Strategy Research Project

21ST Century Cyber Security: Legal Authorities and Requirements

by

Lieutenant Colonel Charles W. Douglass
United States Air Force

United States Army War College
Class of 2012

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 22-03-2012	**2. REPORT TYPE** Strategy Research Project	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE 21ST CENTURY CYBER SECURITY: LEGAL AUTHORITIES AND REQUIREMENTS	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Lieutenant Colonel Charles W. Douglass	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Commander James R. Greenburg Director, Strategic and Operational Planning Department of Military Strategy, Planning and Operations	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army War College 122 Forbes Avenue Carlisle, PA 17013	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Approved for public release distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Cyber warfare has risen to the level of strategic effect. Exigent threats in cyberspace are a critical U.S. strategic vulnerability for which U.S. Cyber Command is ill-equipped to confront. The law enforcement, intelligence gathering, and strategic defense authorities as specified in United States Code, neither constitute a single, whole-of-government approach to defending our critical information infrastructure nor posture the United States to be the most dominant global power in cyberspace. This SRP examines the current legal architecture that governs the activities of federal agencies in cyberspace and explains how that architecture enables a thinking and agile adversary to attack and exploit the U.S. industrial information enterprise through this complex domain. The federal regulatory authorities that govern law enforcement, intelligence gathering, and military offensive cyber operations cross many sections of United States Code. But, they have not yielded a genuine whole-of-government approach. This SRP argues that cyber warfare has become a mainstream way for sovereign states to enhance national prestige, pursue national interests, and preemptively address threats. It recommends establishment of a single federal entity that focuses solely on national cyber security.

15. SUBJECT TERMS

Cyber Warfare, Joint Interagency Task Force, Exploitation

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	30	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC STRATEGY RESEARCH PROJECT

21ST CENTURY CYBER SECURITY: LEGAL AUTHORITIES AND REQUIREMENTS

by

Lieutenant Colonel Charles W. Douglass
United States Air Force

Commander James R. Greenburg
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR:	Lieutenant Colonel Charles W. Douglass
TITLE:	21ST Century Cyber Security: Legal Authorities and Requirements
FORMAT:	Strategy Research Project
DATE:	22 March 2012 WORD COUNT: 6,181 PAGES: 30
KEY TERMS:	Cyber Warfare, Joint Interagency Task Force, Exploitation
CLASSIFICATION:	Unclassified

Cyber warfare has risen to the level of strategic effect. Exigent threats in cyberspace are a critical U.S. strategic vulnerability for which U.S. Cyber Command is ill-equipped to confront. The law enforcement, intelligence gathering, and strategic defense authorities as specified in United States Code, neither constitute a single, whole-of-government approach to defending our critical information infrastructure nor posture the United States to be the most dominant global power in cyberspace. This SRP examines the current legal architecture that governs the activities of federal agencies in cyberspace and explains how that architecture enables a thinking and agile adversary to attack and exploit the U.S. industrial information enterprise through this complex domain. The federal regulatory authorities that govern law enforcement, intelligence gathering, and military offensive cyber operations cross many sections of United States Code. But, they have not yielded a genuine whole-of-government approach. This SRP argues that cyber warfare has become a mainstream way for sovereign states to enhance national prestige, pursue national interests, and preemptively address threats. It recommends establishment of a single federal entity that focuses solely on national cyber security.

21ST CENTURY CYBER SECURITY: LEGAL AUTHORITIES AND REQUIREMENTS

America is at a strategic crossroads. The emergence of cyberspace as warfighting domain has brought with it new dimensions of national power. Unless fully understood by national security professionals, this new domain may constitute the ultimate “Achilles Heel” in U.S. security. The United States could be subdued by a cyber attack for which we are not currently prepared. The nexus between established Department of Defense (DoD) authorities, warfighting doctrine, and evolving cyber policy requires a greater focus on how to fight and win in cyberspace and less focus on how to apply cyber fundamentals to a two-dimensional war of geography. This SRP challenges the assumptions that underpin current DoD organization and readiness to meet the emerging – and very real – cyber threat. Failure to address cyberspace as a wholly new domain, unencumbered by traditional concepts of geographic boundaries and the legal precedents which govern the application of conventional military force, will ultimately compromise the security of our nation.

In order to grasp the complexity of the artificial restraints placed on federal agencies’ ability to meet cyber threats, one need look no further than United States Code (U.S.C).[1] U.S.C is “the codification by subject matter of the general and permanent laws of the United States based on what is printed in the Statutes at Large.”[2] Of the 50 subject matter titles, only 23 have been entered into statutory law. However, U.S. legal authorities for operating in cyberspace (covering everything from appropriations to intelligence systems to warfare to law enforcement) are mentioned either implicitly or explicitly in 10 of the 23 Codes (not counting Statutes at Large or Supplemental issuances).[3] Further complicating this issue is the dysfunctional series of so-called lead agency responsibilities. For example, the Department of Homeland Security (DHS) is the lead federal agency for cyber policy and management, yet it has no direct authority over DoD's cyber operations.[4] Specifically, no single federal department or agency has been granted directive authority to establish a uniform standard of system accreditation, hardware or software interoperability mandates, or individual user access protocols. The current autonomy of each federal department to handle these critical issues presents a clear threat to the U.S. government's operation in and through cyberspace.

