AIR WAR COLLEGE

AIR UNIVERSITY

SACRED COWS AND STUBBORN MULES:

THE IMPERATIVE TO REFORM THE US CODE

by

Brian K. Lehew, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Grant T. Hammond

14 February 2013

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel Brian K. Lehew is a Pennsylvania Air National Guard air battle manager assigned to the Air War College, Air University, Maxwell AFB, AL. He graduated from the University of Pittsburgh in 1994 with a Bachelor of Arts degree and the Pennsylvania State University in 2001 with a Master of Fine Arts degree, both in English writing. His civilian career endeavors include freelance writing, public relations, human resources, and teaching undergraduate English. He most recently served on the National Guard Bureau Joint Staff as Chief, Joint Collective Training where he devised, resourced and implemented joint training doctrine, policies and events for unified action of all joint domestic National Guard operations under US Northern Command. Prior to that, he established and commanded a one-of-a-kind air defense squadron under North American Aerospace Defense Command (NORAD) to execute aircraft early warning and joint active air defense for the National Capital Region as well as facilitate interagency collaboration in the air domain. He is a command air battle manager and a Joint Interface Control Officer. Lt Col Lehew has supported several stateside and overseas deployments that stem back to his active duty enlistment as an Airman Basic in 1986.

Abstract

The intent of this paper is to inspire informed, proactive debates on the structure of the US Code (USC), the imperative for rapid information sharing among government departments, state and local stakeholders, and US citizens, and the need for an overarching interagency mandate akin to the Goldwater-Nichols Act. Over the next 20 years, machine-speed information sharing will prove critical to security. Rapid technological advances and low-cost, high-yield weaponry will provide state, non-state and individual actors the capacity to threaten US national security. Such attacks and the response to them may infringe upon legal boundaries in ways that cause the US to violate its own traditions. Debate must definitively join or decouple legal sacred cows from their practical impact on information sharing and security. This paper does not advocate specific outcomes to those debates. Instead, it argues that despite concerted government efforts to achieve balance between security and liberty in the daily practice of information sharing, procedures to collect, process, evaluate and disseminate critical security information remain disjointed. As the government reference for consolidated law, USC interpretive clarity is masked by disorganization. That disorder encourages vacillating interpretations as presidents, senators, congressmen and departmental lawyers come and go. Revision of the USC must define and refine the interagency. Without an overarching interagency mandate within the USC, individual departments will continue to depend on work-arounds to meet whole of government ends. While work-arounds have proven to be steps in the right direction, they may gradually erode the intent of the laws they slalom through. In the information realm, achieving synergized, high-speed interagency fusion is a vital national interest requiring proactive legal license.

Introduction

A week has passed since the US East coast suddenly went dark on Christmas Eve, 2033. In the cities, hunger, thirst, and winter's cold supplant questions about what happened. From Manhattan to Miami, 118 million Americans instead contemplate survival. The machines and systems that sustain order lay inert. Fear, helplessness and distrust devolve civility into rioting and hoarding. As hospitals close, critical patients die. Hypothermia contributes more death. Tainted water and poor sanitation begin to vector disease. Washington DC is ground zero.

With each day, the means to restore order deteriorate. Local authorities improvise in a communications vacuum reminiscent of the early 19th century. Under the duress of pleading refugees and the alternative of chaos, some military commanders had declared Martial Law, upsetting preordained US Northern Command contingency dual-status command structures. Chaos also served as impetus for the President's own region-wide counter order yesterday. Affected civil leaders acquiesce due to urgency, but cannot spread the word. Media in the Western US dissect unprecedented state sovereignty infringements. Western governors reaffirm assistance compacts and reassert their own contingency plans. On the ground, the Defense Department joins ranks with police and the National Guard. Unity of command remains unresolved. Local emergency compacts, ad hoc arrangements, and the collective survival instincts of colonels, police chiefs and citizens override formalities.

National leadership attempts to coalesce its own departments and prioritize tasks between disparate Continuity of Operations facilities. Priorities include synergizing relief from the West and Canada, reestablishing command and control and rule of law, and securing foreign alliances and assistance. Strategy options form around worst-case assumptions, not facts. Fragmented information and difficult questions cloud, complicate and delay decisions.

Relief operations fall short and are late. Lessons applied post-9/11, hurricane Katrina, and superstorm Sandy help, but this attack/crime/disaster is unprecedented in size, complexity and second-order effects. Losing lives to bureaucratic and technological shortcomings proves heinous. Acknowledging that hesitance is the greater crime and that localized authorities are having greater success, the President foregoes numerous statutory laws to decentralize federal support. Urgency overrides caution; innovation trumps organization.

Some years later, a congressional commission will reveal that the US government did not fail to predict or plan, yet was unprepared to execute. The commission will conclude that for the sake of legal and budgetary sacred cows, departments acted toward change as stubborn mules. Despite decades of rhetoric on "whole of government" synergy, past budgetary parochialisms, legal juggernauts and disjointed information and infrastructure had converged to worsen the crisis, not ameliorate it.

This vignette illustrates the potentially horrific consequences of a full scale, irreparable cyber-attack on US critical infrastructure or the more devastating effects of a weaponized electromagnetic pulse (EMP). This worst-case scenario includes war, but a solar storm like the Carrington Event of 1859 or other devastating natural event could produce similar effects.[1] The risk of such events today is viable.[2] Over the next 20 years, adversary threats will vastly expand.

The number and types of capable actors and technologies, and the speed with which these attacks may occur are daunting.[3] Furthermore, the portfolio of threat options grows broader. In 20 years, the US will no longer be a unipolar power. As during the Cold War, the US will again compete for parity, not primacy. Only then, competition will happen in all power domains against increasingly more capable and diverse groups of state and non-state actors.[4]

The vignette's purpose is to demonstrate preventable consequences driven by contemporary bureaucratic stumbling blocks to information synergy that clash with this very competitive future. Failure to address these stumbling blocks may prove ruinous to government response. To preempt catastrophic threats or mitigate disasters, the US government (USG) must enable machine-speed information sharing. Today, manpower intensive work-arounds are notionally effective, but reactive and limited by their need to meet congressional statutory requirements found within a US Code (USC) that contains 51 individual titles and over 200,000 pages.[5] Synergy must come more naturally. In the same way that unforeseen change drove constitutional amendments throughout American history, unforeseen change to execution requirements following 9/11 compel the need for national leaders to debate and reform the USC. A more discernible USC must emerge from this debate. It must provide clarity to traditional matters of interpretive controversy and proper mandates that drive whole of government information fusion. Work-arounds will not suffice in tomorrow's world. The USC requires synchronized and coherent reform to avert otherwise self-imposed strategic disadvantages in the realm of collecting, processing, evaluating, and disseminating time sensitive information.

