This article analyzes the correlation between the normative value of civil information sharing and the conduct of CIM in the JIIM. Can reducing the number of information systems improve the sharing of civil information across the JIIM while improving relationships throughout the SOF enterprise? Based on the data presented and literature reviewed from Hun, Beadenkopf, Kaiser, Carafano, and Hanhauser, I argue that an autonomous adaptive strategy for the standardization of CIM across a synchronized technological infrastructure will improve the conduct of special operations in the JIIM.

The associated cost of network infrastructure development and management is a limiting factor for synchronizing civil information.

Unilateral and Multilateral Challenges

Countering twenty-first century threats poses unilateral and multilateral challenges for conducting special operations in a complex JIIM environment. The evolving complexity of the global environment presents SOF with unilateral and multilateral challenges for maximizing civil information sharing. Challenges exists in three areas unilaterally: the lack of common legislation that synchronizes CIM in support of SOF and interagency operations, the conduct of special warfare[16]and irregular warfare [17] activities, and the synchronization of organizational technologies creating transparency, further building trust within the JIIM. The multilateral challenge is sharing civil information with coalition forces, host nation partners, and the interagency. Over classifying civil information limits information sharing. Accurately classifying civil information ensures the greatest dissemination of information and provides coalition forces and host nation partners access to information that is otherwise limited by classification. Likewise, the interagency shares information through internal and external

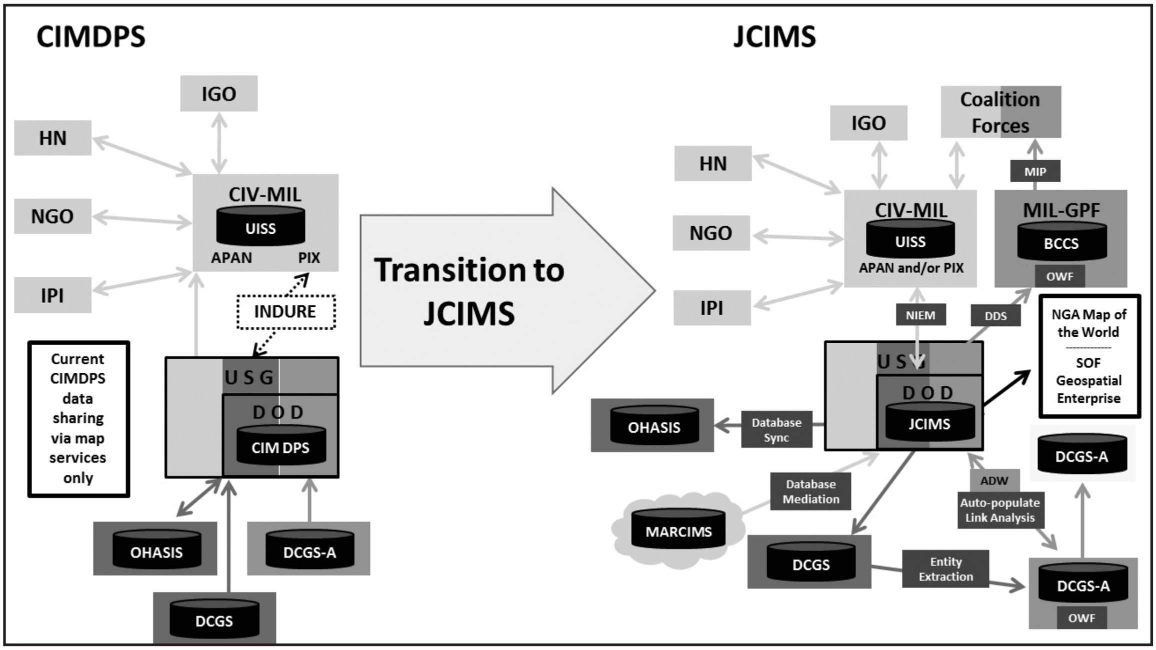


Figure 1. Transition from CIMDPS to JCIMS enhances information sharing.[18]

agreements that define the terms and authorities of the information being shared. The GAO identified 200 processes for collaboration and indicated that these overlapping procedures hinder national security.

The current complex CIM technology infrastructure limits the effective synchronization and distribution of information throughout the JIIM. Figure 1 demonstrates the current limitations and the potential gains for expanding a current civil information management program of record to a joint program of record. The benefit of expanding civil information management into a joint program of record is the facilitation of streamlined civil information sharing through an accessible information communication technology solution. The limitation of non-synchronized, civil-information databases presents a multilateral challenge that impacts the input of information from sister services, the interagency community, NGOs, and host nation partners. Providing the added dimension of civil information collected from external organizations, such as NGOs and host nation partners, expands the DoD capability to provide collaborative civil information analysis that influence strategic success.

CIMDPS is the USSOCOM program of record for synchronizing and collating civil information. USSOCOM has proposed transitioning from CIMDPS to JCIMS. The transition will broaden the global SOF enterprise by enhancing information access across the JIIM that further enables efficient coordination, collaboration, and cooperation in the pursuit of strategic effects. Data suggests that joint synchronization of the information infrastructure effectively integrates multiple operating systems for CIM and increases the efficient distribution of civil information. Streamlining the access to civil information sharing fosters collaboration and efficiency.

Civil Information Sharing Infrastructure

Information and communication technology is the driving factor for the synchronized distribution of civil information that provides accessible real-time information for rapid decision-making. USASOC has built one of the most network-centric organizations within the JIIM, with the capability to collaborate across military and civilian networks.[19] Technology has enabled organization-centric solutions dependent upon the operating network utilized for CIM. Special operations often require the use of mobile ad hoc networks for locating, managing, and allocating resources in areas where network infrastructure may not be available.[20] The ability to establish accessible networks of different classifications is an equally-critical variable for information sharing. Mobile ad hoc networks and their classification levels in support of special operations within the JIIM environment should be considered when framing the civil domain and evaluating civil information.

Civil information management provides a detailed comprehensive understanding of the impact of the civil domain on the operational environment. Information management is equally important during offensive, defensive, and stability operations. Numerous CIM systems exist at the geographic combatant command and below. For example, United States Pacific Command (USPACOM) and United States Southern Command (USSOUTHCOM) utilize a combatant command-sponsored program called All Partners Access Network (APAN); USSOCOM utilizes CIMDPS; the United States Marine Corps utilizes the Marine Civil Information Management System; the interagency utilizes systems. such as the Overseas Humanitarian Assistance Shared Information System, APAN, and Preservation Information Exchange; while the intelligence community utilizes the Distributed Common Ground System. Each of these systems has a differing classification level and capability for information sharing that range from geographic information system file sharing to real-time chat applications.

Problematically, the multitude of information and communication technology (ICT) systems fails to provide a collaborative analysis of the civil domain within the operational environment.[21] The CIMDPS JCIMS Steering Committee suggests that transitioning CIMDPS to a joint program of record will expand the current data-sharing capability and synchronize the multitude of ICT systems across the JIIM environment. [22] In fiscal year 2017, CIMDPS will transition to a joint program of record. The joint program of record transition enables synchronization of the civil information sharing infrastructure within the JIIM, which mitigates resistance barriers associated with culture, doctrine, and best practice challenges, while providing a comprehensive streamlined access point for analysis of the civil domain.

Civil information management provides a detailed comprehensive understanding of the impact of the civil domain on the operational environment.

Guiding Directives

Within the JIIM, a concise definition for the conduct of interagency collaboration is lacking and often overlaps with other necessary collaboration definitions. To address all stakeholder interests within DoD and the Department of State, a comprehensive legislative policy that defines collaboration and establishes a protocol for information sharing is needed. DoD Directive (DoDD) 2000.13 addresses the need to synchronize the organization by coordinating with other government agencies, host nation militaries, and civil agencies.[23] DoDD 3000.07 provides the necessary guidelines facilitating global collaboration and civil information sharing.[24]

A definitive language for interagency collaboration is lacking.[25] The CSR suggests resolution begins with eliminating fragmented policymaking and implementing collaborative

Categories	Benefits	Barriers
Strategic (Micro)	• Synchronizes the joint network domain • Policy-guided collaboration • Accountability	• Multiple networks • Policymaker resistance • Organizational discretion
Operational	• Collaborative operational picture • Promotes strategic success	• Interagency source sharing • Organizational solutions
Tactical (Micro)	• Streamlines CIM • Expands collaboration	• Tactical organization • Change Resistance

Table 1. Jones CIM benefit/barrier comparison.

policy that mitigates redundancy and provides clear directives and jurisdictions for interagency collaboration. The lack of a common policy definition for CIM within the JIIM environment creates the greatest challenge—providing clear procedures for the utilization and management of information across multiple entities.[26] DoDD 2000.13, and 3000.07 begin to synchronize the organizational infrastructure for civil information sharing and collaboration. Hun et al. suggest further collaborative policy is needed to mitigate secrecy and promote efficiency within the JIIM.[27] Arguably, a multitude of policy and directives exist to foster collaboration. A strategy for integration that stems from collaboration across the JIIM and utilizes a synchronous information communication technology solution is a more feasible approach.

Successful Information Sharing

Special Operations Command (SOCOM) 2020 positions SOF to be globally networked throughout the JIIM to rapidly and persistently address regional threats to stability. In support of the National Defense Strategy, collaborative information sharing has manifested success in the integration of SOF, conventional, and interagency counterparts. Successful information integration is dependent upon flattening the organization, synchronizing systems, information collection assets, and intelligence development priorities. Table 1 demonstrates the potential benefits and possible barriers associated with synchronizing civil information management.

Strategic success, that is the ability to implement operational systems that produce predictable outcomes and directly contribute to the decision-making process, is rarely defined by a specific accomplishment. Civil information sharing has mitigated the threat of terrorism against the U.S., improved global military and interagency effectiveness, and reduced unnecessary expenses associated with information and communication technology development. Strategic success has directly resulted from civil information sharing within the JIIM.

Since the Heritage Foundation began tracking post 9/11 foiled terrorist attacks against the U.S. in 2007, 69 foiled terrorist plots have been reported.[28] Increased information sharing between the U.S. and its allies has improved interagency communications among the State Department, the Department of Justice, the Department of Homeland Security, and the interagency community, and support for NATO and U.S. counterinsurgency strategies in Afghanistan, as well as for missions around the globe, are eliminating terrorist safe havens.[29] Information sharing ensures the comprehensive domestic counterterrorism enterprise is capable of understanding the evolving complex terrorism threat in the strategic defense of the U.S.[30]

Successful information sharing requires significant synchronization and deconfliction.[31] The Heritage Foundation study demonstrates the effectiveness of collaborative civil information sharing. Civil information provides the operational picture of the human domain that supports military and interagency operations. The complexity of the emerging terrorism threat underscores the importance of global collaboration and cooperation. Collaboration and cooperation is a move beyond the independent centers of excellence within the geographic combatant commands and the interagency community. Sharing civil information across the JIIM environment requires an autonomous adaptive approach encompassing both the military and interagency to accomplish organizational synchronization.

Discussion

This discussion reviews the benefits and challenges of synchronizing CIM to increase effective collaboration within the JIIM and proposes future research recommendations. Can synchronizing the numerous CIM systems through a singular ICT infrastructure, such as JCIMS, improve civil information distribution throughout the JIIM? An examination of current DoD policies, USSOCOM guiding directives, and military-interagency information sharing success trends identifies three issues: defining the definition of interagency collaboration within the JIIM, synchronizing a complex ICT infrastructure, and developing a multilateral policy for sharing and synchronizing civil information.

Synchronizing CIM requires an autonomous adaptive approach to establish a definitive definition of collaboration, facilitate information sharing within the joint interagency environment, and fully implement the transition to JCIMS across the levels of war (strategic, operational, and tactical). Information and communication technology intensive systems, such as JCIMS, must synchronize data received from the operational environment and interact across the JIIM to provide the geographic combatant commander with an operational framework of the civil domain. Civil information management synchronization cannot be accomplished with an autonomous software solution. Synchronizing civil information requires an autonomous adaptive strategy of personnel and technology to monitor the internal system (JCIMS) and the operational environment. Information providers, system operators, and network technicians are the adaptive elements that enable the autonomous element (software) to provide the civil domain common operating picture. In addition to the autonomous, adaptive strategy, guiding policies that standardize collection and input of civil information between the DoD and the interagency are needed. Establishing guiding policy can mitigate the confusing interagency collaborative framework identified by the GAO. An autonomous, adaptive system strategy enables stakeholders to shape diverse policies into common language that benefits numerous agencies throughout the joint interagency environment. An autonomous, adaptive system strategy enables users at the strategic, operational, and tactical levels of war to implement the transition to the JCIMS. Utilization of multilateral guidelines maintains the SOF capacity to frame the civil domain providing the geographic combatant commanders the ability to adapt to emerging twenty-first century threats.

Synchronizing civil information requires an autonomous adaptive strategy of personnel and technology to monitor the internal system (JCIMS) and the operational environment.

Support for Standardization

United States Army Special Operations Command and other government agencies have each established separate, non-synchronized, CIM systems to support their operations. There is organizational support for standardizing the collection and management of civil information within the DoD. Army Special Operations Forces (ARSOF) 2022 establishes a benchmark for the development of a standardized system for information sharing. Standardizing information management operations within the JIIM environment is an extensive, large-scale implementation that will require multilateral agreement upon guiding legislation that solidifies the practices across the DoD and the interagency community. Synchronizing CIM policy and systems cannot be broken down into smaller policies until a clear policy that synchronizes information collaboration is established. Policy implementation requires complex utilization of policy, power, and negotiation.[32] Additional policy alone will not facilitate improved information management. Improving information management also requires an effective ICT solution that is user friendly and accessible across the joint environment. Utilizing an autonomous, adaptive strategy of people and technology for the implementation of the JCIMS program of record enhances the synchronization by mitigating the associated time and cost of developing an autonomous software solution.