The Cyber Environment

Cyberspace is a man-made domain. In this respect, it is unique among the other four warfighting domains.[5] However, in matters of governmental regulations and national security, cyberspace is very similar to the maritime and air domains in four key ways:

- the preponderance of activity occurring in cyberspace is commercial (or private);
- private industry owns and creates the ways and means to access the domain;
- codification of international conventions originates from the customs and operating procedures of the private and commercial sectors operating in the domain; and
- activity occurring through the domain may involve "transit" through architecture and systems residing in sovereign nations who may not have the

knowledge or capability to identify, restrict or interdict illicit or nefarious actions.

In light of these commonalities, one would expect formation of a federal regulatory body to govern the Cyber Domain comparable to those that exist for governing the maritime and air domains (e.g., the Federal Aviation Administration or the Federal Maritime Administration). Because cyberspace is a man-made domain, a variety of regulatory agencies lay claim to governing functions within it: the Federal Communications Commission, the National Security Agency, the Department of Homeland Security, and the Department of Commerce, to name a few. Additionally, when the threat of a cyber attack exists, an equally confusing array of defense, exploitative, and forensic authorities must be engaged to defend against such an attack. Was the attack directed against intellectual property or military secrets? Was the attack conducted by a state or a non-state actor? Can we ascertain who is responsible for the attack quickly enough to retaliate? What constitutes an act of war in cyberspace? And, in the event of an act of war, who has the authority to direct retaliatory (perhaps anticipatory) actions in response to a cyber threat? These are just a few of the questions that arise concerning the U.S. ability to anticipate and counter a dynamic cyber threat.

Complicating the cyber environment is the much-discussed low "cost of admission" to operate in cyberspace. Unlike the significant economic and technical/industrial capabilities and capacities required to become a space-faring nation, the national investment to have credible and respected cyber power is a bargain. For example, consider the reputed case of Russia's use of "botnets"[6] during the 2008 conflict in Georgia—as well as the assessed technical competence of Russian cyber intrusions. The damage inflicted by cyber warfare can be measured in multiple dimensions; lost intellectual property, state secrets, or “kinetic-like” effects on infrastructure. In comparison to an air strike or naval blockade or spy ring, the attractiveness of an aggressive, offensive cyber campaign is abundantly clear. But an army of competent cyber warriors cannot be quickly assembled by recruiting a ghost army of angry nerds huddled in poorly lit basements or drafty garages across Eastern Europe. State-level cyber warfare capabilities are expensive in real terms. However, investments in cyber capabilities are frequently measured in millions of dollars vice the billions of dollars it takes to build and sustain a modern, conventional military capabilities.

The Case of Estonia

In April and May of 2007 Estonia experienced a wide-ranging, three-week cyber attack on virtually every one of its major governmental information systems by a sophisticated – and experienced – enemy.[7] While Russia has consistently denied responsibility for this distributed denial-of-service barrage attack, it did appear to be the concluding event of a political dispute between Russia and Estonia. This multi-dimensional dispute escalated over the relocation of the Bronze Soldier monument in Tallinn that commemorates Soviet casualties in the Great Patriotic War (World War II).[8] The speed, effectiveness, and depth of the attacks were staggering, paralyzing the Estonian executive branch of government, all of the ministries, all of the state’s political parties, major banks, parliament, half of the news agencies, and a variety of telecommunication companies. As Europe’s most ‘netted’ country with the highest wireless connectivity rate per capita (viewed as a basic human right by the Estonian government), all Estonians immediately felt impact of this devastating attack.[9]

Equally intriguing was the institutional hand-wringing at the European Union (EU) and NATO regarding not *what to do*, but simply *what to say* about the attacks. Political considerations aside (Poland, for example, stymied EU efforts to issue a unanimous statement decrying the attack as an act of cyber warfare), this incident and the subsequent controversy within NATO revealed significant implications for Article V of the North Atlantic Treaty. This Article specifies that an attack on one member is an attack on all, yet it reserves individual national responses to the discretion of the individual member governments. This is the fundamental question: “If Estonia actually came under cyber attack, did the cooperative self-defense provision in Article V come into play?” Article V specifically states that “an armed attack against any ally” requires a response by the NATO members.[10] But, was Estonia subjected to an *armed* attack? Article IV certainly seemed to apply to the situation: “The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.”[11] The central problem was not just the cyber attack, but whether under the North Atlantic Treaty a cyber attack could be considered an attack in the traditional sense of the word.

Ultimately, NATO did nothing to assist Estonia – possibly because the attack caught NATO members off-guard. Although NATO military headquarters has erected a reasonable network defense architecture, many NATO members do not have any such system in place for their national governments. The attack highlighted a critical vulnerability in the 21st century NATO model: operations in cyberspace necessitate a review of defensive capabilities across all member nations. This review should include the cyber networks of civil governance, private and commercial critical infrastructure, and military cyber systems. Following the Estonian ordeal, a flurry of legal discussions, high level conferences, and new policies signaled a watershed in cyber warfare doctrine and theory on both sides of the Atlantic. In NATO, a "digital agenda" was established to set common priorities for the EU digital marketplace and European information and communication technology education.[12] Specific definitions of cyber war and cyber-terrorism were integrated into the NATO lexicon (largely framed by Ahmad Kamal's work, *The Law of CyberSpace*). And NATO's tenth center of excellence was established for Cooperative Cyber Defense (CCDCOE) at, of all places, Tallinn.[13] Perhaps the most important (if underplayed) outcome was CCDCOE's recognition of the need for collaboration among government, military, private and commercial institutions for defense-in-depth of dual-use information technologies.