The vignette exposes several ambiguous, but knowable questions. Is this event war, crime, or calamity; a global battleground or a domestic disaster area? What if the event is some or all of these? What determines sovereignty? What separates defense from law enforcement?

When the environment and jurisdiction are uncertain, which agency has the lead: federal, state or municipal? What are the support relationships between various response agencies? How is law and order to be preserved in such circumstances? If information processes do not support collective knowledge, the answers to these questions remain elusive. To avert tragedy and curtail suffering, those answers must be intuitive under duress. Knowing requires common information and shared understanding that then leads to focused, synchronized effort across federal, state and local channels.

Uncertain Futures with Certain Realities

While the fluidity of rapid technological advances, impending global economic shifts, and rising non-state activism complicate the task of accurately predicting the world political environment in 2033, there are three safe bets one can sketch by projecting powerful contemporary trends. The first is that while US dependence on space and cyber will likely increase, both will emerge as adversary domains of choice in future conflict. The second is that low-cost technological proliferation will increase adversary capabilities, erode US primacy and compound direct threats to the US homeland in all domains. Finally, reliance on US military security and logistics capabilities during natural and man-made disasters at home and abroad will likely increase as alternative resources diminish.[6] Each of these realities imposes essential, but currently unmet holistic, machine-speed information fusion requirements.[7]

Space and Cyber: Dependence, Competition and Vulnerability

Rapid technological evolution has rendered US defense, navigation and commerce information flows dependent on vulnerable satellite constellations and cyber infrastructure.

According to General William Shelton, the head of Air Force Space Command, "Our military's reliance on cyberspace is hard to fully comprehend because our reliance on networked capabilities is so ubiquitous it's taken for granted." [8] Modern designs incorporate space and cyber domain access as afterthoughts. During recent Senate testimony Army Lt. Gen. Richard Formica, who heads Army Space and Missile Defense Command, explained that "space-based capabilities…are critical to land operations. If the Army wants to shoot, move or communicate, it needs space."[9]

Foreign space and cyber balancing, attribution difficulty, and the increased relevance of non-state, proxy and individual "netizen"[10] actors in space and cyberspace raise the stakes.[11] America's antagonists have identified US primacy as a continued threat. Through foreign balancing, technologically superior, competing systems will provide adversaries with strategic advantages. Those advances may compel the US and others to counter balance. [12] As ideological and economic competition rises, virtual conflict will transcend the military power spectrum as diplomatic, informational and economic acts of crime and/or war driven by increased competition for hearts, minds and resources. Cyber incursions now happen in each millisecond. These "weapons of mass disruption," as President Obama has called them, threaten security along with commerce, privacy and identity.[13] Technological speed and innovation outpace human reaction. Future conflicts will lack predictability and precedent. Rapid, actionable information is the coin of the realm. Without USC reform to enable such information, the stakes include critical defense capabilities, national infrastructure, global economics and personal freedoms.

Shrinking Boundaries, More Actors

Rapid, low-cost technology proliferation by state and non-state actors may grind US technological and geographic advantage to near zero.[14] Before 9/11, US homeland defense and security operations principally included nuclear deterrence, alert fighter scrambles against Russian bomber probes, and counterdrug operations. Separation by sea empowered a surprisingly limited defense posture. The 9/11 attacks dispelled this notion of security. Radical, reactionary federal reform followed. [15]

Equalizing initiatives already evident in space and cyber that diminish US advantage represent just the tip of the iceberg, not the greater mass below the surface.[16] Advanced capabilities will likely be available to proxies, corporations, interest groups and individuals. In the information realm, these new threats will force the USG toward new technological baselines for rapid information sharing to possibly include human augmentation.[17] Information conflicts will be difficult to distinguish as acts of crime or war. Cyber events may not reveal nationality. Origins are frequently untraceable, which raises tough questions about whether conflict occurs under "home" or "away" rules.[18] Additional USC reform to reshape USG policy and structure against emergent technologies and elusive threats is unavoidable.

Citizen ← → Soldier

As resources dwindle, recapitalizing military capabilities such as lift, logistics, engineering, medical care, communications and surveillance for domestic uses is a good government business model.[19] Just as 9/11 reset US defense posture, Hurricane Katrina made the Department of Defense's (DOD) role during natural and man-made disasters more deliberate. Military capabilities providing essentials like food, water, fuel and security following natural or

man-made disasters has become standard within US Northern Command (USNORTHCOM) plans. Under congressional direction, USNORTHCOM and the National Guard have also added specialized domestic military missions like the Chemical, Biological, Radiological and Nuclear (CBRN) Response Enterprise to the portfolio of fighting units.[20]

Military intelligence provides increasing support to domestic security and law enforcement. Likewise, the intelligence community has worked in support of DOD and law enforcement agencies to bring terrorists to justice since 9/11. Just as the terrorism threat is not likely to diminish, more innovative means of rapidly sharing information appear unavoidable.

Sacred Cows, Opposing Imperatives: Root Causes of Stove-Piped Planning

Each USG department must follow the law while pursuing its mission. Some of these rules present specific barriers to information sharing for thoughtful reasons. For example, Title 18 restricts DOD from receiving certain types of law enforcement information without congressional authorization due to prohibitions on using the federal military as *posse comitatus*.[21] However, when combatting terrorism the interpretive lines between war and crime become very fine and have led Congress to make exceptions.[22] Further, National Guardsmen under state command and Title 32 authority are not subject to *posse comitatus*.[23]

USC legal language is often vague. Discerning USC intent is complicated by both a lack and a litany of legal precedents. Although there are instances where vague laws may be deliberate by Congress to engender interpretive flexibility or to reach a compromise between ideological differences, when literal legal interpretations of vague laws are institutionalized within organizational cultures, they can become pervasive. Departments sometimes refuse to share information with other departments, particularly those with dissimilar missions or legal authorities, due to organizational cultures.[24] This close-hold phenomenon occurs despite the

President and Congress repeatedly asking departments to develop information synergy through policy guidance and most USC titles.[25] USG departments also lack a *de facto* budget mandate to collaborate on interoperability despite these broader mandates for synergy. Without budget mandates, departments naturally program for stove-piped systems that best meet departmental mission ends rather than collective whole of government purposes.

The USC lacks editorial coherence for the lay reader. It presents a collage of additive and subtractive laws that are subject to change with the vacillating preferences of each Congress or administration. Extracting clear, authoritative policy from within its retractions and chronological footnotes proves overly difficult. When guidance is fragmented or offers more questions and referrals to other guidance than context, follow-on departmental guidance may reach users as ambiguous or arrive as an edict directed by departmental lawyers seeking departmental ends rather than macro-interagency goals.