The nature of conflict is evolving into an ill-defined, complex, grey area of political conflict teetering on the verge of full-spectrum conflict. The strategic challenge facing the DoD and the interagency is adopting and implementing a concise policy for collaboration and the conduct of CIM. Synchronizing the multitude of information and communication technologies systems is an essential element of maintaining an interconnected, joint enterprise capable of addressing complex and emerging threats. Expanding the current U.S. Army program of record for CIM into a joint program of record is a significant move toward multilateral synchronization and is scheduled to go into effect fiscal year 2020. There remains a need for unified policy that establishes concise definitions of collaboration and synchronization between the military and interagency. Utilizing an autonomous, adaptive strategy for implementing a joint CIM program will improve information collection, enhance collaboration, and improve trust within the JIIM. Through the application of comprehensive CIM, framing the civil domain enables informed operational development, which influences strategic success. ***IAJ***

NOTES

1 David Inserra, "69th Islamist Terrorist Plot: Ongoing Spike in Terrorism Should Force Congress to Finally Confront the Terrorist Threat," Heritage Foundation Issue Brief #4416 on terrorism, June 8, 2015, <http://thf_media.s3.amazonaws.com/2015/pdf/IB4416.pdf>, accessed on May 23, 2016.

2 Ronald Beadenkopf, "Conventional Forces Intelligence Integration with Special Operations Forces in Support of Operation Iraqi Freedom III," Joint Special Operations University and National Defense Intelligence Agency SO/LIC Division Essays, 2007.

3 Yasser Gadallah et al., "Middleware Support for Service Discovery in Special Operations Mobile Ad Hoc Networks," *Journal of Network and Computer Applications*, Vol. 33, Issue 5, September 2010, p. 611.

4 Jon R. Lindsay, "Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations," *Journal of Strategic Studies*, Vol. 36, Issue 3, 2013, pp. 422–453.

5 Joint Publication 3-57*, Civil Military Operations*, September 11, 2013, p. GL-6. Civil information management (CIM). Process whereby data relating to the civil component of the operational environment is gathered, collated, processed, analyzed, produced into knowledge products, and disseminated.

6 Army Doctrine Reference Manual 3-05, *Special Operations*, August 2012, p. 1-5. Special warfare activities involve the ability to operate within the population—specifically, to address sociocultural factors by understanding the culture of the population.

7 Frederick M. Kaiser, "Interagency Collaborative Arrangements and Activities: Types, Rationales, Considerations," Congressional Research Service report to Congress, May 31, 2011.

8 Lee Jae Hun et al., "Countering 21st Century Threats: The Need for an Increased Joint, Interagency, Intergovernmental and Multinational (JIIM) Approach to Irregular Warfare," *Small Wars Journal*, January 6, 2015.

9 Kaiser

10 Ibid.

11 Ibid.

12 Beadenkopf and Susan S. Dawes, "Interagency Information Sharing: Expected Benefits, Manageable Risks," *Journal of Policy Analysis and Management*, Vol. 15, Issue 3, June 1996, pp. 377–394.

13 Kaiser and Robert David Steele, "Intelligence Reform: More Needs to be Done," commentary and reply, *Parameters*, Vol. 35, Issue 2, Summer 2005, p. 135.

14Dawes.

15 Gadallah and Lindsay.

16 Ibid and Army Doctrine Reference Manual 3-05, *Special Operations*.

17 Joint Publication 1-02, *Department of Defense Dictionary of Military and Related Terms*, April 12, 2001, p. 280. Irregular warfare. A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, in order to erode an adversary's power, influence, and will. Also called IW.

18 United States John F. Kennedy Special Warfare Center and School Civil Information Management Data Processing System (CIMDPS)/Joint Civil Information Management System Steering Committee (JCIMS) Presentation, May 2015, Fort Bragg, NC, slide 7, "CIMDPS/JCIMS Steering Committee Minutes," May 20, 2015, <https://wss.apan.org/2476 /CIMDPSJCIMS Steering Committee/Steering Committee/CIMDPS-JCIMS Steering Committee_20May2015x.pdf>, accessed on June 2, 2016. United States John F. Kennedy Special Warfare Center and School is the U.S. Army Proponent for Civil Affairs and as a Requirements Manager conducts JCIMS Working Groups and Steering Committees to capture CIM requirements. The Committee consists of joint services, active, and reserve component civil affairs leadership and interagency representation.

19 Lindsay.

20 Gadallah.

21 George J. Hanhauser, IV, "Comprehensive Civil Information Management: How to Provide It," Strategy Research Project, U.S. Army War College, Carlisle Barracks, PA, April 2012, p. 22.

[22] United States John F. Kennedy Special Warfare Center and School Civil Information Management Data Processing System/Joint Civil Information Management System Steering Committee Presentation.

[23] John M. Deutch, "Civil Affairs," Department of Defense Directive Number 2000.13, The White House, Washington, DC, June 27, 1994, pp. 2–3 and 25.

[24] Gordon England, "Irregular Warfare," Department of Defense Instructions Number 3000.07, The White House, Washington, DC, December 1, 2008, pp. 2–3.

[25] Kaiser.

[26] Kaiser and Steele.

[27] Hun et al.

[28] Inserra.

[29] Steven Bucci et al., "Fifty Terror Plots Foiled since 9/11: The Homegrown Threat and the Long War on Terrorism," The Heritage Foundation, April 25, 2011.

[30] Steven Bucci et al., "60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism," The Heritage Foundation, Special Report #137 on terrorism, <http://thf_media.s3.amazonaws.com/2013/pdf/SR137.pdf>, accessed on May 23, 2016.

[31] Beadenkopf.

[32] Patrick E. Connor et al., *Managing Organizational Change,* 3rd ed., Praeger, Westport, CT, 2003.

Art of War: Gifts of Peace

Command and General
Staff College Foundation, Inc.

Learn more about the Art of War Initiative.

www.TheArtOfWarInitiative.org

What were you THINKING?

Biases and Rational Decision Making

by Ted Thomas and Robert J. Rielly

In general, we expect people to think and act rationally. Market theories, negotiations, and other human endeavors are based on people reacting and thinking in sane, rational ways. It is based on an assumption that we are logical and can make good decisions. But are people really that rational? Dan Ariely, a noted scholar, wrote a book on how we are all "Predictably Irrational."[1] Numerous authors have pointed out how psychological traps, cognitive biases, and world views cloud our thinking and lead us to irrational choices. Decision making is the realm of the leader. Leaders make decisions and our assumption is they are making good, rational decisions. However, in our rush to make a decision we forget that psychological traps and biases affect them just as they do the rest of us. This article will use the Bay of Pigs invasion as a case study to examine how these human characteristics often cause us to act in counterproductive ways and what a leader can do to offset them.

Bay of Pigs Invasion

The 1961 Bay of Pigs invasion provides a fertile example of poor thinking and decision-making. In 1959 Fidel Castro completed his overthrow of the corrupt Batista government in Cuba. In the spring of 1960 Castro formally aligned himself with the Soviet Union, establishing a communist regime. Many of those in Batista's regime and those who did not want to live in a communist country left Cuba for the United States.[2] In the era of the Cold War, the U.S. did not relish the idea of having a communist country 90 miles off its coast, much less a nation closely allied with the Soviet Union.

Ted Thomas is director of the Department of Command and Leadership in the U.S. Army Command and General Staff College at Fort Leavenworth, Kansas. Thomas graduated from the United States Military Academy and served in various command and staff positions before retiring. He received a master's from the University of Illinois, and a Ph.D. from Missouri University of Science and Technology.

Robert J. Rielly is a retired Army lieutenant colonel and currently serving as an associate professor in the Department of Command and Leadership, U.S. Army Command and General Staff College, Fort Leavenworth, Kansas.

The U.S. began making plans to overthrow Castro during President Eisenhower's presidency in 1960. President Eisenhower, the Supreme Allied Commander, five star general, and hero of WWII, directed the CIA to start looking at planning covert operations to bring down Castro. Kennedy did not know the planning was going on before the election and even heavily criticized the Eisenhower administration for their passivity.[3] Two days after newly elected President John F. Kennedy was sworn in as President, he was briefed by Richard Bissel, a CIA planner and chief architect of the plan to invade Cuba. Kennedy described Bissel "as the only CIA man he knew well enough to trust."[4] Possessing a certain amount of hubris after winning the election, the Kennedy administration proceeded with the strategy. The plan envisioned recruiting and training approximately 1400 Cuban exiles to do a beach landing in Cuba to overthrow Castro's regime. Should the invasion fail, the exiles were supposed to escape into the Escambray Mountains and link up with guerillas in the mountains continuing an insurgency against the communist government.[5]

Since it was supposed to be a secret operation not many people were briefed, to include the Joint Chiefs of Staff (JCS) who were marginally read in on the plan. When asked their opinion, the chiefs said it had a "fair chance" of success, which President Kennedy interpreted as a "good chance." In the post mortem following the failed invasion the JCS were asked what they meant and said they thought it had a three times higher probability of failure than success. That is not the way President Kennedy interpreted "fair chance."[6]

As a result of the Bay of Pigs invasion the Kennedy administration was diplomatically embarrassed, the CIA was discredited, and several of its leaders were fired. It also provided a major victory for the Cuban revolution, Fidel Castro in particular. Castro was forced deeper into the Soviet Bloc for support and survival. This incident set the stage for the showdown between the United States and the Soviet Union in the Cuban Missile Crisis, bringing the world to the edge of nuclear war.[7]

The question is, how could so many smart people make so many irrational decisions? Kennedy's cabinet was stacked with intellectuals and experts who had years of government and corporate experience or who were Harvard professors and subject matter experts.[8] Irving Janis's book attributes much of the failure of the operation to groupthink. He defines groupthink as "a mode of thinking that people engage in when they are deeply involved in a cohesive in-group, when the members' strivings for unanimity override their motivation to realistically appraise alternative courses of action."[9] Groupthink was certainly a major factor in the poor decision making and lack of critical thinking evidenced at the Bay of Pigs fiasco. However, there are other just as insidious threats to rational decision making evident in this case.

Groupthink was certainly a major factor in the poor decision making and lack of critical thinking evidenced at the Bay of Pigs fiasco.

Cognitive Biases

Cognitive biases or hidden traps in thinking often lead to poor decisions. "People sometimes confuse cognitive biases with logical fallacies, but the two are not the same. A logical fallacy stems from an error in a logical argument, while a cognitive bias is rooted in thought processing errors often arising from problems with memory, attention, attribution, and other mental mistakes."[10] Logical fallacies come from poor thinking while cognitive biases are a part of being human. The problem with these biases is they become part of how we think and are therefore invisible to us, causing us to not see them even as we fall into them.[11] Research has uncovered many cognitive biases. This article will focus on six of the more common traps: confirming evidence, sunk cost, framing, status quo, anchoring, and overconfidence.

The confirming evidence trap leads us to seek out information that confirms our existing point of view and avoids or discounts information that contradicts our point of view.[12] President Kennedy wanted plausible deniability of US involvement. Yet Pierre Salinger, the President's press secretary, referred to the plan as "the least covert military operation in history." Even the President read in the newspapers about secret training camps in Guatemala and efforts to recruit Cubans in Miami to fight in the exile forces. Despite the abundance of leaks, the administration didn't see the information as a problem. Instead, they decided to ignore this evidence and focus on plausible deniability of U.S. participation due to the lack of direct involvement. Somehow, they thought that no "direct involvement" of U.S. forces would be enough to convince the world that the U.S. was not involved.[13]

How a problem is framed influences how we approach the problem.

The sunk cost trap is how we make current decisions based on past decisions regardless of whether or not the past decision has any bearing on the current issue. To change our current decision might make us look like we made a bad prior decision, and we are often unwilling to admit we made a mistake.[14] President Kennedy and his advisors made a decision two days into the presidency to back the invasion of Cuba based on a persuasive briefing by a trusted expert, Richard Bissell. As evidence started to mount on the inadvisability of the decision, the administration did not want to look like they had made a mistake in their earlier decision. Bissell who had put so much emotional energy into planning the invasion was not able to "see clearly or to judge soundly."[15] So much effort and planning were already sunk into the invasion that it moved inexorably forward.

How a problem is framed influences how we approach the problem. People tend to accept the way the problem is given to them without looking at it from a different perspective or point of view. For instance, people tend to be risk-averse when decisions are framed in terms of gains and losses, wanting to avoid losses over possible gains.[16] The CIA framed the Bay of Pigs invasion in terms of the danger of having a Soviet satellite 90 miles off the coast of Florida. With Soviet influence virtually on our borders, the gain was in terms of the safety and security of the U.S., as well as the possibility that other Latin American countries would not follow suit in becoming communist.[17] This strongly influenced how the administration saw the problem. Had the decision been framed by the consequences of failure and loss, the result would have been different. The U.S. lost credibility and the trust of nations throughout the world, and lost security on its borders by the forcing of a closer alliance between Cuba and the Soviet Union.[18]

The status quo trap is based on the fact that people are averse to change and would prefer the current situation over something new or different.[19] When Kennedy became president, the planning for the invasion was already well under way. Rather than change the plan, Kennedy elected to stick with it and maintain the status quo.