Across the Atlantic, the U.S. government has been besieged by internal cyber issues as well. Immediately prior to the Estonian attack, the U.S. Air Force publicly acknowledged a deep intrusion by a foreign entity into contractor-held computer systems supporting the Joint Strike Fighter program. In the months following the Estonian attack, the DoD was subjected to a malicious code propagation (labeled as "Agent.btz") through U.S. Central Command. In response, DoD engaged all of the Department's cyber resources (code named Operation BUCKSHOT YANKEE) to address the problem.[14] Most experts concur that the Agent.btz malicious code was part of a Russian attack.[15] However, attacks known to have originated from within China have exfiltrated terabytes of information. In fact, the Munk Centre for International

Studies, a Toronto-based think tank, estimates China has conducted successful cyber espionage intrusions in 103 countries employing *GhostNet* architecture in a complex strategy to “win the information war.”[16]

As the DoD grappled with these major cyber espionage events, DHS was designated the lead federal agency for protection of critical infrastructure, including cyberspace. DHS was assigned this critical task despite growing evidence that Russia and China had clearly and deliberately organized cyber forces to conduct state-on-state information warfare campaigns. Designating DHS as the lead, while reserving specific authorities for the military has generated unsettling uncertainty regarding the Administration’s policy on cyber attacks resulting in the following question: “Are these attacks purely law enforcement issue or a national security issue that requires an integrated response posture unidentified in current policy?” The situation has not been clarified appreciably since the Estonian attack. In a report to Congress in November 2011, the Office of National Counterintelligence stated bluntly:

> Billions of dollars of trade secrets, technology and intellectual property are being siphoned each year from the computer systems of U.S. government agencies, corporations and research institutions to benefit the economies of China and other countries…[17]

The lessons NATO seems to have learned following Estonia’s experience of a major cyber attack appear to have been noticed – but ignored – by the U.S. government. The implications of a major cyber attack on the economic and information systems of the U.S. commercial sector during a simultaneous attack across the federal government are arguably catastrophic.

Organizing for Cyber Warfare

The 2010 Joint Operating Environment (JOE), the 2011 International Strategy for Cyberspace, and the 2011 Department of Defense Strategy for Operating in Cyberspace all acknowledge that the DoD must consider all operations in cyberspace to have implications for the security of all elements of national power—through the full depth, breadth, and scope of governmental, military, private, and corporate infrastructure.[18] [19] The current military mission in cyberspace is not fully responsive to the President's guidance to maintain "an **inherent right to self-defense** that may be triggered by **certain aggressive acts** in cyberspace" (emphasis in original).[20]Across the federal agencies, the Departments of State, Justice, and Commerce have responsibility for the preponderance of U.S. involvement in global cyber security and governance agreements, entities, and efforts. However, the preponderance of U.S. cyber warfare investments focus on military issues and intelligence collection.[21]

Despite the exploitation of cyberspace as a viable commercial and informational domain for more than 30 years, the DoD has struggled to integrate its role in this domain with the roles of the broader interagency. Although the DoD requirement to classify systems and capabilities tied to intelligence collection and cyber defense/attack methodologies is both understandable and reasonable as justification for keeping the other Departments and Agencies at arm's length, it creates a two-fold problem. First, it fosters a pervasive attitude that a man-made domain is simply a collection of operating systems and their interfaces (e.g., hardware, software, data transmission, and human operators). Hence, a set-piece process of firewalls, accreditation, and technical improvement provides sufficient defense in the Cyber Domain. This view essentially degrades a complex warfighting domain to the level of rudimentary warfare akin to siege craft and castles. This mindset ignores the exceptionally complex nature of the cyber domain and its fluid environment in which military operations constitute only a small fraction of its activities.

Second, the military's current organizing construct for conducting cyber operations is misguided. This construct has evolved from each of the DoD's communications and intelligence "tribes." Each tribe has developed legacy capabilities and counter-capabilities largely independent of other tribes' efforts. While the U.S. was following this dysfunctional, suboptimal approach, its competitor nations with less restrained doctrinal views of the cyber domain wreaked havoc with the intellectual property of defense contractors and planted untold volumes of malicious code and spyware in U.S. defense information systems. These actors effectively shaped the cyber environment before the U.S. military realized it was, in effect, engaged in a "cyber war."

Vice Admiral Arthur Cebrowski, former head of the DoD's Office for Transformation, published several papers and articles through 2004 advancing an important conceptual point. Simply stated, his thesis was that "beyond the more rigid definitions of systems and enablers, cyberspace is a new strategic common." He described cyberspace as:

> …the domain of information and cognition that includes the channels of mass media and finance. Like its conceptual predecessors, it is an international domain of trade and intercontinental communication. Increasingly, it can increase, sustain or diminish a nation's position of power in economic, diplomatic, or military terms.[22]

Similar to the maritime and air domains, cyberspace is dominated by private investment, business innovation, and commercial use. But cyberspace is exponentially more pervasive than the maritime and air domains. Nonetheless, conceiving the implications of the cyber domain in terms of Sea Power Theory may prove useful. For example, a massive naval fleet patrolling the world's oceans—as Alfred T. Mahan advocated—may be far less effective than positioning several smaller naval elements to patrol potential hot-spots and to protect our trade routes as Julian Corbett articulated.[23] A cyber corollary would posit that providing defense-in-depth of only those nodes vital to the defense industrial base, while simultaneously providing for an exploitative and attack capability to be used only when necessary, may be the best course of action rather than a Mahanian "defend all, attack everything" mode of systems defense and "brute cyber force." This cyber strategy is arguably moot because the "cyber gates" have already been breached making it necessary for the federal government contend with enemies within as well as external threats. The fact that the enemy is "within the gates" also makes it necessary to integrate domestic law enforcement into the national cyber defense architecture.