These policy, organizational and budget driven limits on sharing will prove vexing in tomorrow's time-critical information environment. As adversaries operate anonymously within and outside US sovereign territory, they will complicate legal discriminators between what is domestic versus foreign and who is in charge. Meanwhile, opponents to removing these straightjackets are concerned about potential overreach that may erode the very privacy and civil liberties the USG intends to secure. The stalled debate over pending legislation known as the Cybersecurity Act of 2012 is just one of many inevitable debates to come.[26] Policy on *posse comitatus,* for example, will inevitably face debate to reconcile the proper balance between utilitarian security and personal privacy. The 2007 National Defense Authorization Act (NDAA) expanded President Bush's authority to declare martial law through revisions to the Insurrection Act. It also increased the President's power to command the National Guard. Following the

collective protest of the nation's governors, these powers were reversed by Congress in 2008.[27] After signing the 2012 NDAA, President Obama immediately issued a Presidential Policy Directive to waive certain provisions on military detention of suspected terrorists. In other words, the President approved, but then vowed not to use powers he stated would "undermine the national security interests of the United States."[28]

This executive and legislative pendulum effect goes beyond the normal separation of powers struggle of a three-branch democracy. It highlights an exigent post-9/11 legal dilemma between two national imperatives: security and liberty. As adversary actions become more difficult to label as domestic or foreign, criminal or combatant, this debate on opposing imperatives will become more worrisome. Formerly fringe cases like those of "American Taliban" John Walker Lindh and American al-Qaeda operative Anwar al-Aulaqi are becoming part of the new normal of US legal and security affairs.

Work-Arounds: Treating the Symptoms, Not the Problem

Despite clear, progressive calls from Congress and the President for information synergy within the USG, the solutions formed often manifest as stove-piped concepts, *ad hoc* or formal agreements, or even laws to work past other laws. Homeland work-arounds addressing active duty and National Guard domestic interplay, which mainly wrestle over sovereignty issues and *posse comitatus* risk avoidance, include the post-Katrina concept of Contingency Dual-Status Commanders (CDSC) and the long-standing practice of NORAD air sovereignty "hip pocket" Title 10 orders.[29] While the scope of these examples goes well past information sharing, rapid and continuous information synergy is a foundational requirement in all such endeavors. Some

interagency work-arounds have evolved into elaborate coordination centers that both share and protect departmental data.[30]

One should not understate the success of such work-arounds, as these efforts are well intended and save lives. Despite the good they do, these "handshake" agreements are founded on principles of preserving forced limits as much as the need to share. While humans occupy themselves deliberating over what they can and cannot share, machine-speed actions by adversaries not beholden to US law may have already rendered their conclusions irrelevant.

Beyond the matter of speed lies the additive issue of lost intent. Work-arounds act like water. They seek a path of least resistance. In so doing, they create new channels and fissures by creating operational dependencies that gradually erode the legal intent and viability of the restrictions they seek to circumnavigate. Interagency dysfunction reflected in the vignette illustrates the negative effects of a reactionary response. In the future, USG departments will inevitably face unforeseen variables that fall beyond the established boundaries of a well-intended work-around.

Other work-arounds include just-in-time legal blessings. An example is the single hybrid chain of command used by DOD and the Central Intelligence Agency during the raid that killed Osama bin Laden. While heralded and operationally successful, joining Title 10 warfare with Title 50 covert statecraft places military members at significant risk if captured.[31] Such mergers also violate the very rule-of-law principles the US seeks international partners to observe. Freelancing undermines US soft power. Yet in defense of the raid, the tactics and speed employed to execute decisions were in line with meeting today's and tomorrow's threats.

When tracing the problem back to its root cause, one finds the USC. Its ambiguity creates interpretive vacillation between tradition and necessity during crises. This circumstance

both demands restraint and forces innovation. Work-arounds thus enable legal loopholes for whatever ends are sought. That approach may not negatively affect the President who can more readily manipulate laws on the fly, but for the end user without that authority, these contradictions impose strategic and personal risks.

Operating from *ad hoc* plans perpetuates ambiguity that leads to hesitancy. Despite detailed planning and high visibility, National Special Security Events (NSSE) highlight a continuing practice of event-driven, rather than established interagency planning and coordination. Figure 1 lists 29 separate participating entities that shared protection duties during the 2013 Presidential Inauguration NSSE. While the US Secret Service oversaw planning and execution as lead federal agency, the weight of effort of many of the supporting participants occurred from disparate "headquarters" just as they did in 2009, each with their own unique jurisdictional responsibilities. A December 2012 Congressional Research Service report cited weaknesses in 2009 inauguration security despite unprecedented support numbers. The report added that statutory legislation could increase coordination among law enforcement and first responders and eliminate *ad hoc* security funding mechanisms for NSSEs, particularly those with fixed timing. [32]

When everyone is in charge of only their own rice bowl, no one may be in charge of preparing the meal. Despite close coordination with the US Secret Service during NSSEs, the lack of composite command and control leaves a vast potential for fog and friction should things suddenly go awry. Under the current USG model the term "interagency" is a misnomer because participant groups form in reaction to the needs of the situation and their composition and interests may vary widely from issue to issue.

2013 Presidential Inauguration—Participating Agencies

- U. S. Secret Service (Lead Federal Agency)
- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Commonwealth of Pennsylvania
- Commonwealth of Virginia (VEDEM)
- Commonwealth of West Virginia
- DC Fire Department and EMS
- DC Health and Human Services
- DC Homeland Security & Emergency Management Agency
- DC Metropolitan Police Department
- DHS OPs/Principal Federal Official Program
- Federal Aviation Administration
- Federal Bureau of Investigation
- Federal Emergency Management Agency
- Federal Protective Service
- Immigration and Customs Enforcement
- Joint Forces Headquarters/NCR
- NORAD/USNORTHCOM
- Regional Emergency Management, Fire, Police, EMS and Health Departments
- State of Maryland (MEMA)
- Transportation Security Administration
- U.S. Capitol Police
- U.S. Coast Guard
- U.S. Customs and Border Protection
- U.S. Department of Health and Human Services HHS/NCR
- U.S. Department Of Transportation
- U.S. Park Police
- Washington Metropolitan Area Transit Authority
- Federal and National Guard military support (6000 troops from 26 states and territories)
- State and Local Police support (60 departments deputized as US Marshalls)

Figure 1. Participating Agencies During the 2013 Presidential Inauguration (consolidated from multiple sources)

Opposing imperatives on information dissemination and protection in the USC can force departments to choose between conflicting yet intersecting requirements. As structured, the USC frequently asks departments to use limited means to modernize information-sharing ends, but without providing the legal and budgetary mandates required to enact follow-through. This is the equivalent of a building code that asks, but does not require, the Amish to spend money to wire their homes for electricity. Given such an out, of course they will not. Nor will a department prioritize its limited funds to rapid interagency information fusion ahead of departmental goals without a forcing mechanism.