The anchoring trap is reflected by the fact that we give inordinate credence to the first information we receive and then compare any new information to the original thought, idea, or data.[20] Thus, the first information we receive "anchors" our thoughts. The first briefing by Bissell anchored the administration to the idea of an invasion. Bissell himself altered the plan from a small scale covert operation to an invasion in November of 1960. The President was only briefed on the invasion plan two months later in January of 1961. The President and his advisors never seriously considered other options such as using diplomatic and economic leverage, a small scale infiltration of exiles, or even major military intervention with U.S. forces, because they were anchored to the exile brigade beach assault and invasion option.[21]

The overconfidence trap states we are too self-assured about our abilities in making decisions and forecasting future consequences, which causes us to take greater risks.[22] Experts are especially vulnerable to this trap because they are more convinced they are right due to their expertise and partially to maintain the appearance of being an expert.[23] If they don't know the answer, then they are obviously not much of an expert. After the election in 1960, there was a sense of euphoria that nothing could stop the new administration in solving the nation's problems and challenges. Kennedy and his advisors were overly optimistic, giving them a low sense of vulnerability about their cause and ability to win. They viewed the Bay of Pigs plan through the lens of democracy is good and communism is bad and whatever we do will be vindicated by the non-communist nations of the world.[24]

Many of these traps are linked and feed off each other. Overconfidence often starts with anchoring. Confirming evidence is often done after a prior decision is made, and we look for evidence to confirm the sunk cost or the status quo. The status quo is often due to the sunk cost. Our framing of a problem may start with the anchoring of a suggestion or fact that may or may not be relevant. These six cognitive biases are only a few of the biases, but some of the more prevalent. The real importance of understanding these thinking traps and biases is knowing how to deal with them.

Cognitive biases can be particularly common in the military especially with planning and execution. Both commanders and their staffs can be vulnerable to the anchoring trap with the first piece of information they receive. They can view all subsequent pieces of information through this lens. In addition, when the commander makes the decision and the staff begins preparing for execution, we see confirmation bias when people tend to ignore any information or intelligence that contradicts the approved plan. Commanders and their staffs can fall victim to the sunk cost trap when they refuse to reframe a problem or adjust a course of action or decision because of the time, effort and resources already invested. Finally, most leaders are not enthusiastic about change, but change can be necessary. Commanders and their staffs fall victim to the status quo trap when they choose to keep doing the same thing despite evidence to the contrary. We often tend to do more of the same and reinforce failure hoping for a change in the outcome.

The overconfidence trap states we are too self-assured about our abilities in making decisions and forecasting future consequences...

Ways to Address our Biases

There are many different ways to address faulty thinking and cognitive traps. Just knowing that these traps exist, and that we are all subject to them, is the first step in overcoming them. Leaders have to overcome these traps on two levels - first individually as a leader, and secondly as part of a collaborative group. At the individual level a person not only needs to recognize that traps exist, but they also need to be proactive in what they can do about it.

Leaders have a responsibility to examine their thinking and avoid cognitive biases to the best of their ability. To avoid the anchoring trap, good leaders purposely seek out those with different opinions. Leaders should avoid speaking too early and giving their opinion, otherwise they may anchor those they supervise to their own preconceptions. Leaders should also think about the situation on their own before consulting others' opinions to avoid becoming anchored themselves.[25]

Leaders should examine how emotionally attached they are to the situation and realize how that will taint their decision-making. They find people who are uninvolved in the current or past decisions and who do not have the knowledge of sunk costs. They build a climate where people embrace experimenting and failure, where it is accepted to own their mistakes and fail forward.[26]

Protecting against traps is not just an individual responsibility, but also a group responsibility.

They try to look at the problem through a different lens or point of view and try to reframe the question or problem using different perspectives and pose problems neutrally, not favoring either gains or losses.[27] They examine what their current procedures are to determine if those procedures and processes are getting the organization to their vision.

For the status quo trap, leaders need to identify other options and compare them to the status quo to determine if the status quo is the best option to reach the objective. They should also examine if the status quo would still be an option if it was not already in place.[28]

The principle ways to combat the confirming evidence trap are to examine all information equally with the same criteria and use red team techniques (explained below) or designate a trusted person to play devil's advocate. Finally, leaders should avoid asking leading questions to get the answers they are looking for and instead ask open ended questions to explore the situation and encourage debate.[29]

Finally, leaders should conduct pre-mortems and post-mortems as a way to counter overconfidence. A pre-mortem looks at how the project, plan, or organization could fail in the future, while a post-mortem takes a view from the future looking into the past to determine why it did fail. The decision maker should challenge their own judgment especially when forecasting results of actions. In addition, the decision maker can provide data to support their predictions.[30] Leaders drive the process to help their organization overcome biases and that process starts with themselves.

Protecting against traps is not just an individual responsibility, but also a group responsibility. Combatting traps in a collaborative group begins with climate. When leaders set the proper climate in terms of policies, procedures and systems to protect against biases, they will make better collaborative decisions. A few techniques and methods for leaders to improve decision making in a collaborative group are red teaming, diversity, questioning, and establishing a safe to fail climate.

Red teaming involves establishing a team to look at the issue from the adversary's or opponent's view point. It is more than just playing devil's advocate. It seeks to get in the mind of the adversary and think the way they do. Red teams challenge assumptions, look at "what-if" scenarios, and provide possible answers to how the opponent would act and react to different decisions and scenarios. A few of its goals are to break through cognitive biases, improve decision making, and avoid surprises.[31] Red teaming avoids groupthink by taking people out of the group to look at the problem. It also addresses each of the other six cognitive traps. The red team challenges the evidence and looks at disconfirming information. They are not worried about sunk cost or the status quo. They look at the problem from different points of view and avoid the framing and anchoring traps. They are trying to find ways for the plan or decision to fail and avoid the overconfidence trap.

Diversity ensures there are differing opinions in a group including minority views, dissenting opinions, and disinterested parties who have not made a judgment on the problem. Diversity can be accomplished through different nationalities, religions, cultures, races, gender, ethnicity, language, age, social status, experiences, and political affiliation, to name a few. A diverse set of viewpoints increases creativity and innovation[32] and helps overcome groupthink, anchoring, sunk cost, and status quo traps.

Establishing a climate where questions are encouraged and valued helps people to challenge assumptions, predispositions, and paradigms that lead to cognitive biases. Questioning helps organizations survive and thrive in volatile and quickly changing environments. Questioning requires humility and a desire to learn, which comes from genuinely listening. Understanding the foundations of critical thinking are a great place to start in developing a keener ability to ask the right questions and overcome biases. Questioning facts, assumptions, points of view, paradigms and mental models, purpose, and problems are key lines of thinking to exposing all of the cognitive biases addressed here.[33]

Leaders who create a climate where it's safe to fail have an organization in which people are willing to expose their thinking and reasoning to the group. It means leaders are eager for feedback to improve their thinking and processes, especially when things go wrong. In order to achieve a safe to fail environment, we need a climate where it's safe to think and safe to challenge. A safe to think climate is one in which people have time to read and think, to be curious and gain new information. A safe to challenge climate is one in which people are able to challenge the organization's idea of who it is and what it does, to question its mental models without fear or threat of reprisal. Safe to fail is about allowing and taking risks to stay relevant[34] and to avoid the cognitive traps of anchoring, status quo, sunk cost, and framing.

Establishing a climate where questions are encouraged and valued helps people to challenge assumptions, predispositions, and paradigms that lead to cognitive biases.

Conclusion

The next major emergency that President Kennedy faced was the Cuban Missile Crisis. He learned from his previous fiasco. His embarrassment and failure in the Bay of Pigs certainly prevented him from becoming overconfident in dealing with Soviet nuclear weapons in Cuba. The administration continuously examined what could go wrong and projected what would be the cascading effects from possible decisions they could make. President Kennedy widened his circle of trusted advisors, including people from outside his party and with divergent views to help in framing the problem and finding an answer. He created a special group to come up with solutions and look at different alternatives which helped to prevent anchoring. Nuclear weapons in Cuba was a totally new problem to this administration, but rules of engagement and contingency plans were already written and could have boxed him into a decision resulting in world war three. He did not let the sunk cost of those plans and the status quo they represented constrain his thinking and decision-making. He learned to not blindly trust the experts, since the experts are often narrow in their viewpoints. He also used different experts to counter each other's opinions and avoid the danger of confirming evidence. In effect, he learned to counteract his cognitive biases and avoid groupthink to solve a very complicated problem and avoid thermonuclear war.

Our decisions may not have as catastrophic consequences as thermonuclear war, but poor decision making due to faulty logic and cognitive biases can certainly lead to the demise of companies, programs, or people's careers. Our assumptions are heavily influenced by cognitive biases. Understanding our human tendencies to fall into these traps is needed to have the self-awareness to avoid them. Knowing how to overcome these thinking traps and biases is an invaluable tool for leaders to have and use. ***IAJ***

NOTES

[1] Ariely, Dan. Predictably Irrational. Harper Collins: New York, pg. xix, 2008.

[2] Neustadt, Richard E. and Ernest R. May, *Thinking in Time*, The Free Press: New York, 1986, pg. 141.

[3] Neustadt, pg. 141-142.

[4] Ibid. pg. 145.

[5] The Bay of Pigs Invasion, 2016 Featured Story, https://www.cia.gov/news-information/featured-story-archive/2016-featured-story-archive/the-bay-of-pigs-invasion.html, accessed 26 May 2017.

[6] Neustadt, pg. 142.

[7] Braudel, Fernand. Invasion at Bay of Pigs, http://www.historyofcuba.com/history/baypigs/pigs6.htm, accessed 11 April 2017.

[8] Janis, Irving, Groupthink 2nd Edition, Houghton Mifflin Co: Boston, 1982, pg. 16-17.

[9] Ibid. pg. 9.

[10] Cherry, Kendra. "What is a Cognitive Bias? Definition and Examples," Verywell, May 9, 2016, https://www.verywell.com/what-is-a-cognitive-bias-2794963, accessed 22 March 2017.

[11] Hammond, John S, Keeney, Ralph L., and Raiffa, Howard. Smart Choices, Broadway Books: New York, 1999, pg. 186.

[12] Ibid. pg. 194

[13] Janis, pg. 20.

[14] Hammond, pg. 192.

[15] Janis, pg. 46.

[16] Hammond, pg. 197-199.

[17] Janis, pg. 30.

[18] Janis, pg. 15.

[19] Hammond, pg. 190.

[20] Hammond, pg. 187.

[21] Neustadt, pg. 142 and 146.

[22] Hammond, pg. 162.

[23] Lee, Samantha, and Lebowitz, Shana. “20 Cognitive biases that screw up your decisions,” August 26, 2015, http://www.businessinsider.com/cognitive-biases-that-affect-decisions-2015-8, accessed 22 March 2017.

[24] Janis, pg. 35 and 37.

[25] Brusman, Maynard, “The 8 Traps of Decision Making,” Working Resources, http://www.workingresources.com/professionaleffectivenessarticles/the-8-traps-of-decision-making.html, accessed 23 March 2017.

[26] Hammond, 193.

[27] Ibid, pg 200.

[28] Ibid, pg 190-191.

[29] Ibid, pg 196.

[30] Ibid, pg 202

[31] Red Team Journal, “Red Teaming and Alternative Analysis,” http://redteamjournal.com/about/red-teaming-and-alternative-analysis/, accessed 22 Mar 2017.

[32] Abreu, Kim. “The Myriad Benefits of Diversity in the Workforce,” Entrepreneur, December 9, 2014, https://www.entrepreneur.com/article/240550, accessed 22 March 2017.

[33] Thomas, Ted and Thomas, James. “Developing a Culture of Questioning or Don’t Tell, do Ask,” InterAgency Journal, Vol. 7, Issue 3, Fall 2016.

[34] Power, Gus. Energized Work, “Safe to Fail,” April 23, 2015, https://www.energizedwork.com/weblog/2015/04/safe-fail, accessed 22 March 2017.

Covert Action and Unintended Consequences

by John G. Breen

Introduction: The Cold War, Water Boarding, and ISIS

In the middle of the CIA's 1954 covert overthrow of the democratically-elected government of Guatemala, with waning rebel force momentum and facing calls to increase support to the insurgents with unmarked surplus WWII bombers, President Eisenhower turned to his CIA Director and asked what the chances of success would be without the additional aid. Allen Dulles responded, "About zero." When asked what the chances would be with the bombers, Dulles responded, "About 20 percent." This was a strikingly honest calculation of risk in a political environment that most would suspect was rife with yes-men. Eisenhower appreciated Dulles's rather bleak assessment: "It showed me you had thought this matter through realistically. If you had told me the chance would be 90 percent, I would have had a much more difficult decision."[1] The President ordered the planes delivered, and the coup, code-named PBSUCCESS, was, at least in the short-term, a success.

This concept of covert-action success is operationally elusive and certainly ill-defined. Some programs are easily recognized as failures—the Bay of Pigs invasion of Cuba is a commonly cited example—though it may represent more of an overt invasion rather than a more classic example of covert action. By definition, covert programs should comprise a subversive-influence act or acts undertaken secretly or with misdirection so as to remain not attributable to the U.S. Some longer-term, institutionalized programs, such as MKULTRA (the Cold War-era effort to use mind-altering drugs to sap an individual's free will, perhaps useful to create an assassin or to fully interrogate a detainee), were not only operational failures, but also seemingly undertaken with little to no moral or ethical considerations.

Other historical, covert-action programs are less easily characterized. Did operation TPAJAX, the overthrow of the democratically-elected government of Iran in 1953, provide 26 years of

John G. Breen, Ph.D., was formerly the Commandant's Distinguished Chair for National Intelligence Studies at the U.S. Army Command and General Staff College. Dr. Breen earned his Ph.D. from the University of Rochester.

relative stability and free-flowing oil? Or did it ultimately contribute to the disastrous events of 1979, with subsequent decades of instability, support to Israeli and Western-directed terrorist groups, and the pursuit of an Iranian offensive nuclear capability? Did the optimistically named PBSUCCESS operation prevent a communist takeover of Guatemala or lead to years of human rights abuse by a repressive regime? Did CIA support to the Afghan Mujahidin in the 1980s block Soviet aggression or incubate the progenitor planners and perpetrators of 9/11? Could it have resulted in both seemingly diametrically opposed outcomes?