Domestic law enforcement in cyberspace is complex. The Defense Cyber Crimes Center (DCCC) and its law enforcement agency liaisons are bound by law to orient and operate against only clearly defined, domestically based criminal attacks or acts. But state-sponsored espionage and attacks on the defense architecture remain Title 10 and Title 50 operations managed by Cyber Command's Service components and the National Security Agency (NSA). This construct requires an unrealistic level of coordination *in real time* to monitor and exploit an attack, and then develop Title 10 response options (when applicable and only if approved). This compartmentalization of authorities among commands and agencies is insufficient for post-attack forensics or for characterizing a transient attack when an attack lasts mere seconds. Similarly, law enforcement agencies must cede monitoring responsibility of a cyber attack when Title 10 (Armed Service Secretary or Combatant Commander) or Title 50 (technical intelligence gathering) authorities are required. Overall, the current interagency construct is a confusing myriad of competing authorities. This uncoordinated diffusion of authority and responsibility hinders the federal capacity to operate offensively in cyberspace and cedes freedom of maneuver to an enemy.

The Corbett-like approach to cyber defense would also enable the government, military, private and commercial sectors to better coordinate and synchronize their activities, thereby enhancing DoD's intelligence and cyber superiority missions. This may require the commercial sector to subordinate some of its priorities to the economic, statutory – and even diplomatic – controls necessary to sustain national security within cyberspace, much as commercial aviation shares the skies with military flights. Unifying cyber defense under a single agency for coordination and control provides significant advantages for strengthening national cyber security, particularly given limited federal resources to meet the emerging threat and competing commercial and private interests.

Assessing the Next Threat and Calculating Risk

Nothing in this world is free. Certainly in a time of fiscal austerity for all federal departments and agencies, the need to evaluate priorities for allocating resources is even more essential. So, against what threat should the nation focus its scarce national resources? The problem is difficult to frame in clear terms. What does appear to be clear however is that the intellectual property of the U.S. is a key target that is currently under attack by organized cyber espionage. Additionally, the potential for a deliberate, state-on-state cyber attack is not just possible, but likely.

Regarding intellectual property, we must expand the working definitions of what is meant by the term. In an all encompassing sense, intellectual property should include the product of individual expression (such as music, art, poetry, architectural design, etc.) as well as the culmination of years of business expertise, research, and technological advances. What used to be viewed as a corporate secret – not necessarily the target of state-sponsored espionage – is now the principal target of economic espionage through cyberspace. Steven Chabinsky, Deputy Assitant Direcotr of the FBI's Cyber Division, provided candid – and eye-opening – commentary on this issue:

> This is definitely the golden age of cyber espionage." Foreign states are stealing data left and right from private-sector companies, nonprofit organizations and government agencies.[24]

A key problem is the seeming failure of U.S. national leadership to recognize cyber espionage as a form of information and economic warfare. The commercial sector produces new technologies and capabilities employed by the federal government—the government itself does not produce or design information technology.[25] If a competitor nation - like China or Russia - with a nationalized business model can acquire the trade secrets of these companies, they can compete in the market-place without having to develop the product through costly and time intensive research and innovation, making their product cheaper and comparable U.S. products more expensive. Worse, as the U.S. company fails to compete successfully, it may also fail as a viable business model. So, the U.S. technological advantage dissipates. In effect, the advantage has been stolen and then used against the United States. However, viewing this reality as a threat requires a cognitive strategic awareness which U.S. leaders seem to lack.

According to National Security Agency Director General Keith Alexander, in only two days a major American company recently lost one billion dollars worth of intellectual property developed over 20-plus years.[26] In many cases the victims can't place a precise value on the stolen information. In other cases, the cost is staggering: "$100 million worth of insecticide research from Dow Chemical; $400 million worth of chemical formulas from DuPont; and $600 million of proprietary data from Motorola."[27]

Beyond this economic threat is the very real potential of a state-sponsored attack on the United States – beyond the scope of that which occurred in Estonia. What would happen if a competitor nation decided that acquiring a credible cyber warfare capability was in its vital interest, and that the principal target for this capability was the U.S.? Unfortunately, this is not fiction but a developing reality.