A shortage of federal synergy also fosters non-government work-arounds. The National Emergency Management Agency's (NEMA) highly successful Emergency Management

Assistance Compact (EMAC) provides a relevant example of proactive, non-governmental innovation borne out of necessity and common logic. In an overall effort to assure mutual assistance during emergencies, EMAC also works to assure the interoperability of local infrastructures such as volunteer fire companies, county engineers, and law enforcement. EMAC has evolved bottom-up into law borne out of agreement between state and territorial leaders for mutual aid during catastrophes.[33] It stands to reason that our central government ought to be urgently seeking similar degrees of departmental cooperation. Achieving synergy beyond work-arounds requires a legal mandate.

Sacred cows like *posse comitatus* have compelled niche work-around agreements or legal exceptions crafted to slalom through rather than confront the ethical conflict between tradition and foreseeable futures embedded in the USC. The bin Laden example provides a case in point. Aberrations to meet emergent needs are becoming far too normal. The law requires reform that not only promotes unity of effort, but incentivizes or insists upon it.

System Requirements:

While the need for better policy is obvious, there are practical information sharing requirements that enable uninhibited interagency cooperation. First, the elimination of departmental stovepipes to establish true interagency information sharing networks is essential. These networks must be accessible to users across intra-agency security domains. While an unrestricted "opening of the floodgates" may not be the answer, neither is withholding time-sensitive data that matters to decision makers. Legal, ethical and practical factors must remain very important parts of doing business, but implementation must also succumb to inevitable requirements for speed, discernibility and use. A pragmatic culture of need-to-share must finally

supersede the dogmatic culture of need-to-know.[34] Second, adversary information attack, masking and deception may occur rapidly. This creates a shell game where following the enemy pea is impossible without responding in kind. Without machine-speed counterattack, counter spoofing and information-protection protocols, reaction will be late and limited.

Third, these interagency networks must evolve well past sharing raw information. Captured adversary information will have a brief half-life. Information must be sorted and analyzed within a shared understanding of threat and event contexts. That analysis, and its analysts, must take on whole of government business practices. These practices must inspire meaningful and deliberate crosstalk to rapidly tease out relevant information from terabytes of data. Fourth, information systems and processes must be robust. While interconnected for synergy, they must also have stand-alone capabilities. If severed or attacked, the network must be resilient, survivable, redundant and able to reconstitute. When network failure occurs, information must degrade gracefully. While the command and control must be more distributed, so should the information databases.

Policy Enablers

A revised USC must give full respect to the inevitable realities of future diplomatic, economic, military and informational conflict in space and cyberspace along with increased risks to the homeland. Such recognition is easier said than done. It requires a complete and coherent debate that leads to clearer laws on how to facilitate security while preserving privacy and civil rights. Post 9/11 efforts to balance security and liberty have been robust, yet the threat posed by future rivals will drive this challenge further.[35]

Debating yesteryear's policies against tomorrow's threats should happen today. Doing so will legally enable the USG to implement interoperable technical means within robust, interconnected information systems to collect, process, evaluate and disseminate actionable information throughout the whole of government at machine speed. That debate will be passionate and lead to a menu of compromises. But the US cannot wish away adversary national, non-state, and individual threats. Nor can it avoid natural disasters be they disruptions caused by solar flares, hurricanes, tornadoes or massive forest fires. While policy may not reach a perfect place, policy must reach a common place from which practitioners at federal, state, local and private levels can mutually understand one another, plan, and cooperate. Unison is still progress.

A second policy enabler for national defense and security is legal recognition that distinctions between home and away "games" are rapidly diminishing. Globalization and digitization are turning hard borders into soft borders. The US military will need clear license and collectively understood rules to operate within defined guideline edges, rather than in margins. For instance, if the US conducts distributed operations in a domestic Air Operations Center for an overseas air war, is it willing to accept an enemy interpretation of expansion of the battlespace and the associated risks of domestic attack? The US already flies UAVs this way today. Geographically, the state of Nevada (Nellis AFB) is at war in Afghanistan. What are the legal implications for the military and the security risks for the surrounding community unaware that it is "at war?" What civil legal liabilities does the USG face? While the US strives to reach an international code of conduct and rule of law to govern behavior, not all adversaries will follow these rules, particularly if the US is not also following clear legal guidelines. US laws must unequivocally support domestic, foreign and geographically nebulous activities.

The USG must also modify statutes to create interdepartmental information technology budgets. Budgetary fusion is required to minimize gaps, reduce duplications, and connect state and local infrastructure with federal infrastructure. Information must be actionable both top-down and bottom-up. Such building-block efforts are encouraged in the USC and, to a far lesser degree, are underway. But without budget policy that forces a foundation, full cooperation is much less likely. Starting in 2013, all intelligence budgets are under the centralized control of the Director of National Intelligence (DNI). This move by Congress indicates its resolve to maximize intelligence community performance while also preempting waste and risk to ultimately save blood and treasure. This is a major step. Whether it acts as a catalyst for other whole of government budget reforms within the USC remains to be seen. Additional efforts to streamline USG information technologies are needed.

Finally, to gain lay-reader coherence, the USC requires common-sense editing. Today's USC is often counterintuitive and confusing. It must be simplified and clearly communicated beyond the legal office to the users. User clarity will permit true operationally-based debates and enable forward-thinking plans that do not otherwise die at the water cooler. Clarity will allow the US to preposition its laws and capabilities to avert or minimize catastrophe. Questions from the vignette are knowable. So too are the inconsistencies in the USC. The USG must fix the latter to avoid the former.

Concluding Recommendations

Three sequential actions are recommended to reshape and clarify the USC. First, the USC requires basic structural editing for clarity within and across its titles. As written, the USC presents as a collage of laws formatted to reflect history rather than serving as an authoritative reference useful to departmental dialogue. That history is important, but belongs in separate

references or appendices. The USC must be discernible and actionable by lay readers charged with policy implementation throughout every organizational level. The USC must communicate the law clearly to readers in far less than 200,000 pages. Departments within the USG have done an admirable job recently of standardizing processes and sharing best practices. The DOD Quadrennial Defense Review (QDR), for example, has been copied by the Department of Homeland Security (DHS) and the Department of State (DOS) in crafting their respective Quadrennial Homeland Security Review (QHSR) and Quadrennial Diplomacy and Development Review (QDDR). Such efforts indicate desires for uniformity and synergy. A congressionally supported overhaul of the USC to take each title's format beyond that of a legal catch basin can provide immediate incentives for unity of purpose.