The CIA's systematic detention and enhanced interrogation of prisoners is a more recent example of a covert-action program resulting in inconclusive operational success, with at least questionable attention to ethical/moral considerations and leading to years of Congressional inquiry and known and unknown second- and third-order unintended consequences. Was the use of the water board an effective technique to locate Osama bin Laden, or did public revelations motivate the next generation of devoted terrorists? Part of the problem is perhaps the program's revelation to the public, but a larger issue is certainly the ethical/moral nature of the activities themselves. What seemed lost in the debate was not so much if waterboarding worked, but if it was right that it was utilized in the first place.[2]

Given recent and anticipated future interest in covert-action programs, to include possible kinetic-lethal operations, it seems appropriate to ask if these efforts have a detectably positive impact on U.S. strategic foreign policy goals. An important consideration, as well, is if "success" can be something accurately assessed in the short and/or long term. Indeed, over time even successful short-term programs can give rise to a spectrum of minor to significant, deleterious, unintended consequences, such as Afghanistan covert support in the 1980s and potential connections to Al-Qaeda in 2001 or in the Middle East, with the subsequent rise of the Islamic State in Iraq and Syria (ISIS). Despite these challenges, Presidents continue to view covert- action programs as valuable opportunities to influence international events in the murky space between diplomacy and overt military intervention. And at a time when near-peer rivals seem poised to expand their spheres of influence into previously U.S.-dominated arenas (whether that be geographic, economic, and/or cyber), it may be that Presidentially-directed covert action becomes more and more attractive to deter but also prevent all out conflagration, much as it was during the Cold War. How do we focus these efforts on what works best and avoid the mistakes of the past?

> **...over time even successful short-term programs can give rise to a spectrum of minor to significant, deleterious, unintended consequences...**

Second- and Third-Order Effects: Ripples in the Pond

A review of the CIA's various covert-action programs since 1947, at least those automatically or voluntarily declassified, revealed in the press, and/or following Congressional inquiry, illustrates how unforeseen, unanticipated, or, perhaps, unappreciated consequences impact the following:

- Traditional espionage operations. The vital but characteristically low-probability effort to convince a prospective agent that a CIA case officer can keep him safe is made even more challenging when confronted with a front-page article on the latest lethal covert-action operation blown to the press.

- The international security strategy of an administration. The rapid and relatively inexpensive, short-term success of CIA's interventions in Iran and then Guatemala in the early 1950s may have influenced decades of overconfident Presidential attempts at a repeat performance. In fact, Richard Bissell, the CIA's Deputy Director of Plans, in charge of covert action during much of the Cold War, questioned in his memoirs if a victory at the Bay of Pigs might have allowed President Kennedy to either avoid Vietnam altogether, or if it would have further emboldened him to become even more engaged.[3]

It may be simply impossible to forecast the potential unintended consequences of covert action beyond the very short term...

- The public's trust in their intelligence systems. The CIA's experimentations with LSD and mind alteration, along with assassination plots, U.S. letter-opening campaigns, and infiltration of student groups in the 1950s and 1960s almost destroyed the Agency in the 1970s, when the Church Committee hearings laid bare these activities to a public still reeling from Nixon's Watergate scandal. A decade or so later, Reagan's denials that he knew about Iran-Contra suggested that either his national security apparatus was out of control, or he was simply unaware or incurious about major aspects of his administration's efforts on the international stage—either interpretation lending credence to press narrative skepticism about his suitability.

It may be simply impossible to forecast the potential unintended consequences of covert action beyond the very short term; things can spin out of control in ways unimagined and be connected to issues with unanticipated linkage.

These unintended or unanticipated consequences resulting from ill-conceived (or perhaps also well-conceived) covert operations are often called "blowback." In his memoir, Bissell devotes a chapter to his philosophy of covert action, touching on exactly this issue. He seems a particularly relevant source of insight, given his role in such pivotal covert-action programs as the U-2 spy plane incident and the Bay of Pigs invasion.

Bissell infamously told President Eisenhower that the chances of a U-2 pilot surviving a shoot down over Soviet sovereign territory was one in a million. The disastrous shoot-down and capture of U-2 pilot Gary Powers (who survived the crash), along with the botched cover story and subsequently bungled public affairs effort, wrecked the Four Powers Paris Summit Conference of May 1960, and as Stephen Ambrose described, "made [President Eisenhower] look indecisive, foolish, and not in control of his own government." With an unnerving link to CIA Director Tenet's decades-later "slam dunk" comment, Bissell code-named this last U-2 flight Operation Grand Slam—making the case that less-optimistic codenames should forever be adopted.[4,5]

The Bay of Pigs fiasco speaks for itself, but it was again Bissell who brought to the 5412 Committee the plans for the invasion and set in motion the preparation and staging of the exile insurgent troops. This 5412 Committee or "Special Group" was the President's executive body established to appraise and approve CIA covert-action programs.[6] Resulting from these episodes, particularly following the Bay of Pigs, 5412 oversight was modified. And in 1962, an embarrassed President Kennedy fired Dulles and asked Bissell to move along to another job at the CIA as the director of a new science and technology department. Seeing the job as a step down, Bissell declined and moved on.[7]

According to Bissell, it seems revelations in the press and their negative effect on CIA planners are the main problem: "Not everything a government is doing, or even just thinking about and discussing, should be disclosed—that would be the end of the skillful, subtly designed action. Publicity is the enemy of intellectual honesty, objectivity, and decisiveness."[8]

Remember that the CIA conducts both covert action and clandestine activity; these are not the same thing. The former is expected to hide (or at least obscure) U.S. involvement, to be unacknowledged but to have an observable/measurable effect, i.e., a kinetic strike, a coup, or even a covert influence campaign designed to affect the outcome of an election. In contrast, if the activity is truly clandestine, i.e., the recruitment and handling of a strategic human asset with access to vital secrets, this too is expected to hide U.S. involvement (at least to other than the recruited agent) and be unacknowledged, but no effect should be observed (other than perhaps well-informed U.S. policymakers). With the employment of rigorous assessment and tradecraft, recruitments of this sort can remain truly secret forever.

Bissell contends that in the planning stages, CIA covert-action programs should adequately address the potential for blowback, i.e., an assessment of the CIA's ability to keep a program truly not attributable to the U.S. He points out that if more objective assessments had been communicated (presumably to the 5412 Committee), many plans might have been rejected and, therefore, the number of compromised programs greatly reduced. Unfortunately, Bissell also concludes antithetically that if questionable covert actions from the Cold War had not been revealed publicly, the "cost of most of the failures would have been reported as negligible."[9]

This may be true but, perhaps, also misses the larger counterpoint that if they had remained secret and the impact of these failed programs had been considered negligible, it would have also possibly made it easier for subsequent presidential administrations to keep doing the same types of questionable things. Remember in this Cold War context that Bissell is talking about assassination, the illegal opening of U.S. mail, and wiretapping American citizens. Bissell seems to presume that negative effects follow solely from public revelation. But it must be said that ill-conceived and/or unethical programs, even if kept secret forever, appear to have an inherent potential for the proliferation of visible and wicked, unintended outcomes.

"Publicity is the enemy of intellectual honesty, objectivity, and decisiveness."

Paramilitary covert action, especially when it involves work with larger, indigenous military units, seems to greatly concern Bissell:

> Most large operations cannot be truly secret: if they involve many people (as in paramilitary activities) or a lot of money (as in political subsidies) or significant hardware development and employment (as in reconnaissance), the activities are simply too massive to be unobservable.[10]

Where does tradecraft fall into this mix, particularly with paramilitary activities? Bissell states that while it may prevent clear-cut evidence of U.S. involvement, it will always remain more of a fig leaf, with the assumption of U.S. involvement accepted as a constant risk. Revelations of this sort result in those aggrieved able to link their grievances back to the U.S. and, rightly or wrongly, seek retribution.

Covert-Action Success: Where's Bin Laden?

As a first step, might we be able to lessen the impact, if not the frequency, of unintended consequences by ensuring the efficacy of the programs themselves? David Robarge, the CIA's chief historian, believes determination of covert-action success depends on whether or not it accomplished the policy objectives it was intended to help implement.[11] In a November 2014 presentation at the School for Advanced Military Studies (SAMS) at Fort Leavenworth, Kansas, Robarge commented that these programs were historically a small share of the CIA's budget, but also politically sensitive and potentially embarrassing, misunderstood, and misused.[12] Given these challenges, both CIA planners and policymakers must understand those elements of historic, covert-action programs that led to success and those that led to failure. Robarge evaluated the CIA's historical, covert-action programs and offered such an evaluation. Perhaps adopting these operational elements can enhance the odds of program success.

...CIA planners and policymakers must understand those elements of historic, covert-action programs that led to success and those that led to failure....

Robarge's subjective evaluation of historical, declassified, covert-action programs found they were most effective when they were:

- Strategically conceived as part of an overall policy.
- Implemented early in the policy initiative.
- Had small footprints and used flexible methods.
- Allowed field officers wide latitude to adapt to changes.
- Exploited preexisting views and trends and did not try to create attitudes or magnify fringe elements.
- Gave locals the prerogative to choose outcomes.
- Were based on sound counterintelligence, reliable current intelligence, and extensive knowledge of the target.

Conversely, these programs were least effective when they were:

- Not coordinated with overt policies.
- Started late in the policy initiative.
- Were heavily managed from CIA Headquarters.
- Put many officers in the target country.
- Did not fit the target's political culture.
- Employed proxies seen as illegitimate.
- Used when the target government had popular support and/or kept control with a security service, or to salvage an otherwise failing U.S. foreign policy.[13]

The impact of this evaluative framework can be significant. President Obama commented in 2014 that he "actually asked the C.I.A. to analyze examples of America financing and supplying arms to an insurgency in a country that actually worked out well. And they couldn't come up with much." Later in this same interview, President Obama emphasized the importance of planning when he suggested:

> We have to be able to distinguish between these problems analytically, so that we're not using a pliers where we need a hammer, or we're not using a battalion when what we should be doing is partnering with the local government to train their police force more effectively, improve their intelligence capacities.[14]

A more rigorously empirical determination of whether covert interventions have a chance to be truly effective, thus, has deep implications for leadership decision making and formulation and implementation of U.S. foreign policy.

To formulate effective strategy, policymakers need the most realistic assessment they can obtain from intelligence professionals about the cost/benefit of these programs. Their policy decisions have strategic implications, short and long term, and future presidents will undoubtedly look to the CIA and other organizations to develop programs that incorporate deeper insight into their potential for success and for blowback. The CIA's ability/inability to communicate chances of covert-action success, as well as the ripples in the pond that seem to flow from these programs, will be important to their continuing utility.

Nobel Prize winning economist Daniel Kahneman in *Thinking, Fast and Slow* discusses some of the characteristic problems with planning and forecasting and offers important insights applicable to the CIA's covert-action, campaign-planning challenges. The first and perhaps most important hurdle seems to be getting past overly-optimistic intuition about how things should be or how they should proceed. He calls this element of an individual's thinking "System 1." These rapid evaluations are quite sensitive to the negative influences of many pernicious biases and are, thus, highly unreliable. Think President Bush's comments about making decisions with his gut versus Obama's more scholarly exploration of the issues. The latter would be more akin to what Kahneman calls "System 2" thinking. At its best, System 2 is a more rigorous, cognitive (and slower) approach to decision-making. While "System 1" will save your life in the split-second, "System 2" could save your life in the long run. Exploitation of "System 2" thinking and avoiding the pitfalls of "System 1" may lead to better covert-action campaign planning.

Kahneman's WYSIATI concept (What You See Is All There Is) states that even if you know the information you are receiving about a decision is skewed or even wrong, your "System 1" will process it as meaningful, and your lazy "System 2" will tend to endorse it. Crucially, it does not necessarily matter if the information you receive is complete. If the narrative sounds good, i.e., it is consistent with, for example, previously held beliefs, you will overconfidently buy it. "Indeed, you will often find that knowing little makes it easier to fit everything you know into a coherent pattern."[15] Kahneman's practical examples relate everyday scenarios, but in an intelligence context, one can imagine the pitfalls of analysts and covert-action campaign planners buying into their intuitions too comfortably. Not accounting for what Donald Rumsfeld infamously called "unknown unknowns," those issues that will inevitably arise out of (most often) bad luck and/or poor foresight, can cause the best plans to fail and estimates of campaign success to fall well short.

To formulate effective strategy, policymakers need the most realistic assessment they can obtain from intelligence professionals about the cost/benefit of these programs.

Planners and policymakers may be overly focused on the individual case in front of them. They likely do not understand or appreciate the success/failure statistics of the category to which the case belongs, i.e., the proposal in front of them versus base rates of success for historical covert-action programs of the same type. As a result, they may become overly optimistic about successful outcomes, something Kahneman might call the "inside view." Using the statistics of case-similar, covert-action program success should, therefore, permit more accurate assessments of risk/gain by providing what Kahneman calls the "outside view" or reference-class forecasting. This evaluation would importantly also allow for more accurate and objective communication with policymakers. Whether the policymakers incorporate this assessment into their decision making is another matter.