In mid-December 2011, Iran announced investment of $1 billion in its defensive and offensive cyber warfare capabilities. At the same time, Univision aired a documentary of Venezuelan and Iranian diplomats receiving a briefing on future cyber attacks on the U.S.[28] It is hard to evaluate the viability of Iranian offensive cyber capabilities. But it is not so difficult to estimate the formidable skills of Russian and Chinese experts with whom Iran has collaborated in recent years to develop cyber capabilities. Iran's interest in an offensive cyber weapon is as much a factor of prestige as revenge. However, revenge may be the key, given the case of the "Stuxnet" malicious code which propagated through the Iranian nuclear enrichment facilities at Natanz[29] in 2010. Interestingly, Iran did not immediately acknowledge the attack, although the malicious code destroyed a number of uranium enrichment centrifuges and industrial system controllers. Although this cyber attack is generally assumed to be an

Israeli or Israeli-U.S. cyber attack, the source of the malicious code (as indicated by Russian-owned Kaspersky Labs) was untraceable.

> Kaspersky Lab has not seen enough evidence to identify the attackers or the intended target but we can confirm that this is a one-of-a-kind, sophisticated malware attack backed by a well-funded, highly skilled attack team with intimate knowledge of SCADA technology. We believe this type of attack could only be conducted with nation-state support and backing.[30]

Israel has established a precedent for taking military action against the nuclear capabilities of its adversarial neighbors. It is plausible that Stuxnet was the cyber equivalent of an air strike. Such a cyber attack may be an Israeli strategic choice: “Israel certainly has the ability to create Stuxnet…and there is little downside to such an attack, because it would be virtually impossible to prove who did it.”[31] Interestingly, a cyber attack may have neutralized ground radar and anti-aircraft systems in Syria prior to the September 2007 Israeli Air Force strike on an alleged reactor site in Deir-ez-Zor during Operation ORCHARD.[32] Whether or not ORCHARD was a precursor to the Natanz / Stuxnet cyber attack, the damage to the Natanz facility was significant. [33] Indeed, it spread to several hundred personal computers and the associated Siemans-controlled industrial systems, including sub-components of the Bushehr Reactor Facility. No matter who launched Stuxnet, the global community has received a clear message: Cyber warfare is now a viable tool in the national arsenal and may be employed with or without conventional military forces. Iran and its technical assistants in North Korea now have all the incentive and the technical know-how they will ever need to develop an offensive cyber warfare capability and employ it against the U.S.

Whole of Government Approach?

U.S. Cyber Command was organized to provide a command and control element capable of synergizing the nation's defensive cyber operations and architectures with intelligence gathering (ie, computer network exploitation) and attack options resident within the National Security Agency (NSA) in support of Geographic Combatant Commands, the Services, and Defense Agencies. In short, Cyber Command was conceived as the clearing house for all cyber warfare activities for the joint community and to serve as the DoD interface with the interagency.

Arguably, Cyber Command does not yet have a sufficient track record to be assessed as adequate to perform its mission. However, the risk incurred with conducting *business as usual* given the steadily growing threat of cyber espionage and the implications of a major cyber attack like that executed on Estonia in 2007 leaves little doubt that a whole of government approach is needed to protect the economic and political underpinnings of our country. The defense of our government, private, and corporate information and banking systems is at least equal in importance – possibly of greater importance – than protecting the military's cyber infrastructure.

One defense agency is specifically charged with the integration and standardization of the defensive and technical components of the DoD's cyber portfolio: the Defense Information Systems Agency (DISA). With its information technology portfolio easily eclipsing that of any other federal agency (measured in billions of dollars and employing nearly 170,000 dedicated communications, information and cyber personnel), the DoD has a surprisingly discordant array of cyber and network architectures.[34] DISA, one part of this corporate structure headed by the Deputy Assistant Secretary of Defense (DASD) for Cyber, Identity, and Information Assurance, was to be enhanced by the addition of a new sub-Secretariat for Networks, Integration and Information (NII). DISA was initially planned to become part of U.S. Cyber Command's integrated span of control. This initiative would have unified defensive and interoperability standards under a single DASD by integrating the NII/DISA roles and missions to provide a unified approach to standardization across the DoD information technology portfolio. This effort to create a DoD-wide enterprise information technology strategy, possibly as a precursor to an interagency Federal Information Technology Sharing Directive, would have provided the catalyst needed to ensure unity of effort, a defendable baseline of software and hardware, and a governmental accreditation standard. However, in July 2011, in one of his final official acts, Secretary of Defense Robert Gates disapprove the the DISA and Cyber Command merger. The NII office was then officially disbanded. Touted as an efficiency-in-government measure, this action has yet to prove efficient across the cyber defense portfolio in terms of interoperability, unity of acquisition (strategy and accreditation), or oversight under a single Deputy Assistant Secretary of Defense (DASD) or Unified/Sub-unified Commander. The most recent National Defense Authorization Act seems to direct a DoD information technology strategy modeled on commercial "cloud" servers. Its specific language countermands DISA's directive to manage a central common DoD server.[35]

In view of the seeming inability of DoD to formulate a coherent strategy to fulfill Title 10 and Title 50 cyber requirements v – as balanced against the information technology enterprise – no interagency proposal has yet been advanced to address the nation's cyber vulnerabilities. Currently, responsibilities for the nation's cyber defense reside in certain legal authorizations and diverse direction from various federal agencies that make up a loose interagency architecture to manage issues of cost-sharing, standardization, and protocols of cyber defense. The benefit of a truly consolidated and defendable federal cyber portfolio appears to remain a goal – but, not at the expense of each department's autonomy. If a severe external catalyst is required to achieve such integration, the cost of such an attack may be far too expensive for our national security to bear. The reality of such a threat demands a fresh review of legal authorities and organizational constructs.