Step two is a macro-debate to determine whether there might be areas where policy is at cross purposes with itself as it promotes information synergy, but incentivizes departmental solutions. A key consideration in such debate is that policy must keep pace with technology in ways that sustain US advantage over its rivals. The USC must reconcile whether legal restrictions and enablers to rapid information fusion collectively meet constitutional and security imperatives, and whether those imperatives can survive first contact with a new and broader set of adversaries. Such an overarching policy review goes well past editing today's content. Answers may evolve over time. Nevertheless, whole of government response demands proactive legal licenses embedded within technologies that enable fluidity, speed and collaboration. The USC must take more literal steps toward a balance between protecting freedoms and being liberal enough to combat a nontraditional foe operating without a legal conscience. Given the scope and controversy of such a debate, this second recommendation represents the "long pole in the tent" towards resolution.

Finally, the USC requires an overarching mandate that provides mass to the concept of an interagency process. Prior to the Goldwater-Nichols Act in 1986, "joint" was only a mostly toothless concept within DOD. Goldwater-Nichols merged the services in a tangible manner that both promoted and mandated unity of effort and unity of command. It forced shared procurement and interoperability goals upon otherwise self-interested military services. As written, the separate titles of the USC position departmental interests in a manner akin to states in a confederacy. This "confederate" approach to departmental governance and budgeting overrides federal unity of purpose, practically ensuring departmental parochialism. The US abandoned the Articles of Confederation in favor of the Constitution and a federal government. To set the tone for a true interagency, it should do the same for its federal statutory structure. Many have argued the need for a Goldwater-Nichols like interagency reform to promote whole of government approaches to matters of national security.[36] Others have argued for an interagency homeland response doctrine.[37] This paper agrees with the former.

While various departments have made great progress toward developing interagency coordination plans, such as DOD's Joint Publication 3-08 "Interorganizational Coordination During Joint Operations," these efforts remain internal solutions to external issues. Top-down executive and congressional direction, as well as bottom-up initiatives like EMAC, have also led to some improvements in information sharing since 9/11. The National Network of Fusion Centers, the National Information Exchange Model, and fusion efforts through the National Counterterrorism Center have yielded new levels of partnering. However, significant gaps remain as the threat increases. Legislation to mandate unity of effort could represent the *coup de grâce* to the inefficiencies of stove-piped departmental budgets and compartmentalized information security. Beyond legislation to unify effort, USC structure must evolve from a

collection of departmentally-based, semi-autonomous titles to a more holistic body of interdependent statues with procedural and budgetary norms that incentivize collaboration.

Enactment of comprehensive USC reform can provide the foundational mandate required beneath whole of government synergy by giving concrete meaning to the term “interagency.” While each department has worked hard to develop elaborate procedures to ensure security and protect liberty, combined approaches to collecting, processing, evaluating and disseminating information at machine speed are critical to preempting catastrophic threats or mitigating disasters in the near future. The opening vignette raised several knowable, sharable, yet unanswered questions. The consequences of not knowing illustrated in the vignette are preventable. To study and debate is to better understand. To understand is to know and prevent through unity of purpose. Reforming the USC to facilitate time-sensitive information sharing is critical to our survival as a nation.

Notes

1. The 1859 Carrington Event is the largest recorded solar flare incident. The event impacted telegraph systems by shocking operators and causing telegraph paper to catch fire. Upon disconnecting power, many telegraph systems remained operable. Lesser solar flares have knocked out power grids, caused transformers to blow, and temporarily impacted the global positioning system. Given today's increased reliance on sensitive electronics, a Carrington-sized event could have effects similar to an EMP, wiping out satellites, frying electronic components and shutting down power around the world. Predicting such incidents is imperfect given their brief tracking history, but estimates place the average likelihood of a Carrington-sized event as once every 500 years. See Trudy E. Bell and Dr. Tony Phillips, "A Super Solar Flare," *NASA Science*, 6 May 2008, http://science.nasa.gov/science-news/science-at-nasa/2008/06may_ carringtonflare/ (accessed 26 January 2013).

2. According to a cyberspace policy review directed by President Obama, the Central Intelligence Agency confirmed cyber-attacks disrupted electric power in multiple regions overseas, including one case of a multi-city outage. See The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," 2, http://www.whitehouse.gov/assets/ documents/Cyberspace_Policy_Review_ final.pdf.

3. A recent National Intelligence Council study lists cyber and EMP as exigent future threats, adding that the most predictable future megatrend is empowerment. "Individuals and small groups will have greater access to lethal and disruptive technologies (particularly precision-strike capabilities, cyber instruments, and bioterror weaponry), enabling them to perpetrate large-scale violence—a capability formerly the monopoly of states." See National Intelligence Council, *Global Trends 2030: Alternative Worlds*, NIC 2012-001 (Washington, DC: National Intelligence Council, December 2012), 9.

4. The 2011 National Military Strategy forecasts significant state and non-state threats to US access in the global commons. See US Department of Defense, *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership,* (Washington DC: Chairman of the Joint Chiefs of Staff, February 2011), 3-4.

5. The collective US Code is the library equivalent of an encyclopedia of US laws. Each "volume" is a statutory title (there are currently 51) that is generally applicable to a department or some particular aspect of the USG. For example, Title Six "Domestic Security" provides legal guidance or cross references to other titles pertaining overwhelmingly to DHS, making Title Six the "go-to" reference document for DHS statutory law. Title 10, which is 2489 pages long, pertains to the "Armed Forces." Title 32 pertains to the "National Guard." Title 50 provides overarching guidance on "War and National Defense." While revised every six years along with supplements published each year intended to provide clarity, lay reader interpretation is not a USC strong suit. Among the difficulties is the reality that one issue may be included across several titles.

6. Recent presidential guidance lists support to civil authorities and conducting humanitarian, disaster relief and other operations among the primary missions of the armed forces. See Department of Defense, *Sustaining US Global Leadership: Priorities for 21st Century Defense* (Washington DC: Office of the Secretary of Defense, January 2012), 5-6.

7. Harvey Rishikof and Roger George conclude that the 2001 Hart-Rudman Commission report, the 2009 Project on National Security Reform and others have recognized that "the new century would require agencies to adjust their portfolios and achieve a level of interagency

cooperation and partnering with non-government organizations as well as allies to a degree [of whole of government synergy] not anticipated." These complex needs remain unmet. See Harvey Rishikof and Roger George, "Conclusion: Navigating the Labyrinth of the National Security Enterprise," in *The National Security Enterprise*, ed. Roger Z. George et al. (Washington, DC: Georgetown University Press, 2011), 331-334.