An example detailed in Tetlock and Gardner's *Superforecasting* is illustrative. As President Obama faced the difficult decision whether to launch the raid that ultimately killed Osama bin Laden, he was provided a wide range of success estimates from his intelligence community and national security representatives. Though the numbers varied widely, using a rough calculation, Tetlock and Gardner estimate that taken together they came out to a "wisdom of the group" 70 percent chance that bin Laden was in the Abbottabad compound. Despite this, Obama complained that he was actually faced with a 50 percent chance, or as he reportedly called it "a coin-toss."[16] *Superforecasting* details many of the thought-process challenges Obama faced in finally giving these estimates their due respect and making the right call. But it seems there was, perhaps, some poor risk communication on the part of his national security team. WYSIATI, and some significant "System 1" thinking, at least initially, was getting in the way of appreciating the value of his advisors' true risk calculations. What would this President have done if faced with Eisenhower's dilemma—offered only a 20 percent chance by CIA Director Dulles that the Guatemalan PBSUCCESS coup in 1954 would be successful?

...succumbing to planning fallacy means CIA planners would be susceptible to grounding decisions on delusional optimism rather than on a rational consideration of risk.

Reference Class Forecasting: Limiting the Ripples in the Pond

"Planning fallacy" is a term used to describe overly-optimistic estimates of a plan's success.[17] In the case of covert-action programs, succumbing to planning fallacy means CIA planners would be susceptible to grounding decisions on delusional optimism rather than on a rational consideration of risk. This tendency leads to overestimating gains and chances of success, while underestimating odds of failure and, perhaps, the long-term threat from ripples in the pond. To guard against and perhaps defeat these decision-making biases, Kahneman offers a step-wise, reference-class, forecasting technique.[18]

1. **Identify a historical base rate for the class of issue at hand**. In this case, we are talking, in general, about covert action, but this can be broken down to paramilitary, political, or covert influence; additional categorizations and variables of covert-action type could be accounted for and perhaps add to the specificity of the assessment.

2. **Make an intuitive prediction for success of the new covert-action campaign based on what is known so far of the case-specific challenges and opportunities**. Making the prediction in this order suggests the planner might find his or her "intuitive" assessment is driven closer to the base rate, an example of using anchoring bias to the conservative advantage.

3. **If there is no useful data on which to support or question the chances of success, the planners should stick with the historic baseline success rate.** It is usually not the case that planners in this situation would be able to easily admit that there was simply no data or useful intelligence insight into a particular program. The challenge would be in identifying information that truly was

a causative factor (not just correlative) in predicting success or failure.

4. **If the planners do feel they have strong data in support of this new program, they can move their predicted chances of success toward their intuitive, likely, more optimistic, risk assessment, but only after a rigorous review of their supporting intelligence.** Of note, Robarge's elements of successful or failed covert action may be considered one good starting point for the "supporting intelligence" on which to further evaluate an intuitive sense of chances for the plan's success.

Using declassified, historical data evaluated subjectively by CIA historian David Robarge, the base rates of success/failure of different types of covert-action programs (paramilitary, propaganda, or political) can be calculated (See Table 1, page 114).[19] From the CIA's efforts in Italy in 1948 to the most recent, declassified efforts in Afghanistan, Robarge scored 49 covert-action programs as either success, mixed, or failure (with the long-term success of the take-down of the UBL compound in Abbottabad marked as "undetermined"). Overall, Robarge's recently-updated evaluation of the programs indicates 53 percent were short-term or mixed successes, or just a bit better than a coin toss. In the long-term however, his data suggests that only about 41 percent were either successful or of mixed success—roughly 50/50 short term and 40/60 long term.

One should probably not make too much of statistics in such a subjective evaluation. A quick look at the data highlights some important issues with their interpretation. First, this is admittedly the assessment of a single historian, albeit the CIA's historian. If anything, his own unconscious bias might be to favor outcomes; therefore, even the relatively coin-toss nature of the results might suggest an overestimate of success. The true success rate, even in the short term, may be less than the coin-toss, if the listing of programs is subjected to more of a "wisdom of the crowd" evaluation.

Most programs evaluated also took place before 1980, likely owing to declassification timelines; therefore, the base rate of success data represents programs that were designed and implemented during the Cold War, early in the CIA's history, which also accounts for the anti-communist focus of about 70 percent of the programs. About 50 percent of the programs included some potentially-lethal or violent component, to include paramilitary activity, assassination plots, and/or coup. The remaining 50 percent were solely political and/or propaganda programs without an acknowledged lethal aspect.

...the CIA's focus on lethal or at least potentially-lethal covert action is nothing new.

Some have suggested that the CIA has become more focused on paramilitary activities in response to 9/11, but the table of declassified programs reveals that the CIA's focus on lethal or at least potentially-lethal covert action is nothing new. It may simply be that we go to what we know best in a time of crisis (or what is most instinctive and prone to bias—"System 1"); Communism and the threat of nuclear annihilation or 9/11 terrorism that kills thousands influences our decision making to respond decisively. When the grass rustled on the Serengeti some thousands of years ago, did we sit and wait to see if it was a lion? Or did we throw our spear, even it was just the wind or our buddy (unluckily) making his way through the tall grass.

Iran as a Case Study

How does Kahneman's step-wise, reference-class evaluation combined with Robarge's

Country/Region	Start Date	End Date	CA Type	Short-term Success	Long-term Success
Italy	1948	1976	Political	success	success
Albania	1949	1954	Paramilitary	failure	failure
Soviet Union	1949	1959	Paramilitary	failure	failure
France	late 1940s	late 1950s	Political	success	success
Western Europe	1950s	1960s	Propaganda, political	success	success
Phillipines 1	early 1950s	early 1950s	Paramilitary, Political	success	success
North Korea	1950	1953	Paramilitary	failure	n/a
China 1	1951	1956	Paramilitary	failure	failure
Tibet	1951	1972	Political, Paramilitary	failure	failure
East Asia	1951	1967	Propaganda, political	mixed	failure
Soviet Bloc 1	1951	1972	Propaganda	success	success
Iran	1953	1953	Political, Paramilitary	success	failure
Guatemala	1954	1954	Paramilitary	success	failure
Vietnam 1	1954	1956	Political	success	failure
Indonesia 1	1955	1958	Propaganda, Paramilitary	failure	failure
Soviet Bloc 2	1956	1991	Propaganda	success	success
Japan	1958	1968	Political, Propaganda	success	success
Cuba 1	1960	1963	Assassinations plots, Paramilitary	failure	failure
Congo	1960	1968	Political, Assassination plot	failure	mixed
Dominican Republic 1and 2	1960	1971	Political, Assassination plot	failure	success
Laos	1960	1973	Paramilitary	success	failure
Vietman 2	1961	1973	Political, Paramilitary	failure	failure
Cuba 2	1961	1965	Political, Propaganda, Paramilitary	failure	failure
British Guyana	1962	1971	Political	success	mixed
Chile	1964	1973	Political, Military Coup	mixed	failure

Table 1. Covert Action Program Evaluation

Source: **CIA historian David Robarge, subjective evaluation using declassified historical data.**

elements of successful covert-action programs stand up to historical case studies? One should see at least a subjective correlation between Robarge's evaluations and his determination of success/fail covert action attributes. Iran may serve as a useful case study. From the Table, one can see that the CIA's intervention in Iran in 1953 (Operation TPAJAX) was categorized by Robarge as a short-term success but an internal, political, long-term failure.

Following the end of World War II, the British economy was struggling to recover and close to bankruptcy. By 1951, Iranian Prime Minister Mohammed Mossadegh had nationalized the profitable, but UK-dominated, Anglo-Iranian Oil Company venture (which supplied 90 percent of European petroleum). While President Truman did not support military action, once Eisenhower became president, the UK focused its influence operation on convincing the U.S. that the overthrow of the Mossadegh government was about fighting communism vice UK economic concerns.[20,21,22,23] With Churchill back in power in Britain and Eisenhower in the U.S., fear of communism won the day, and Eisenhower approved a covert CIA operation to overthrow Mossadegh.

The coup itself does seem to meet Robarge's first and second elements of a successful covert action—strategically conceived as part of an overall policy and implemented early in the policy initiative. Thus, other elements of U.S. power were brought to bear, and covert action was not an afterthought. There were some signs that the Iranian nationalist government had strengthened its relationship with the Soviet Union (the Soviets had entered into financial and trade negotiations with the Iranians), and the

Country/Region	Start Date	End Date	CA Type	Short-term Success	Long-term Success
Indonesia 2	1964	1965	Political	mixed	n/a
Haiti	1965	1969	Poltiical, Propaganda	failure	failure
Thailand	1965	1968	Political	success	success
Colombia	1967	1970	Paramilitary, Political	success	failure
Bolivia 1	1967	1967	Paramilitary	success	success
China 2	1969	1972	Propaganda	failure	failure
Cuba 3	1968	1974, 80s	Propaganda	failure	failure
Angola 1	1971	1976	Paramilitary	failure	failure
Bolivia 2	1971	1971	Poltical, Propaganda	n/a	n/a
Iraq	1972	1975	Paramilitary	failure	failure
Portugal	1974	1976	Political	success	success
Afghanistan 1	1979	1987	Paramilitary	success	mixed
Nicaragua	1980s	1980s	Paramilitary, Political	success	success
Afghanistan 2	2001		Paramilitary	success	mixed
Phillippines 2	1965	1968	Political	mixed	success
Greece	1967	1967	Political	n/a	n/a
Soviet Bloc 3	1969	1970	Political, Propaganda	failure	success
Libya	1973	1974	Political	failure	failure
Angola 2	1977	1980	Propaganda	failure	failure
Grenada	1979	1983	Political	n/a	n/a
Ethiopia	1980s	1980s	Political, Propaganda	n/a	n/a
Yemen	1980s	1980s	Propaganda, Paramilitary	success	failure
International (RDI)	2002	2009	Paramilitary	mixed	mixed
Pakistan	2011	2011	Paramilitary	success	mixed (undetermined)

Table 1. Covert Action Program Evaluation (continued)
Source: **CIA historian David Robarge, subjective evaluation using declassified historical data.**

communist Tudeh Party had aligned itself with Mossadegh, at the expense of Shah Mohammed Reza Pahlavi.[24] U.S. strategic policy at the time was clearly focused on stopping the spread of communism, and Iran's petroleum reserves and strategic location made it a key buffer state against Soviet expansion. The linkage between an overthrow, keeping the Shah in power while dumping his Prime Minister, and resistance to communism does mesh with overall U.S. policy at the time. That it was justified due to an aggressive Soviet threat is less clear. After the Shah fled Iran in late February 1953, when Mossadegh first got wind of a potential coup:

> No one seemed to notice that throughout this crisis, in which the stakes were nothing less than one of the world's greatest oil pools, the Russians were content to stand aside. Nor did anyone in the West ever point out that Mossadegh had not appealed to his northern neighbor for help.[25]

An overt military takeover of all or some subset of Iranian oil fields, let alone of Iran itself, risked a conflagration that would destabilize the region. Not to mention, the UK was in no economic shape to invade, and the U.S. had been tied up on the Korean peninsula. Diplomatic efforts to seek some compromise had largely failed by August 1953. Secretary of State John Foster Dulles had ominously warned Eisenhower in a March National Security Council meeting that the Communist takeover of Iran would result in significant loss:

> Not only would the free world be deprived of the enormous assets represented by Iranian oil production and reserves, but

> the Russians would secure these assets and thus henceforth be free of any anxiety about their petroleum situation. Worse still, Mr. Dulles pointed out, if Iran succumbed to the Communists there was little doubt that in short order the other areas of the Middle East, with some 60% of the world's oil reserves, would fall into Communist control.[26]

The third and fourth of Robarge's elements also seem to have been met—the action had small footprints and used flexible methods—allowing field officers wide latitude to adapt to changes. Two of the main characters involved in the coup were famously H. Norman Schwarzkopf and Kim Roosevelt. The latter, grandson of President Teddy Roosevelt, and the former, father of Desert Storm's "Stormin Norman." The senior Schwarzkopf, who had been chief of the New Jersey State Police and involved in the handling of the Lindbergh kidnapping case, had between 1942 and 1948 trained the Imperial Iranian Gendarmerie and the Iranian Savak, the brutal internal intelligence and security service.[27] He reemerged in Iran during the coup in 1953 with "millions of dollars."[28]

...money can be an influential component of a covert-action campaign.

In the right hands and then passed along to the right hands, money can be an influential component of a covert-action campaign. But it takes someone with the operational judgement and freedom to act for it to be effective. Kim Roosevelt seems to have been the right person at the right time, influencing military units to revolt, manipulating interim leadership, and, at least on the surface, seeming to make it up as he went along. Robarge himself, writing a review of Stephen Kinzer's *All the Shah's Men* notes that:

> The [operational] design that looked good on paper, failed on its first try…and succeeded largely through happenstance and Roosevelt's nimble improvisations. No matter how meticulously scripted a covert action may be, the "fog of war" affects it as readily as military forces on a battlefield.[29]

Did Operation TPAJAX exploit preexisting views and trends and not try to create attitudes or magnify fringe elements and give locals the prerogative to choose outcomes? By the time Truman was out of the picture and the British found a more supportive Eisenhower in office, there was already growing dissatisfaction in Iran among those who preferred to see a return of the Shah.[30] Mossadegh's apparent indecision in the face of crises and his troubled relationship with the Majlis were significant factors in the political situation prior to the coup.[31]

Thus, discontent was already there, waiting for someone to exploit it, in this case with cash and propaganda. As Roosevelt saw the final act of the coup unfolding, with Iranian military units, police, and rural tribesman ostensibly under his control, he reportedly was asked by a colleague if "the time [had] come to turn General Zahedi loose to lead the crowd?"[32,33] He did so, and a two-hour battle raged outside Mossadegh's home, with Royalist troops succeeding in taking the objective by the next day; indications that Roosevelt rode into the fray on an Iranian tank seem apocryphal. Zahedi, of note, had been chosen by the Shah (not by any outside force) to replace Mossadegh, much to the consternation of the British, who acquiesced in the face of limited options.[34] In the end, and it seems reasonable to say these elements of successful covert action were met, the coup was the lucky orchestration of riots by locals and an internal, Iranian military struggle that ended happily in Mossadegh's overthrow, again at the hands of his own countrymen.