Recommendations

The cyber policy review directed by the President suggests three possible options to address the perceived disconnect between U.S. Code cyber authorities and current federal agency authorities.[36] The most effective solution must balance three imperatives to:

- measurably improve national cyber security by consolidating necessary authorities in order to enhance interagency capacity to operate in cyberspace;
- integrate allied and commercial cyber efforts; and
- deny adversaries freedom to act in cyberspace.

One option that satisfies these three imperatives is to continue with U.S. Cyber Command as a sub-unified functional command with operational authority over NSA and Service Title 10 cyber warfare capabilities. Under this option, the security classification and controls necessary to conduct Title 50 operations would be preserved, but Title 10 authorities would be separated from Title 18 to preclude the appearance of a "digital posse-comitatus" as interpreted through 18 U.S.C. subsection 1385. Specifically, the requirement to conduct intelligence operations in cyberspace would be sustained, but the warfighting and law enforcement elements—and their appropriate legal statutes—would remain separated. This approach would support current U.S. policy to not militarize cyberspace. However, the opportunity costs with such a minimalist approach may be unacceptably high given our current inability to uniformly respond to cyber threats which are currently addressed by more than one set of U.S. Code authorities. In effect, the current approach is cumbersome and diffuse. It fosters an environment in which the attacker is the only fluid player. If this option is implemented, interagency efforts in cyberspace would remain as they are for law enforcement and for commercial and international players. Further, Cyber Command as a military-only solution retains the risk of sustaining a functional seam between the attacker and the Title 10/18 exercising authorities. Cyber Command may continue to identify and disclose vulnerabilities throughout U.S. networks.

A second option would segregate authorities that employ cyber capabilities in a centralized control/decentralized execution scheme akin to the current employment of airpower. This option entails two key requirements. First, consistent with Presidential guidance, the DoD must meet interoperability goals by establishing a single agency responsible for all hardware, software, and transmission accreditation as a federal standard. Second, this agency must be empowered with the preponderance of defensive capability and exercise institutional control over all federal system firewalls, authentication and access standards, and security classification/encryption baselines across the U.S. government. This option would advantageously impose a stable process to address the majority of vulnerabilities across the federal information system architecture. However, if this agency lacks the authority to compel other federal agencies and departments to comply with its regulations, it may not fulfill its mission. This risk can be mitigated only if funding for information technology and cyber systems is also centralized. Without a compulsory mechanism, it could not effectively accredit the security of the government's operating systems. To succeed, this option must address how different agencies with disparate U.S. Code authorities can operate collaboratively within cyberspace in a unified effort. Lacking such provisions, this option would not resolve the core problem. Even so, it would improve the nation's cyber defense.

Despite failing to address the issue of a single entity prosecuting cyber crimes and threats, this option remains attractive from the perspective of a standardized network defense and DoD's autonomy. It would likely be the most palatable option in political terms. Federal agencies and departments could maintain their autonomy to develop and field software, systems and operating environments to meet their mission requirement while enabling a single agency to standardize a basic level of security, certification, and incident response capabilities.

A third option would transform U.S. Cyber Command from a sub-unified command to the headquarters of a Joint Interagency Task Force (JIATF). As a JIATF, the DCCC and NSA cyber elements would form the core of a netted operational command that would consolidate cyber control elements from other federal agencies. Thus a single commander at the JIATF would inherit authorities delegated by all of the component federal partners (U.S.C. 6, 10, 18, etc), but would not assume a "force provider" role. A JIATF could operate across federal agency authorities (U.S. Code) as a single command responsible for coordinating and conducting law enforcement, network defense, cyber security, intelligence exploitation, and cyber warfare. For addressing system accreditation and interoperability, the original plan to place DISA as the central coordinating and control authority remains the most viable option. The decision to move away from an enterprise approach to dismantle the single common server solution under DISA may prove to be misguided—especially when whole-of-government cyber security requirements are weighed against the growing threat.

One example of a functioning, successful, mission-oriented JIATF model can be found in the federal counter-narcotics effort at Joint Interagency Task Force – South (JIATF-South). This Task Force operates under the command of a U.S. Coast Guard flag officer with elements of the command holding both Title 10 and Title 14 law enforcement authorities. Incorporating nearly a dozen federal agencies it has reached a high level of success after nearly 23 years of experimental and iterative growth both within the task force itself and in terms of the interagency pursuit of unity of effort. The JIATF option provides the requisite depth, breadth, and scope of response across U.S. Code authorities. It also enables constituent federal agencies and military services to procure, operate, and defend their information systems and networks. A JIATF model would provide the most clearly defined consolidation of authorities to plan, coordinate, integrate, and synchronize law enforcement and military missions in cyberspace. However, the JIATF option also risks a political reaction. Any perceived U.S. efforts to militarize cyberspace would not be well received by the commercial telecommunications industry and by certain competitor nations. Therefore, if this option is pursued, a strategic communication campaign explaining the interagency nature of the JIATF would be required well in advance of the announcement of its formation.