8. General William L. Shelton (address, Armed Forces Communications and Electronics Association Cyberspace 2012 Symposium, Peterson Air Force Base, CO, 15 February 2012).

9. Walter Pincus, "Hearings Show Our Dependence on Military Space Technology," *The Washington Post*, 26 March 2012, http://articles.washingtonpost.com/2012-03-26/world /35448260_1_military-space-space-command-aehf (accessed 11 December 2012).

10. "Netizen" is a colloquialism that refers to an erosion of national identity among Internet-educated persons that identify more closely with globally-oriented groups or causes.

11. A bi-partisan commission recently labeled China the top cyberspace exploitation actor, citing military vulnerabilities along with non-military threats to international free speech, US supply chain integrity and industrial espionage in its annual report to Congress. See Eliza Krigman, "Report Labels China 'Most Threatening' Cyber Actor," *The Politico*, 14 November 2012, https//www.politicopro.com/go/?id=16060 (accessed 15 November 2012).

12. India recently announced successful development of the Agni-V intercontinental ballistic missile to provide "India's answer to China's anti-satellite weapon" and thus joins the growing number of nations pursuing anti-satellite (ASAT) capabilities. India plans to field a full capability by 2014, according to India's *Defence News*. See "India's Reply to China's Anti-Satellite Weapon," *Defence News*, 11 May 2012, http://www.defencenews.in/defence-news-internal.asp?get=new&id=1215 (accessed 29 November 2012).

13. During a press conference on the release of the administration's Cyberspace Policy Review, President Obama noted that cybercrime totaled over $8 billion in the last two years while intellectual property theft estimates topped $1 trillion worldwide. Due to our dependencies and vulnerabilities both as a nation and as private citizens, the President classified cyber as a "strategic national asset…where no single agency has the skill to match the scope of the challenge," adding that "ad hoc responses will not do." See Barack Obama, *Cybersecurity* (The White House, 29 May 2009), 16 min., 30 sec., MP4 Video File, http://www.whitehouse.gov/ administration /eop/nsc/cybersecurity (accessed 26 January 2013).

14. Computer power nearly doubles annually due to Moore's Law. Michio Kaku illustrates that the magnitude of this effect is easy to underestimate. "For example, when you receive a birthday card in the mail, it often has a chip that sings 'Happy Birthday' to you. Remarkably, that chip has more computer power than all of the Allied forces of 1945." That same power also cost millions (in 1945 dollars) to produce. Kaku explains that over time computer chips will proliferate to permeate most everything as throw away items at costs cheaper than paper. When such low costs are coupled with technology theft, high-tech proliferation well beyond the contemporary example of the copycat Chinese J-20 fighter becomes probable. See Michio Kaku, *Physics of the Future*,(New York, NY: Anchor Books, 2011), 23-25.

15. DHS establishment in 2003 consolidated 22 agencies into one. As the largest reorganization of the federal government since the National Security Act of 1947 created DOD, this merger caused sweeping revisions, additions and retractions within the USC that are still evident ten years later.

16. According to a 2012 annual report to Congress, Chinese technological research focus between now and 2020 includes: advanced aerospace, aeronautics, lasers and materials along with cognitive science, structure and condensing of matter, biotechnology, nanotechnology, quantum research, high-end chip design and software, extra large-scale integrated circuit manufacturing, genetically modified organisms, high-definition earth observation systems, water and gas-cooled nuclear reactors, manned space and lunar exploration, and speculatively, a second-generation Beidou satellite navigation system and a hypersonic vehicle technology project. See U.S.-China Economic and Security Review Commission, *2012 Report to Congress of the U.S.-China Economic and Security Review Commission,* (Washington DC: General Accounting Office, 2012), 397-398.

17. According to the National Intelligence Council, "brain-machine interfaces could provide 'superhuman' abilities, enhancing strength and speed, as well as providing functions not previously available." See National Intelligence Council, *Global Trends 2030: Alternative Worlds*, 100.

18. Rishikof and George provide a compelling case regarding the difficulty in distinguishing between domestic and international events caused by transnational threats. This confusion will raise unavoidable conflict between needed surveillance and individual privacy rights. See Rishikof, "Conclusion: Navigating the Labyrinth of the National Security Enterprise," 344.

19. Today, most National Guard domestic military activities occur in a supporting role to another designated lead federal agency such as the Department of Homeland Security through Federal Emergency Management Agency (FEMA) regional response plans or the US Secret Service during a National Special Security Event.

20. National Guard Title 32 forces of the domestic CBRN Response Enterprise number approximately 10,000 parsed between individual states and consist of 10 Homeland Response Forces (one per FEMA region), 17 CBRN Enhanced Response Force Packages, and 57 Weapons of Mass Destruction-Civil Support Teams. These Title 32 teams are formed using existing state-based units that receive extra training days to train to both the CBRN mission and their traditional warfighting missions. Title 10 CBRN forces (a mixture of active duty and National Guard) number an additional 9000 and include a Defense CBRN Response Force (DCRF) and two CBRN Response Elements (CRE). The US Marines also maintain two Chemical, Biological Incident Response Forces (CBIRF) for domestic and global WMD response (most notably, Operation Tomodachi in Japan). For more information on the broader scope of homeland military support, see US Department of Defense, *Strategy for Homeland Defense and Civil Support* (Washington DC: Office of the Secretary of Defense, June 2005).

21. *Posse comitatus* refers to federal law that limits the federal government in using Title 10 military personnel to enforce state laws without an act of Congress or Constitutional authority (found only in the Insurrection Act). The applicable Title 18 language reads: "Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both." *Posse comitatus* restrictions are reaffirmed in Title 10, which reads: "The Secretary of Defense shall prescribe such regulations as may be necessary to ensure that any activity (including the provision of any equipment or facility or the assignment or detail of any personnel) under this chapter does not include or permit direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in

such activity by such member is otherwise authorized by law." See Title 18-Crimes and Criminal Procedure, 18 U.S.C. §1385 (2011) and Title 10-Armed Forces, 10 USC § 375 (2011).

22. See Richard A. Best Jr., *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, Congressional Research Service (Washington, DC: Library of Congress, 3 December 2001), 35.

23. National Guard Regulation 500-5 provides a very comprehensive historical and practical explanation of *posse comitatus* and serves as an excellent guidebook for the proper authorities and use of military personnel in law enforcement under current law. See National Guard Regulation 500-5/Air National Guard Instruction 10-208, *National Guard Domestic Law Enforcement Support and Mission Assurance Operations*, 18 August 2010.