Lastly, Robarge notes that successful covert action should be based on sound counterintelligence, reliable current intelligence, and extensive knowledge of the target. The British had decades of experience in the country, at least in the oil fields, but had been officially kicked out of the country by Mossadegh. Despite this, they apparently did have an indigenous agent who retained solid bona fides with the Shah. The small number of British regional experts and a shortage of personnel dedicated specifically to Iran were cited as challenges in a CIA report following the coup.[35,36,37] The U.S. did have a Station operating, with agents recruited over a considerable amount of time and ideologically motivated.[38] CIA agents were also present inside the military in Tehran, able to ensure military cooperation and presumably report on any counterintelligence challenges.[39] Kim Roosevelt, himself an OSS Mideastern expert during WWII, had interviewed the Shah in 1947 in support of a book he was authoring, giving him good insight and early appreciation perhaps for the Shah and the region.[40] Lastly, it appears that contemporary planners understood the requirement for extensive knowledge of the target; in their once classified operational plan they noted: "The preceding material represents a Western-type plan offered for execution by Orientals. However, it was drafted by authors with an intensive knowledge of the country and its people who endeavored to examine and evaluate all the details from the Iranian point of view."[41] Of course, it goes on right afterward in a decidedly xenophobic manner to suggest:

> Given the recognized incapacity of Iranians to plan or act in a thoroughly logical manner, we would never expect such a plan to be re-studied and executed in the local atmosphere like a Western staff operation.
>
> Security among all local elements involved is a serious weakness inherent in the Persian character. We must be aware of the fact that security breaches might lead to repressive measures by Mossadeq.[42]

It was around this same timeframe, of course, in which British spy Kim Philby and the Cambridge spy ring was providing damaging information to the Soviets, and Cold War secrets flowed freely from the American nuclear program to the Russians. Western character was equally flawed, and self-awareness was one of the planners' apparent weaknesses. Despite their ethnocentrism, it seems they at least understood the counterintelligence challenges and were attempting to mitigate risks with adequate planning.

Did Iran 1953 lead to Iran 1979 to Iran 2016 to...?

The themes of public compromise, ethics and morality, and unconscious bias—the dangers of the planning fallacy—can be seen throughout the preceding discussion. Bissell proposed that successful covert action planning would need to include short- and long-term risk assessment and an appreciation for the potential that any compromise would impair CIA capabilities. He further argued that only short-term results in an operation are important, and that the CIA cannot be expected to be responsible for the long-term significance or outcome of a complicated situation:

> Most covert-action operations (like military operations) are directed at short-term objectives. Their success or failure must be judged by the degree to which these objectives are achieved. Their *effectiveness* must be measured by the degree to which achievement of the short-term objectives will contribute to the national interest. It can be argued that, although few uncompromised operations actually failed, the successful achievement of their short-term results made only a limited contribution to the national interest.[43]

His pessimism and parochialism aside, Bissell seems clear in his belief that long-term impacts are not the CIA's responsibility.

It has been said many times, at least in the aftermath of failed U.S. interventions, that there is no such thing as a policy failure, only intelligence failure. The CIA tends to accept this criticism as a normal cost of doing business. Operation TPAJAX was most clearly a short-term success, and unlike Robarge, I believe it was also a relatively, long-term, covert-action success. The coup took place in 1953, and the Shah was not overthrown until 1979. In the interim, it seems overall U.S. foreign policy was more to blame in leading to or, at least, not preventing the Shah's eventual downfall. Covert action is normally thought to give time and space for military or foreign policy interventions; 26 years seems more than enough time and space.

It has been said many times, at least in the aftermath of failed U.S. interventions, that there is no such thing as a policy failure, only intelligence failure.

Robert Jervis touches on this issue in *Why Intelligence Fails* and suggests that the Shah's liberalization program, overtly supported by the U.S., was at least partially to blame. While last minute CIA covert action was, of course, not going to fix years of poor governance, it may in fairness have been at least a failure of intelligence analysis:

> This question [the problem of liberalizing a repressive regime] was of obvious importance after the fall of 1977 when the Shah started to liberalize and when the USG [U.S. government] had to decide how much to push the Shah to liberalize, but at no time in the succeeding year was there a [CIA] discussion that was more than a few sentences long.[44]

One also cannot completely ignore the negative, long-term, unintended consequences of the 1953 coup, the ripples in the pond decades later. Noting in the same vein as Bissell the impact of public compromise, Jervis suggests the American role in Operation TPAJAX was probably known in an exaggerated version by all Iranians in the late 1970s. They would attribute American meddling to daily events and struggles, and this contributed to the view that the Shah was an American puppet. Knowledge of the U.S. role in the coup delegitimized the Shah's rule and perhaps shored up Nationalist support (in addition to religious support) for Khomeini.[45] But again, it is not at all clear the compromise and knowledge of it was causative or merely correlative.

So, the Iran case study itself is problematic in that the assessment of its success/failure is certainly subjective and possibly incomplete, as ripples still emanate. For example, as of this writing, the effects of the 1953 coup and of the 1979 overthrow seem to impact negatively on U.S./Iran diplomatic efforts and any possibility of a reframing of the relationship on the world stage. Americans of a certain age can still easily recall the painful events of 1979, watching the American hostages on TV night after night. With understandable historic bias, Iranians still believe the CIA is actively trying to undermine their country. During the 2016 election cycle, the two main candidates argued both sides of recent nuclear agreement negotiations, but neither was calling for any sort of a true reset.

Conclusions: Policymakers Need to Know If We Are Simply Guessing

As President Eisenhower, an aggressive proponent of covert action, famously said "plans are useless but planning is indispensable." Robarge's assessment of historical programs and his identified elements of covert-action success/failure provide the practitioner with a base rate for use in reference-class forecasting and guidelines, albeit subjective, for covert-action, operational planning. To extend the potential value of this work, it might be useful for more than one historian to evaluate all 49 declassified, covert-actions programs using Robarge's elements, with each element assessed with a numerical score (1–5) to see if they stand up to this empirical evaluation. Like the eponymous checklist used to rapidly evaluate newborns, we would have a checklist for covert-action campaign plans, an Apgar score for covert action.[46] If such a simple checklist could be validated, it might serve as, at least, a quick heuristic for future covert-action planners and those communicating risk to policymakers. Low scores would mean your program is not healthy and help avoid the delusion of skill in the CIA's ability to make forecasts of covert-action success.

Even using reference class forecasting and a covert-action Apgar score, it seems that unintended consequences of tactical covert actions and certainly of longer-term, covert-action campaigns simply cannot be predicted past a very short time horizon. With greater time, size, and complexity, the drip-drip of relatively low-impact ripples can suddenly and without warning, become a tidal wave of consequence. Perhaps more troubling for planners and policymakers, it is not at all certain that unintended consequences emanate uniquely from failed programs.

The original plan for Operation TPAJAX—a short-term and at least "longish"-term success example—offered an overly-broad risk assessment of a "reasonable chance of success," but at least it did address the risks of failure—if only in the short term. It did not consider any long-term negative effects that might emanate from even a successful coup.[47] These types of consequence assessments (both from failed and successful covert intervention) should be worked into formal CIA planning and assessments, as well as verbal briefings and other personal engagements with policymakers.

It seems other elements of planning should be added to Robarge's elements of covert-action success. In a previously published article, I argued that a Just Theory of Espionage derived from the Just Theory of War framework could have been used during the CIA's campaign planning to mitigate the negative consequences of the Rendition, Detention, and Interrogation (RDI) program. Perhaps now I would suggest choosing not to pursue it in the first place would have been the better course.[48] One can see the potential utility in serious consideration of ethics and morality during covert-action planning, especially if we define success in a broader fashion, including the mitigation of downstream, unintended, negative consequences.

Perhaps more troubling for planners and policymakers, it is not at all certain that unintended consequences emanate uniquely from failed programs.

So, these plans, particularly the more strategic, never survive first contact with the enemy, are close to useless as forecasting tools beyond an acute time horizon, and should be flexible to allow for adaptive leaders on the ground to adjust fire. I would also contend that the mere act of planning seems to result in greater connectivity between headquarters and the field, greater inherent consideration of ethics and morality, an enhanced sense of accountability for success or failure, and a potentially greater ability to anticipate catastrophic, unintended consequences, what Nassim Nicholas Taleb might call "black swan" events (rare but highly impactful).

In *Antifragile: Things that Gain from Disorder,* Taleb argues, by way of example, that instead of nuclear energy firms predicting the probabilities of disaster, they should instead focus on limiting exposure to failure (redundant safety measures), which would make prediction or non-prediction of failure beside the point. In many ways, Robarge's elements of covert-action success, along with my suggested addition of ethical/moral considerations are these redundant safety measures.

As a practitioner, I appreciate Taleb's focus on the value of trial and error: "We can, from the trial that fails to deliver, figure out progressively where to go."[49] This sort of trial and error-based tinkering has certainly been going on with CIA covert-action planning over the years. Though the term "tinkering" gives the method a seemingly less-than-serious note, this sort of learning can be effective, especially when early covert-action programs (perhaps simply from good luck) provided some positive examples from which to learn valuable lessons applicable to subsequent campaigns. As a colleague of mine joked: "The CIA has a two-step planning process. We are told what to do, and then we do it." Though an exaggeration, the comment does capture the less doctrinaire nature of historical CIA planning, especially when comparing it to the more mature military decision making process (MDMP), operational art, or operational design. Robarge's covert-action success base rates, therefore, might be thought to represent the results of an anti-fragile discovery process based on CIA tinkering (good and bad) since 1947. With a gradual increase in military presence and influence at CIA since 9/11, there has also likely been an equal or at least detectable increase in military-planning expertise buoying this historical tinkering. Perhaps a study done by a future CIA historian will show the covert-action success rate following this enhanced collaboration moving up into ever more satisfying percentages.

Finally, I suspect that the relationship between the final cost of covert-action failure and either public compromise or lack of ethical consideration is non-linear. The damage caused when these programs are inappropriately revealed to the public or when ethics is not considered during planning is much greater than one would intuitively expect, greater than 1-1. Taleb might say covert-action programs are extremely fragile to compromise and immorality. The onus, therefore, is on the CIA to ensure these elements are deeply explored during the covert-action planning process and communicated accurately. Public compromise makes the programs attributable; lack of moral standards makes the CIA and policymakers culpable. ***IAJ***

All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the Central Intelligence Agency (CIA) or any other U.S. government agency. Nothing in the contents should be construed as asserting or implying U.S. government authentication of information or CIA endorsement of the author's views. This material has been reviewed by the CIA to prevent the disclosure of classified information.

NOTES

[1] Evan Thomas, *Ike's Bluff: President Eisenhower's Secret Battle to Save the World*, Little, Brown and Co., New York, 2012, pp. 140–141.

[2] John G. Breen, "The Ethics of Espionage and Covert Action: The CIA's Rendition, Detention and Interrogation Program as a Case Study," *InterAgency Journal*, Vol. 7, No. 2, 2016, p. 76.

[3] Richard Bissell, *Reflections of a Cold Warrior: From Yalta to the Bay of Pigs*, Yale University Press, New Haven, CT, 1996, p. 151.

[4] Thomas, pp. 370–371.

[5] Stephen Ambrose, *Ike's Spies: Eisenhower and the Espionage Establishment*, Anchor Books, New

York, 2012, p. 280.

[6] Myra F. Burton and Adam M. Howard, *Foreign Relations of the United States, 1977–1980*, Volume XVI, United States Government Publishing Office, Washington, 2016, note on U.S. Covert Actions, p. XXIX.

[7] Central Intelligence Agency, "The People of the CIA ... Richard Bissell: An Agency Leader," October 6, 2016, <https://www.cia.gov/news-information/featured-story-archive/2012-featured-story-archive>, accessed on February 13, 2017.

[8] Bissell, p. 205.

[9] Ibid., p. 207.

[10] Ibid., p. 217.

[11] Dr. David Robarge, personal communication.

[12] Dr. David Robarge, "CIA and Covert Action," presentation at the U.S. Army's School of Advanced Military Studies, Fort Leavenworth, KS, November 12, 2014.

[13] Ibid.

[14] David Remnick, "Going the Distance," *The New Yorker*. June 26, 2015, <http://www.newyorker.com/magazine/2014/01/27/going-the-distance-david-remnick>, accessed on February 13, 2017.

[15] Daniel Kahneman, *Thinking, Fast and Slow*, Farrar, Straus, and Giroux, New York, 2013, p. 87.

[16] Philip E. Tetlock and Dan Gardner, *Superforecasting: The Art and Science of Prediction*, Random House Books, London, 2016, p. 210.

[17] Kahneman, p. 250.

[18] Kahneman, pp. 190–192.

[19] Robarge, personal communication.

[20] Ambrose, pp. 189–198.

[21] Torey L. McCurdo, "The Economics of Overthrow: The United States, Britain, and the Hidden Justification of Operation TPAJAX," *Studies in Intelligence*, Vol. 56, No. 2, June 2012, pp. 15–26, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-2/pdfs/McMurdo-The%20Economics%20of%20Overthrow.pdf>, accessed on February 13, 2017.

[22] "The Secret CIA History of the Iran Coup, 1953," <http://nsarchive.gwu.edu/NSAEBB / NSAEBB28/>, accessed on February 13, 2017.

[23] Central Intelligence Agency, "The Agency and the Hill," July 5, 2012, pp. 261–262, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/agency-and-the-hill-The Agency and the Hill_Part2-Chapter9.pdf>, accessed on February 13, 2017.