Conclusion

In the JIATF construct, the role of organizing, training, and equipping the component pieces of the task force would remain within the purview of the military services and other federal departments and agencies, subject to DISA-directed standardization and accreditation. In this approach, each element of the federal cyber infrastructure would be individually responsible for consolidation of security standards and operations, yet each constituent would retain its identity and ability to operate in cyberspace. A benefit to this approach would be the potential cost savings from the use of standardized software, a reduced number of network operations centers, and a diminished bandwidth requirement for duplicate transmission backbones. Federal agencies with smaller resource pools could realize economies of scale from larger, interdepartmental procurement efforts. Ultimately, the highest payoff of a single integrated command operating across all relevant legal authorities to address all aspects of national cyberspace security can be achieved in a JIATF construct. However, this option is not without risk. The perceived militarization of cyberspace may muddle political and diplomatic sensitivities regarding cyber operations for the Departments of State, Commerce, and Justice and may complicate the commercial and private sector's integration of their cyber systems with the federal government.

Given the nature of evolving cyber threats, DoD must re-orient its operating parameters relative to all federal agencies. This new approach would leverage an economy-of-force effort to provide collective cyber defense and multilateral operations (as articulated in the 8 June 2011 NATO Cyber Defence Policy). It would also consolidate authorities to address and respond to threats to the nation's cyber security. Historically, nations go to war for reasons of national prestige, pursuit of vital interests, or fear of attack. Recently Russia allegedly employed cyber power against Estonia for reasons relating to national prestige. China has employed cyber power to acquire economic dominance. And perhaps some nations have engaged in cyber warfare to preempt a clear nuclear threat.

Clausewitz's preeminent advice to strategists was to know when you are at war and the nature of that war. The United States is under cyber attack in a war which our national leadership has not yet acknowledged. This new form of warfare has been directed against our national information infrastructure. The threat of future – and more damaging – attacks has been signaled by Iran and those who would challenge U.S. global leadership. Now is the time to organize and fight this war that is being waged against our nation. Now is the time to unify and refocus United States cyber defenses to protect the nation's vital interests in cyberspace.

Endnotes

[1] Here the term "Federal" is used to specifically address whole of government as opposed to just the Department of Defense or Department of Homeland Security.

[2] The United States Government Printing Office Home Page, http://www.gpoaccess.gov/uscode/about.html (accessed November 15, 2011).

[3] The United States Government Printing Office Home Page, http://www.gpoaccess.gov/uscode/about.html (accessed November 15, 2011).

[4] 6 U.S.C. (Domestic Security) Chapter 1 governs the Department of Homeland Security; subchapter II describes DHS's role in information security and critical infrastructure protection.

[5] US Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13 (Washington DC: US Joint Chiefs of Staff, February 13, 2006), I-1. The five warfighting domains are air, land, sea, space, and cyber. Of the five, only cyber is man-made and the domain is dependent upon man's continued, deliberate operation of systems and electromagnetic principles to exist.

[6] Remote robotic networks (aka, "botnets" or "zombie army") are the result of several netted computers operating in concert toward an execution – or series of executions – designed by an outside entity without the computer owner/operator's involvement through corruption or

usurpation of the computers' access to the network and operating system. Microsoft Corporation agrees with US and NATO definitions of cyber activity of this nature, and their corporate home page offers the following commentary: "Criminals distribute malicious software (also known as malware) that can turn [a] computer into a bot (also known as a zombie). When this occurs, [the] computer can perform automated tasks over the Internet, without [the operator] knowing it. Criminals typically use bots to infect large numbers of computers. These computers form a network, or a *botnet*. Criminals use botnets to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. If [a] computer becomes part of a botnet, [the] computer might slow down and [the host] might inadvertently be helping criminals." (Microsoft Corporation Safety and Security Center Home Page http://www.microsoft.com/security/resources/botnet-whatis.aspx (accessed February 12, 2012). The true danger of a botnet is that each infected or usurped computer has a traceable entry through the network, but it is figuratively impossible to determine which individual "zombie" is the actual source of the attack, which assumes one of the attacking computers is, indeed, a source computer. Attack attribution is nearly impossible to determine.

[7] Haly Laasme, "Estonia: Cyber Window into the Future of NATO," *Joint Force Quarterly*, 4th Quarter, October, 2011, 58-63.

[8] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 16, 2007.

[9] Haly Laasme, "Estonia: Cyber Window into the Future of NATO," *Joint Force Quarterly*, 4th Quarter, October, 2011, 59.

[10] Haly Laasme, "Estonia: Cyber Window into the Future of NATO," *Joint Force Quarterly*, 4th Quarter, October, 2011, 59.

[11] The North Atlantic Treaty, Article IV http://www.nato.int/ cps/en/natolive/ official_texts_17120.htm (accessed November 19, 2011).

[12] Haly Laasme, "Estonia: Cyber Window into the Future of NATO," Joint Force Quarterly, 4th Quarter, October, 2011, 60.

[13] Haly Laasme, "Estonia: Cyber Window into the Future of NATO," *Joint Force Quarterly*, 4th Quarter, October, 2011, 61.

[14] Phil Stewart and Jim Wolf, "Old Worm Won't Die After 2008 Attack on Military," *Reuters*, June 16, 2011.

[15] Phil Stewart and Jim Wolf, "Old Worm Won't Die After 2008 Attack on Military," *Reuters*, June 16, 2011.

[16] Malcolm Moore, "China's Global Cyber-espionage Network GhostNet Penetrates 103 Countries," *The Telegraph*, March 29, 2009.

[17] Ellen Nakashima, "China, Russia Are Main Culprits in Cyberspying, US Agency Says," *Pittsburg Post Gazette*, November 4, 2011.