24. For example, USC Title divisions tend toward separating or placing legal distance between foreign and domestic operations (DOD authorities versus DHS, CIA versus FBI). The Information Sharing Environment, an interagency policy committee charged with facilitating information sharing, discusses the prevalence and impact of these organizational factors within a recent white paper. See Information Sharing Environment, "A Legal and Policy Approach for Responsible Information Sharing: The Role Of The Information Sharing Environment (ISE)," 3-4, http://www.ise.gov/sites/default/files/Legal_and_ Policy_Approach_White_Paper.pdf.

25. The President's *National Strategy for Information Sharing and Safeguarding* provides the most recent and perhaps most explicit reiterations of a consistently articulated message over the past decade on the need for information sharing (within legal limits) across agencies and departments. Congress has included similar language (albeit non-binding) within several USC Titles. See The White House, *The President's National Strategy for Information Sharing and Safeguarding* (Washington DC: Office of the President, December 2012), 1-2.

26. Defense Secretary Leon Panetta likened the destructive effects of cyber threat actors to a "cyber Pearl Harbor" that could "paralyze the nation." He added that DOD will introduce new rules of engagement that extend DOD responsibility beyond protecting DOD networks to protecting national networks. He urged Congress to pass legislation to eliminate legal barriers and baseline sharing standards between the government and the private sector via Senate bill *S. 2105 (112th): Cybersecurity Act of 2012* introduced by Senator Joseph Lieberman. This legislation failed in August 2012 over concerns that it may erode freedoms through overreach, but will likely be reintroduced. Failing passage, President Obama is said to be considering an Executive Order. See Jim Garamone, "Panetta Spells Out DOD Roles in Cyberdefense," *American Forces Press Service*, 11 October 2012, 1-2.

27. National Governors Association, *America Wins: The Struggle for Control of the National Guard* (Washington DC: National Governors Association, 2012), 3-4, http://www.nga.org/files/live/sites/NGA/files/pdf/1210NationalGuardAmericaWins.pdf.

28. The White House, *Presidential Policy Directive -- Requirements of the National Defense Authorization Act*, http://www.whitehouse.gov/the-press-office/2012/02/28/presidential-policy-directive-requirements-national-defense-authorizatio (accessed 27 January 2013).

29. As a prearranged agreement between the President and an affected governor, the CDSC concept allows a single officer to command both Title 10 active duty and Title 32 National Guard forces for unity of command during designated domestic contingencies within a sovereign state. *Posse comitatus* restrictions still apply to Title 10. CDSC was legalized through the 2012 NDAA to allow domestic forces to act collectively without otherwise changing the USC. Hip pocket Title 10 orders allow a Title 32 National Guardsman to temporarily transition to Title 10

status in order to execute federal Homeland Defense roles, such as an Air Sovereignty Alert fighter intercepts. These military orders allow National Guardsmen to monitor federal missions in non-federal status, and then briefly act as federal forces upon activation of some predetermined trigger. Following the event, the Guardsmen revert back to Title 32.

30. For instance, the National Capital Region Coordination Center (NCRCC) is an operations center that employs watch officers from each department or agency to continuously monitor the air domain and share information on federal and local actions for air defense and security around the nation's capital. Each watch officer represents the lone interests of their agency or department and operates independently without unity of command, but by charter shares situational awareness information within distinct access limits to facilitate unity of effort. At the NCRCC, one operator may be monitoring or operating a departmentally stove-piped C2 system next to another operator on an equally dissimilar system. As events unfold, these operators achieve collective situational awareness by watching overhead monitors of one another's displays where permissible or by voice or electronic chat when legalities preclude one agency from monitoring the systems of another agency. Each agency commands and controls its own personnel and resources. No one organization leads a collective interagency response.

31. LTC Joseph Berger provides an alarming assessment of significant risk issues when blending Title 10 and Title 50 authorities. Using the "covert" raid into Pakistan, Berger factually anchors his assertion that confusion on statutory legal authorities regarding chain of command and associated risks resides at the very highest levels of government. While Berger argues for sustaining today's statutes, blended operations appear more likely than not in the future when considered against threats. Debate on proper legal structure seems prudent for many operational reasons, but particularly as means to sustain USG legitimacy and credibility internationally. By killing bin Laden in Pakistan, the US military invaded a sovereign state, which is an act of war under international law. See LTC Joseph B. Berger III, "Covert Action: Title 10, Title 50, and the Chain Of Command—Consequences of Policy Decisions," (Coursework, National War College, April 2012), 1-34.

32. Shawn Reese, Jacob R. Straus, and Christina M. Bailey, *Inauguration Security: Operations, Appropriations, and Issues for Congress,* Congressional Research Service (Washington, DC: Library of Congress, 17 December 2012), 8-10.

33. Congress ratified Public Law 104-321 in 1996. All 50 states, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands have enacted legislation to become EMAC members. NEMA is a non-profit professional association, not a part of the federal government. For a very comprehensive guide to EMAC, see National Emergency Management Agency, "Emergency Management Assistance Compact," http://www.emacweb.org/.

34. According to the December, 2012 *National Strategy for Information Sharing and Safeguarding*, "the imperative to secure and protect the American public is a partnership shared at all levels including Federal, state, local, tribal, and territorial. Partnerships and collaboration must occur within and among intelligence, defense, diplomatic, homeland security, law enforcement, and private sector communities." Time will tell whether promised follow-on implementation guidance will contain the specifics needed to realize this document's intent in accordance with the law. See The White House, *National Strategy for Information Sharing and Safeguarding*, 3.

35. The USG has thoroughly and admirably institutionalized privacy and civil rights training and oversight through privacy and civil rights officers within most departments. Overarching

guidance on information sharing tends toward generalized edicts on the imperative of protecting privacy and civil rights. These edicts manifest as authoritative "caveats" within nearly all information sharing related correspondence. The USC is just as forceful in its language on imperatives, but unacceptably short on specifics that may inform clear determinations on how to best balance privacy and civil rights against security. End users are either ill-informed or inadequately empowered to make rational interpretations on what security actions are permissible. Instead, privacy offices make such determinations on behalf of users through lengthy, bureaucratic vetting processes at the department level. The net effect of staunch departmental conditioning and oversight is often "gun shy" personnel that for fear of personal liability or bureaucratic hassle may choose inaction over common sense. Departmental privacy and civil rights oversight details are readily available by web searching "privacy" or "civil rights" on department websites. As an example, see the DHS privacy website at Homeland Security, "Privacy," http://www.dhs.gov/topic/privacy (accessed 30 January 2013).