[24] Ambrose, p. 199.

[25] Ambrose, p. 198.

[26] *Foreign Relations of the United States, 1952–1954*, "Iran, 1952-1954," Volume X, Office of the Historian, U.S. Department of State, <https://history.state.gov/historicaldocuments/frus1952-54v10/pg_693>, accessed on February 13, 2017.

[27] Ambrose, p. 193.

[28] Ambrose, p. 204.

[29] Central Intelligence Agency, "All the Shah's Men: An American Coup and the Roots of Middle East Terro," June 27, 2008, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no2/article10.html>, accessed on February 13, 2017.

[30] Central Intelligence Agency, "The Agency and the Hill," p. 262.

[31] McCurdo, p. 23.

[32] Ambrose, p. 210.

[33] Central Intelligence Agency, "The Agency and the Hill, p. 263.

[34] Ambrose, p. 201.

[35] Central Intelligence Agency, "The Agency and the Hill, p. 263.

[36] Central Intelligence Agency, "Overthrow of Premier Mossadeq of Iran," p. 87, <http://www.nytimes.com/library/world/mideast/iran-cia-main.10.pdf>, accessed on February 13, 2017.

[37] Ibid., p. viii.

[38] Ibid., p. 92.

[39] Ibid., p. ix.

[40] Ambrose, p. 192.

[41] Central Intelligence Agency, "Overthrow of Premier Mossadeq of Iran," Appendix B.

[42] Ibid.

[43] Bissell, pp. 218–220.

[44] Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*, Cornell Paperbacks, Ithaca, NY, 2010, p. 63.

[45] Jervis, p. 89.

[46] Kahneman, p. 227.

[47] Central Intelligence Agency, "Overthrow of Premier Mossadeq of Iran," pp. 26–27.

[48] Breen.

[49] Nassim Nicholas Tale, *Antifragile: Things That Gain from Disorder*, Random House Trade Paperbacks, NY, 2012, p. 192.

Contributors Wanted!

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

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)

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.

We're also looking for book reviews!

Submit a book review or suggest a book to review to editor@TheSimonsCenter.org.

Contact the Arthur D. Simons Center for Interagency Cooperation

www.TheSimonsCenter.org • editor@TheSimonsCenter.org
www.facebook.com/TheSimonsCenter
Location: 655 Biddle Blvd., Fort Leavenworth, KS 66027
Mailing Address: CGSC Foundation, 100 Stimson Ave., Suite 1149, Fort Leavenworth, KS 66027
913.682.7244 - office • 913.682.7247 - fax

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

Worth Noting

Hackers target nuclear facilities

In early July, the New York Times published a piece detailing how hackers have been targeting the computer networks of nuclear power stations, energy facilities, and manufacturing plants. The revelation came from a joint report from the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), and was confirmed by security specialists who responded to the cyberattacks.

The hackers' methods included sending fake resumes with malicious code to senior industrial control engineers and "watering hole" and "man-in-the-middle" attacks. The DHS/FBI report did not disclose if the attacks were an attempt at espionage or how many facilities were targeted, but did indicate that an "advanced persistent threat" actor was responsible and that the hackers' actions were similar to a known Russian hacking group.

According to the report, the attacks have been occurring since May, around the same time President Trump signed the new Executive Order on cybersecurity, which focused on protecting federal networks and critical infrastructure.

- ***The New York Times***

Cyber Guard tests cyber force's skills

In June, U.S. Cyber Command (Cybercom), the Department of Homeland Security (DHS), and the FBI led the sixth annual, week-long Cyber Guard exercise in Suffolk, Virginia. Over 700 participants from across U.S. government and military, as well partners in academia, industry, and around the world took part in the event.

Cyber Guard 2017 pitted Cybercom's Cyber Mission Force personnel and those from other state and federal organizations against a broad range of high-stakes cyber scenarios. The exercise ran participants through possible situations that would occur in the event cyberattacks knock out critical infrastructure, such has the electrical grid and financial sector.

Navy Admiral Michael S. Rogers, commander of Cybercom, spoke at the opening of the exercise, saying "I will accept failure in a training environment if it generates knowledge and insight that makes us better… What I constantly tell the team leads is it's about pushing the envelope. It's about challenging your teams, and it's about trying different things."

Coast Guard Rear Adm. David M. Dermanelian, Cybercom's training and exercises director, described Cyber Guard as "the most realistic training environment possible," noting that the exercise is maturing at an impressive rate. Air Force Lt. Gen. J. Kevin McLaughlin, Cybercom's deputy commander also remarked on the growth of the exercise, commenting that "Every year, we learn something new that we wish we would have thought about the year before."

While this was the sixth iteration of the Cyber Guard exercise, it was only the second year that incorporated international partners, devoting an entire day to highlight the importance of multinational cooperation.

- Department of Defense

2017 Trafficking in Persons report released

On June 27, the Department of State released the 2017 Trafficking in Persons (TIP) Report. Secretary of State Rex Tillerson and Ambassador-at-Large to Monitor and Combat Trafficking in Persons Susan Coppedge each addressed the report in separate briefings, speaking about the global tragedy of human trafficking and the responsibility of governments to bring an end to this crime.

The State Department's TIP Reports highlight strategies to prevent human trafficking around the globe, analyzing governments' prosecution, protection, and prevention efforts. The focus of the 2017 TIP Report is the responsibility of governments to criminalize human trafficking in all its forms, as laid out in the Palermo Protocol, which was adopted in 2000. In his remarks, Tillerson spoke of the need to root out members of law enforcement and the military who are complicit in the trafficking of persons, while Coppedge asserted that victims of human trafficking should not face charges for criminal acts they may have committed due to coercion and exploitation.

The 2017 TIP Report assesses countries' anti-trafficking efforts, measuring government efforts across the 3P paradigm – prosecuting traffickers, protecting victims, and preventing the crime. While governments have made progress to criminalize all forms of human trafficking and strengthen victim protections, traffickers continue to exploit millions of victims around the world.

In his opening letter, Tillerson recognizes the global scope of trafficking and the need to cooperate with international partners, through governments, civil society, law enforcement groups, and survivors of trafficking.

- Department of State

Conference focuses on civ-mil relations

The Center for Strategic & International Studies (CSIS) recently hosted an all-day conference focused on relations between the military and the civilian world. "Command Climate: The State of U.S. Civil-Military Relations" took place on May 23, with panelists representing the Department of Defense (DoD) and other U.S. government entities discussing different aspects of civil-military relations.

The first panel focused on the role of the military in policy making. Panelists discussed DoD's role in whole-of-government planning and strategizing, emphasizing the importance of civ-mil cooperation to achieve the best possible outcomes in U.S. operations.

Dr. Kori Schake, Research Fellow, Stanford University, touched on breakdowns in communication and cooperation between civilian and military operators, saying that differences in agency and department cultures can impede adaptiveness, while Dr. Janine Davidson, former Undersecretary of the Navy, pointed out that these problems are sometimes the result of civilian agencies being tasked with missions they have no training for.

In his remarks, Admiral William Gortney, U.S. Navy (ret.), stressed that DoD must not be perceived to be "in charge." Instead, Gortney said DoD's role was to provide support to other agencies and departments involved. Major General Richard Clarke, Vice Director for Strategic Plans and Policy, Joint Staff, J-5, expressed similar views, saying that while military's part of the overall mission is "easy, measurable, quantifiable," the focus should not be on the military at the expense of the civilian agencies.

The two other panels focused on the military's role in politics and their relationship with the public.

- Center for Strategic & International Studies

President of Special Forces Association "Bull" Simons chapter visits Simons Center

Mr. Terry Buckler, President of Chapter 29 of the U.S. Army Special Forces Association, visited the Simons Center on June 6. Chapter 29 is the Colonel Arthur D. "Bull" Simons Memorial Chapter of the Special Forces Association, and serves the greater Kansas City metropolitan area.

Colonel Arthur "Bull" Simons led the Son Tay Raid, a rescue operation of American prisoners of war being held in North Vietnam, on 21 November 1970. Buckler was the youngest member of the Son Tay Raiders, and was interested in the Simons Center and its association with "The Bull." During his visit, Mr. Buckler spoke about the preparatory training and conduct of the Son Tay Raid operation.

Program Director Rod Cox gave Buckler a tour of the facility and briefed him on the mission and history of the CGSC Foundation and the Simons Center, including the story behind Mr. Perot's decision to name the Center in Colonel Simons' honor.

- Simons Center

Greater interagency cooperation needed to thwart transnational organized crime

RAND Corporation recently published a report on countering the expansion of transnational criminal networks (TCNs) involved in trafficking drugs, persons, weapons, and other illicit goods. These networks pose a serious threat to U.S. national security and security interests in the Western Hemisphere, especially those that with ties to terrorist groups.

RAND's report analyzes two transnational criminal pipelines originating in South America. The report aims to identify the operational characteristics of TCNs and strategic alliances among criminal groups; examine how TCNs threaten U.S. interests; describe and analyze U.S. government policies and programs to combat these networks; and identify potential U.S. Army roles to combat TCNs.

Countering TCNs will require whole-of-government and international approaches. Among RAND's recommendations is the need for improved interagency coordination, with RAND suggesting that the National Security Council be made responsible for coordinating the activities of the departments and agencies involved in counter TCN efforts. RAND also recommends the Army help develop interagency and multinational strategies to counter TCNs, and that Army leaders encourage their units to take advantage of training opportunities with joint interagency task forces.

- RAND Corporation

Senior Executive Service reform needed

The National Academy of Public Administration recently published a book concerning the role of the Senior Executive Service (SES) nearly forty years after the SES was created. Building a 21st Century Senior Executive Service is the result of a November 2014 Brookings Institution summit that focused on modernizing the SES.

The book is a collection of perspectives on the SES from the nation's most respected public sector leaders, and includes 23 recommendations for reforming the SES and meant to enable the SES to best lead across the whole-of-government to address pressing 21st century challenges. Authors include the Honorable Michele Flournoy, Ambassador Patrick Kennedy, Admiral Thad Allen (USCG, retired), among others.

- National Academy of Public Administration

Cybersecurity order finally released

On May 11, the Trump administration released the long-delayed Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. The order calls for government agencies to follow best cybersecurity practices and holds agency leaders accountable for security breaches.

Department of Homeland Security (DHS) Secretary John Kelly spoke about DHS's cybersecurity efforts and the new executive order, saying "DHS has long been a leader in protecting our nation against cyber threats and this executive order reaffirms our central role in ongoing cybersecurity efforts." While other government agencies are responsible for the cybersecurity of their networks, the executive order build's on DHS's legal authorities and directs DHS to lead efforts to ensure a baseline of security across the civilian executive branch.

The executive order calls on DHS to coordinate with other departments and agencies to protect critical infrastructure that is vulnerable to cyberattacks, including commerce, communications, defense industry, and the electric grid. The order also promotes "an open, interoperable, reliable, and secure internet," directing interagency teams to report on options for protecting the American people from cyber threats and develop an international cybersecurity engagement strategy.

- Department of Homeland Security

House passes Intelligence Authorization Act

On May 3, the House of Representatives passed the Intelligence Authorization Act (IAA) for Fiscal Year 2017. The bill ensures that the programs and activities of the U.S. intelligence community are authorized by law, fully resourced, and subject to rigorous congressional oversight.

The IAA provides urgent funds and authorities to help thwart potential attacks and deny these terrorists safe haven in Iraq, Syria, North Africa, and elsewhere.The bill also provides the means to counter significant threats from nation-state actors, and bolsters counterproliferation and counterintelligence capabilities.

The IAA also establishes within the executive branch an interagency committee to counter Russian activities to influence the U.S., like the interference with the 2016 presidential election. The committee will include representative from various U.S. departments and government entities, including the Director of National Intelligence, the Federal Bureau of Investigation, and the Departments of State and Defense.

- U.S. House of Representatives Permanent Select Committee on Intelligence

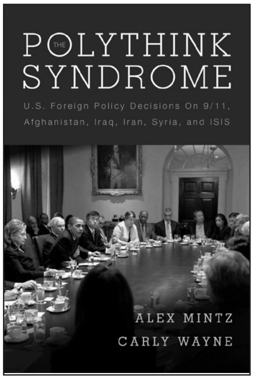
Ambassador Moon visits Fort Leavenworth

Ambassador (Ret.) Patrick S. Moon, former U.S. Ambassador to Bosnia and Herzegovina and former Deputy Assistant Secretary of State for South and Central Asian Affairs, visited the Leavenworth area 26-28 April where he shared his expertise as part of the Simons Center's Interagency Speaker Series program.

Ambassador Moon met with students at the University of Saint Mary, where he discussed the important role of women in the development of the Balkans, the various on-going U.S. efforts in Afghanistan, and public service as a Foreign Service Officer with the Department of State. He also met with several seminars of U.S. Army Command and General Staff College students and faculty, where he discussed the topics of European Security Affairs and Country Team operations.

- Simons Center

Book Review



The Polythink Syndrome: U.S. Foreign Policy Decisions on 9/11, Afghanistan, Iraq, Iran, Syria, and ISIS

Alex Mintz and Carly Wayne

Stanford University Press, 2016, 200 pp.

Reviewed by by Lt. Col. Todd Schmidt, U.S. Army
Military Research Fellow
Arthur D. Simons Center for Interagency Cooperation

Why do elite decision-makers often make sub-optimal decisions? This is the primary research question driving the theory and empirical analysis offered in *The Polythink Syndrome* by Alex Mintz and Carly Wayne.[1] The authors propose "polythink," an alternative theory to "groupthink," a dynamic characterized by *uniformity* of opinion. Polythink, on the other hand, features a *plurality* of opinions that results in intragroup conflict, disjointed decision-making process, and decision paralysis as each group member pushes for their preferred policy action. The authors support their theory with meticulous, systematic and illustrative case study analysis spanning decisions from 9/11 to the final years of the Obama administration. They demonstrate the symptoms and implications of their theory for elite, small-group decision-making in foreign policy arenas, and offer prescriptions and strategies for avoiding negative aspects of polythink, while taking advantage of its useful qualities.