[18] Barrack H. Obama, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (Washington, DC: The White House, May 2011), pp. 11-14. Issued in 2011, this document addresses the basic problem scope for nations in today's cyberspace domain: diplomacy, defense, and development. The document articulates seven policy priorities which frame interagency and alliance-based operations rather than a compartmented strategy focused more on geography that the reality of the cyber domain.

[19] Robert M. Gates, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: The Pentagon, July 2011), pp. 5-7.

[20] Barrack H. Obama, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (Washington, DC: The White House, May 2011), pp. 10.

[21] U.S. Government Accountability Office, Cyberspace: Report to Congressional Committees (Washington, DC: U.S. Government Accountability Office, July 2010), pp. 30.

[22] Arthur K. Cebrowski, "Transforming Transformation -- Will it Change the Character of War?" May 25, 2004,http://www.au.af.mil/au/awc/awcgate/cia/nic2020/ceb_transformation25may04.pdf (accessed November 15, 2011), pp. 11. See also Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *U.S. Naval Institute Proceedings* 124, no. 1 (January 1998), 28–35.

[23] Julian S. Corbett, *Some Principles of Maritime Strat*egy. New York, Longmans, Green and Co., 1911. Corbett advances the counter-Mahanian argument by stating a Fleet in Being can simultaneously protect trade as well as posture a combatant force along the enemy's sea lines of communication. This strategy, contrary to a singular large fleet existing solely to seek out and destroy the enemy fleet, provides the opportunity for the other elements of national power to be brought to bear and ultimately provide both means and ways to achieve the strategic ends.

[24] Ellen Nakashima, "China, Russia Are Main Culprits in Cyberspying, U.S. Agency Says," *Pittsburg Post Gazette*, November 4, 2011.

[25] Certainly, organizations like the Defense Advanced Research Projects Agency and the various military department research organizations do, on occasion, "create" technologies or capabilities. The author's point is that the economic and technological base in America is in the hands of commercial corporations and not a nationalized or state-owned entity.

[26] Ellen Nakashima, "China, Russia Are Main Culprits in Cyberspying, U.S. Agency Says," *Pittsburg Post Gazette*, November 4, 2011.

[27] Ellen Nakashima, "China, Russia Are Main Culprits in Cyberspying, U.S. Agency Says," *Pittsburg Post Gazette*, November 4, 2011.

[28] Yaakov Katz, "Iran Embarks on $1B Cyberwarfare Program," *The Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/ Article.aspx?id=249864(accessed December 20, 2011).

[29] Lukas Milevski, "Stuxnet and Strategy: A Special Operation in Cyberspace?" *Joint Force Quarterly*, 4th Quarter, October, 2011, 64-69. The malicious code (actually a worm designed to

target industrial systems and subvert them using a programmable logic controller rootkit) was publicly discovered in August 2010 when Siemans-produced SCADA systems became infected. Approximately 60% of the infected systems reside in Iran, and are employed to control uranium enrichment centrifuges. Out of an estimated 9,000 units, at least 1,000 and as many as 2,000 were destroyed as a result of the attack.

[30] Kaspersky Labs, "Kaspersky Labs Provides Its Insight on Stuxnet Worm," *Kaspersky Labs Home Pag*e, September 24, 2010 http://www.kaspersky.com/about/news/virus/2010/ Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm (accessed December 20, 2011).

[31] "The Stuxnet Outbreak: A Worm In The Centrifuge," *The Economist Newspaper Limited*, September 30, 2010 http://www.economist.com/node/ 17147818 (accessed December 20, 2011).

[32] Dan Williams, "ANALYSIS: Wary of Naked Force, Israelis Eye Cyber War on Iran," *Reuters*, July 7, 2009.

[33] Peter Beaumont, "Was Israeli Raid a Dry Run for Attack on Iran?" *The Observer*, September 15, 2007 http://www.guardian.co.uk/world/2007/ sep/16/iran.israel (accessed December 20, 2011).

[34] John Foley, "Pentagon Unveils Enterprise IT Strategy," *Information Week* Online, December 15, 2011, http://www.informationweek.com/news/government/policy/232300614 (accessed February 12, 2012).

[35] J. Nicholas Hoover, "Feds Launch Shared Services Initiative", *Information Week* Online, December 13, 2011, http://www.informationweek.com/news/government/policy/ 232300440?itc=edit_in_body_cross (accessed February 12, 2012). As the article indicates, the Shared Services initiative by the new US Chief Information Officer, Steven VanRoekel, may go a long way to trimming the cost of interdepartmental IT costs while simultaneously enhancing interoperability. While the DoD is still an insular player – in fact only the Army has formally signed up to a single DISA-managed email server, though the other Services may follow suit – other federal agencies are being driven toward collaboration on software suites, applications, and information management servers. The draft document "Federal Information Technology Shared Services Stragegy" was released by VanRoekel's staff to all federal agencies for input on December 8, 2011, with a multi-phased approach and deadlines for initial collaboration as early as February and March of 2012. Whether this will become a viable IT Enterprise solution or merely a cost-cutting venture is yet to be seen.

[36] Barrack H. Obama, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: The White House, January 3, 2012), pp. 3-5, 8. In addition to the National Security Strategy, National Military Strategy, and the previously cited International Cyberspace Strategy, the President has released more detailed (and fiscally relevant) direction regarding Defense Strategic Guidance.