36. Most recently, the Joint Staff J7 made the following observations as part of its review of lessons learned over the past decade of war: "In the wide range of operations conducted over the previous decade, interagency coordination was uneven due to inconsistent participation in planning, training, and operations; policy gaps; resources; and differences in organizational culture." In response, J7 recommends "mak[ing] interagency coordination mandatory: Pursue development of a Goldwater-Nichols-type act to mandate and develop a framework for increased interagency coordination for a whole of government approach." The J7 also proposed "operationalizing" the interagency through better resourcing, policy, planning, education and training, exchange tours and execution tests. See Joint and Coalition Operational Analysis, Joint Staff J7, *Decade of War, Volume 1: Enduring Lessons from the Past Decade of Operations*, staff study, 15 June 2012, 25-28.

37. LTG (Ret.) H. Steven Blum and LTC (Ret.) Kerry McIntyre argue that unity of effort remains elusive and that national response doctrine is federal rather than national. They suggest a national doctrine modeled after the DOD's Joint Interagency Task Force (JIATF) for application when separate response organizations must work together across jurisdictional lines. This doctrine would include federal, state and local interagency response elements. Blum and McIntyre also argue for the removal of certain legal barriers to the use of military capabilities in the homeland, offering that "it makes little difference to the injured, hungry, and dispossessed that the soldier who rescued them is a National Guardsman, a Title 10 reservist, or an active duty service member." See H. Steven Blum and Kerry McIntyre, *Enabling Unity of Effort in Homeland Response Operations,* (Carlisle, PA: U.S. Army War College Strategic Studies Institute, April 2012), xi, 23-25, 28-30.

Bibliography

Bell, Trudy E. and Dr. Tony Phillips. “A Super Solar Flare.” *NASA Science*, 6 May 2008. http://science.nasa.gov/science-news/science-at-nasa/2008/06may_carringtonflare/ (accessed 26 January 2013).

Berger III, LTC Joseph B. "Covert Action: Title 10, Title 50, and the Chain of Command—Consequences of Policy Decisions.” Coursework, National War College, April 2012.

Best, Richard A. Jr. *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.* Congressional Research Service. Washington, DC: Library of Congress, 3 December 2001.

Blum, H. Steven and Kerry McIntyre. *Enabling Unity of Effort in Homeland Response Operations.* Carlisle, PA: U.S. Army War College Strategic Studies Institute, April 2012.

Garamone, Jim. “Panetta Spells Out DOD Roles in Cyberdefense.” *American Forces Press Service*, 11 October 2012.

Global Trends 2030: Alternative Worlds. NIC 2012-001. Washington, DC: National Intelligence Council, December 2012.

Homeland Security. “Privacy.” http://www.dhs.gov/topic/privacy (accessed 20 January 2013).

Information Sharing Environment. “A Legal and Policy Approach for Responsible Information Sharing: The Role of the Information Sharing Environment (ISE).” http://www.ise.gov /sites/default/files/Legal_and_Policy_Approach_White_Paper.pdf (accessed 30 January 2013).

“India’s Reply to China’s Anti-Satellite Weapon.” *Defence News*, 11 May 2012. http://www.defencenews.in/defence-news-internal.asp?get=new&id=1215 (accessed 29 November 2012).

Joint and Coalition Operational Analysis, Joint Staff J7. *Decade of War, Volume 1: Enduring Lessons from the Past Decade of Operations*. Staff study. 15 June 2012.

Kaku, Michio. *Physics of the Future*. New York, NY: Anchor Books, 2011. 23-25.

Krigman, Eliza. “Report Labels China ‘Most Threatening’ Cyber Actor.” *The Politico*, 14 November 2012. https//www.politicopro.com/go/?id=16060 (accessed 15 November 2012).

National Emergency Management Agency. “Emergency Management Assistance Compact.” http://www.emacweb.org/ (accessed 30 January 2013).

National Governors Association. *America Wins: The Struggle for Control of the National Guard.* Washington DC: National Governors Association, 2012. http://www.nga.org/files/ live/sites /NGA/files/pdf/1210NationalGuardAmericaWins.pdf.

National Guard Regulation 500-5/Air National Guard Instruction 10-208. *National Guard Domestic Law Enforcement Support and Mission Assurance Operations*, 18 August 2010.

Obama, Barack. *Cybersecurity.* The White House, 29 May 2009; 16 min., 30 sec. MP4 Video File. http://www.whitehouse.gov/administration/eop/nsc/cybersecurity (accessed 26 January 2013).

Pincus, Walter. “Hearings Show Our Dependence on Military Space Technology.” *The Washington Post*, 26 March 2012. http://articles.washingtonpost.com/ 2012-03-26/world/35448260_1_military-space-space-command-aehf (accessed 11 December 2012).

Reese, Shawn, Jacob R. Straus, and Christina M. Bailey. *Inauguration Security: Operations,*

Appropriations, and Issues for Congress. Congressional Research Service. Washington, DC: Library of Congress, 17 December 2012.
Rishikof, Harvey and Roger George. "Conclusion: Navigating the Labyrinth of the National Security Enterprise." In *The National Security Enterprise,* edited by Roger Z. George and Harvey Rishikof, 331-350. Washington, DC: Georgetown University Press, 2011.
Schwartz, Peter. *Inevitable Surprises.* New York, NY: Gotham Books. 2003.
Shelton, Gen William L., Address. Armed Forces Communications and Electronics Association Cyberspace 2012 Symposium, Peterson Air Force Base, CO, 15 February 2012.
The White House. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* http://www.whitehouse.gov/assets/documents/ Cyberspace_Policy_Review_ final.pdf (accessed 19 January 2013).
The White House. *Presidential Policy Directive—Requirements of the National Defense Authorization Act.* http://www.whitehouse.gov/the-press-office/2012/02/28/presidential-policy-directive-requirements-national-defense-authorizatio (accessed 27 January 2013).
The White House. *The President's National Strategy for Information Sharing and Safeguarding.* Washington DC: Office of the President, December 2012.
Title 10-Armed Forces. 10 USC § 375. 2011.
Title 18-Crimes and Criminal Procedure. 18 U.S.C. §1385. 2011.
U.S.-China Economic and Security Review Commission. *2012 Report to Congress of the U.S.-China Economic and Security Review Commission.* Washington DC: General Accounting Office, 2012.
US Department of Defense. *Strategy for Homeland Defense and Civil Support*. Washington DC: Office of the Secretary of Defense, June 2005.
US Department of Defense. *Sustaining US Global Leadership: Priorities for 21st Century Defense*. Washington DC: Office of the Secretary of Defense, January 2012.
US Department of Defense. *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership.* Washington DC: Chairman of the Joint Chiefs of Staff, February 2011.