Polythink offers an equally problematic phenomenon to groupthink, a leading theory in foreign policy decision-making explored by Yale Research Psychologist Irving Janis. Understanding polythink requires understanding groupthink for context, comparison and contrast. Groupthink theory describes natural psychological tendency and pressure within small groups to maximize unanimity and uniformity; minimize dissent and conflict; fail to consider, analyze and evaluate all feasible options; ignore limitations of their decisions; and overestimate the odds of success. Conformity of thought results in stifled creativity and little independent thought. It is "a mode of thinking that people engage in when they are deeply involved in a cohesive in-group, when the members' striving for unanimity override their motivation to realistically appraise alternative courses of action."[2]

The book is an important contribution to international relations and the foreign policy analysis literature for four primary reasons. First, its release at a time of presidential administration transition makes it a timely alternative theory to groupthink. Secondly, with its 21st century focus, it is a contemporary addition to the decision-making models outlined in Graham Allison's *Essence of Decision*. Additionally, it provides explanations for international relations scholars, and high-ranking civilian and military practitioners seeking to understand why elite decision-makers engage in flawed decision-making process resulting in flawed policy that produce flawed policy outcomes. Finally, for students of civil-military relations, the case studies provide important applications and lessons for highly competitive organizations. They demonstrate how intra-departmental or interagency decision-making can be influenced and potentially flawed through "expert-novice" divides, as well as manipulating leader-follower relationships.

In contrast, polythink is a theory of small-group, elite decision-making that is fraught with intragroup conflict and disunity, disagreement and plurality of opinions, divergent and disjointed recommendations, paralysis and inaction. Challenges arise because of differing world views, political and institutional considerations and affiliations, personality and leadership traits, competing expert-novice perspectives, and unaligned leader-follower interests, goals and objectives. Symptoms include conflict, turf battles, leaks, confusion, disjointed communications, limited options, little or no appraisal of critical information, compromised position-taking, and paralysis.

The authors explore foreign policy decision-making in five major case studies: the 9/11 Attacks; Afghanistan War Decisions; Iraq War Decisions; the Iranian Nuclear Dispute; and foreign policy challenges surrounding Syria, the Israeli-Palestinian Conflict, and the Islamic State of Iraq and Syria. Each case study is analyzed using a rubric that demonstrates the symptoms of polythink, as well as normative, value-driven differences, expert-novice divides, and leader-follower relationships within elite, small-group, decision-making bodies.

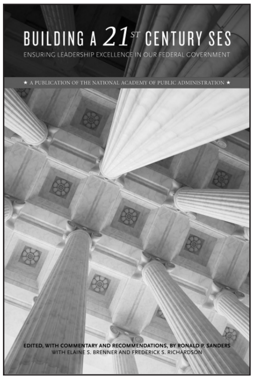
The authors' theory assumes decision-making process is a human process and state decisions are human decisions. To understand human decision-making, we must understand the human process. Understanding microfoundations in international relations and foreign policy analysis is critical to identifying elite, small-group decision-making dynamics. Is the small-group competitive, collegial, formal or informal? Identifying and understanding these group dynamics can help identify potential flaws to which the small-group may be susceptible. Collegial groups are more susceptible to groupthink symptoms, while competitive groups are more susceptible to polythink symptoms.

In conclusion, the authors suggest there are positive qualities inherent in polythink that can be exploited. Strong leadership, clear vision, unambiguous goals and objectives, open discussion, diverse membership, and a balanced process can exploit polythink inherent advantages. Advantages include increased effectiveness and efficiency at which diverse groups learn, adapt, and remain agile in the ability to confront and negotiate a complex and chaotic international environment. This book is highly recommended for foreign policy analysis scholars, as well as for students of civil-military relations and senior-executive elites in civilian and military leadership positions. ***IAJ***

NOTES

[1] Mintz serves as Chairman of the Israeli Political Science Association, Director of the Institute for Policy and Strategy at the Interdisciplinary Center (IDC), Herzliya, Israel. Wayne is a PhD candidate at University of Michigan. Both authors' research and scholarship is deeply grounded in International Relations and Foreign Policy Analysis and Decision-making.

[2] Janis, Irving, *Victims of Groupthink: A Psychological Study of Foreign Policy Decisions and Fiascos*, (2d ed), (Boston, MA: Houghton Mifflin, 1982), 9.


BUILDING A 21ST CENTURY SES
ENSURING LEADERSHIP EXCELLENCE IN OUR FEDERAL GOVERNMENT
A PUBLICATION OF THE NATIONAL ACADEMY OF PUBLIC ADMINISTRATION
EDITED, WITH COMMENTARY AND RECOMMENDATIONS, BY RONALD P. SANDERS
WITH ELAINE S. BRENNER AND FREDERICK S. RICHARDSON

Building a 21st Century SES Ensuring Leadership Excellence in our Federal Government

Edited by Dr. Ronald P. Sanders with
Dr. Elaine S. Brenner and Frederick S. Richardson

The National Academy of Public Administration, 2017, 327 pp.

Reviewed by Ralph Erwin
Senior Geospatial Intelligence Officer and
National Geospatial-Intelligence Agency liaison –
U.S. Army Command and General Staff College

Building a 21st Century SES Ensuring Leadership Excellence in our Federal Government provides some valuable insight into the thought processes, experiences, and analysis behind decisions that senior government officials have had to make in the pre-9/11 era. In addition to chapters from various senior government officials, the editor provided ample introductions with a bottom line up front, numerous challenges, much commentary, many recommendations, and a conclusion. I did grasp many "war stories" and very few 21st century course-charting anecdotes. Very few short articles actually addressed building blocks or a way ahead for future government leaders.

In their writings, it appears that some of the senior government officials were not in touch with a Generation X and Y workforce that has different aspirations. These generations have to be developed much differently than the Baby Boomers, and I mean this as a revolutionary transformation requirement. Stephen Shih did provide a possible road map for the next generation:

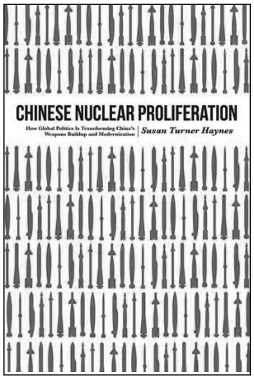
> …SES leaders will need to possess heightened people skills to manage and influence a multigenerational workforce and diverse multisector groups of national and often international stakeholders. Federal agencies and other organizations will no longer succeed with only a local or even regional focus, nor can they be led only by senior leaders with conventional competencies involving traditional top-down project management approaches confined to local silos and narrowly confined operational responsibilities.

There seemed to be abundant discussion of Executive Core Qualifications and very little discussion of how to achieve those qualifications. Ms. Long and Admiral Allen did talk about talent management development and lifelong learning, which led me to assess that those on hiring panels won't get to the most capable individual because their executive model is stuck in the 20th century standards. Robert Tobias clearly addressed the urgent requirement for collaboration, self-development, and self-awareness – some qualities of emotional intelligence for the individual. Robert Corsi approached SES development by discussing key positions, mobility, career broadening, and even following the military officer development model. Suffice it to say, not all U.S. military officer development programs are managed the same or efficient.

As with many government mandates, if the well-defined goals of the December 15, 2015, White House-issued Executive Order on *Strengthening the Senior Executive Service* are followed by current senior executives, the annual talent management and succession planning process to assess the development needs of all SES members as appropriate would help to inform readiness decisions about hiring, career development, and executive reassignments and rotations.

Robert Goldenkoff provides important counsel when he states "Instead of a position-based approach to succession planning, they [GAO] use a more strategic, scenario-based approach that emphasizes strengthening both current and future organizational capacity, focusing on the skills and competencies necessary to carry out today's mission and over-the-horizon requirements."

I recommend that both aspiring government leaders and those managing these executives-to-be, review the Executive Order and note the recommendations of the editor, which is the most valuable part of this paper. ***IAJ***


CHINESE NUCLEAR PROLIFERATION
How Global Politics Is Transforming China's Weapons Buildup and Modernization
Susan Turner Haynes

Chinese Nuclear Proliferation: How Global Politics Is Transforming China's Weapons Buildup and Modernization

Susan Turner Haynes

Potomac Books, 2016, 198 pp.

Reviewed by Kailah Murry
Department of Army civilian at the U.S. Army Command and General Staff College, and Military Intelligence Warrant Officer in the Kansas Army National Guard

Susan Turner Haynes tackles the issue of Chinese nuclear proliferation in *Chinese Nuclear Proliferation: How Global Politics Is Transforming China's Weapons Buildup and Modernization*. This book attempts to answer, "Why [is] China the only nuclear weapon state recognized under the Nuclear Nonproliferation Treaty that continues to pursue qualitative and quantitative advancements in its nuclear force." Haynes endeavors to provide background and clarity to China's buildup of its nuclear weapons program through utilizing primary sources. This book is a great read for those who do not have a firm grasp on politics or national security studies with a focus on China.

Haynes begins by introducing the reader to the need for the research, essentially, "China is the only state that has chosen to pursue… advancements to its nuclear force since the end of the Cold War." Which, according to the author, is unlike the United States, Russia, Great Britain, and France; all of whom have reduced their arsenal. Various policies are then discussed, noting that the surprise to the advancements rests in the fact that China has "repeatedly emphasized a desire for the complete prohibition and thorough destruction of nuclear weapons." The introduction provides the initial context for the data presented in the rest of the book.

The rest of the book follows what one would find in a normal thesis format. Chapter one is a literature review on nuclear strategy; specifically Haynes goes into depth on deterrence strategy, existential deterrence, minimum deterrence, limited deterrence, extensive deterrence, and maximum deterrence. Chapter two outlines empirical evidence while examining the capabilities and nuclear force levels of the United States, Russia, Great Britain, France, and China. Chapter three expands on how China defines and implements deterrence and what type of nuclear strategy it is following while discussing the impetuses behind any nuclear evolution China is making. The remaining chapters discuss the influence of the United States, other regional powers, and the idea of prestige and how this affects China. The conclusion wraps the research together and offers policy advice for the future.

The best portions, and where perhaps the reader will get the most out of the book, discuss the influence of the United States, other regional powers, and the idea of prestige. The author notes that experts believe that the "international [environment has] the most impact on a state's security decisions" and the recurrent notation in Chinese literature of the international environment would lend credence to this being true for China's shaping policies. Specific to the United States, "literature reveals that China perceives U.S. military advancement… [as] a shift… from limited deterrence to maximum deterrence." Shifting from the United States, the regional powers discussed are India, Pakistan, Russia, Japan, Taiwan, North Korea, and Iran. Haynes discusses the intent of each regional power and then deliberates if there are the means available to accomplish what that power may seek in relation to Chinese nuclear proliferation. What is presented is by no means a surprise to those well-read in nuclear policy, but can be of value knowing how the other powers view China. Then the idea of prestige is further explored through acquisition, enhancement, and the pace of growth for the Chinese arsenal. After reading the portions relating to how these factors influence China, Haynes concludes the book by offering policy recommendations for both the international community and, separately, the United States.

In closing, Haynes offers ways to reverse the trend of Chinese proliferation through bilateral agreements between the U.S. and China, additional requirements on already agreed upon treaties, and having the U.S. clarify intent regarding China and Chinese relations. Each of these recommendations, again, are not new to the community. And, unfortunately, are obvious ways forward to possibly reduce not only the Chinese proliferation, but misunderstandings between countries regarding intent. The conclusion should have gone beyond what is already available, such as policies and talks, and could have used some creative thinking to go beyond the paper and pen between China and those interested in its proliferation.

Overall the book is a good read for those new to national security studies or nuclear policy studies with a focus on China. However, the book falls short in providing additional insight beyond what could be considered a basic to intermediate level of investigation. Conversely, Haynes does make an argument against the experts who view China's nuclear deterrence strategy as one dimensional; she challenges the expert by noting "analysts in the West will sometimes erroneously equate a change in one dimension of China's nuclear strategy with a change in its overall strategy." The book foreword notes, "This book will be of use to casual China watchers and military experts alike." I would disagree. The book is great for the casual China watcher, but will only provide slight additional insight or a possible alternate argument to the expert who likely has read through the same data Haynes utilized. ***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.

The articles published in the *IAJ* represent the opinions of the authors and do not reflect the official views of any United States government agency, the Department of Defense, the Department of the Army, the U.S. Army Command and General Staff College, the Command and General Staff College Foundation, the Simons Center, or any other non-government, private, public or international organization.

Contributions:
The Simons Center encourages the submission of original articles based on research and/or which stem from lessons learned via personal experiences.

Copyright:
Publications released by the Simons Center are copyrighted. Please contact the Simons Center for use of its materials. *InterAgency Journal* should be acknowledged whenever material is quoted from or based on its content.

Copyright Transfer Agreement:
By virtue of submitting a manuscript, the author agrees to transfer to the Simons Center for the Study of Interagency Cooperation full ownership of all rights, titles, and interests, including the copyright in and to the work submitted.

Acceptance of this agreement further signifies the author represents and warrants that he/she is the sole author and sole proprietor of all rights in and to any portion of the work; that the work is original and not in the public domain; that it has not been previously published; that it does not violate or infringe on any personal or property rights of others; that it contains nothing libelous or contrary to law; and that he/she has full power to enter into this agreement.

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.