National Cyber Doctrine: The Missing Link in the Application of American Cyber Power

Mark D. Young[*]

On June 23, 2009, Secretary of Defense Robert Gates established the U.S. Cyber Command as a sub-unified command under the U.S. Strategic Command in order to defend military information networks against cyber attacks.[1] This organization is the most recent Department of Defense (DoD) response to the increasing threats to U.S. military, government, and commercial information systems and rapidly developing adversarial network capabilities.

Such capabilities are illustrated by the Russian attacks in Estonia and Georgia that disabled government, banking, and media web sites. The U.S. air traffic control and telecommunications systems have also been attacked, and the U.S. electric power grid has been hacked by both China and Russia. Software used to disrupt the power grid control systems was installed by the hackers and could have caused massive power outages, and congressional offices have received reports that China has infiltrated Congress's information systems.[2]

The protection of vital U.S. interests in cyberspace requires adjustments to the applications of all aspects of U.S. power. Network intrusions continue to confound geographically- and politically-based U.S. government organizations, while those engaged in illicit activities exploit the borderless nature of cyberspace. The current division of cyber labor in the U.S. Government is unbalanced: the capacity of civilian agencies is too small, while the Defense Department's role in network operations is too large.[3] "Civilian agencies, it is argued, are under-resourced, under-staffed, non-optimally organized and trained, and/or lack the necessary expeditionary institutional culture."[4]

The lack of civilian capacity to address national security threats – including those from, in, and through cyberspace – forces military elements

[*] Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence. The views expressed in this article are those of the author and do not reflect the official policy or position of any members or staff of the House Permanent Select Committee on Intelligence or any part of the U. S. government. This article is derived entirely from open source material and contains no classified information.

[1] Ellen Nakashima, *Gates Creates Cyber-Defense Command*, WASH. POST, June 24, 2009, at 8.

[2] Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies*, WALL ST. J., Apr. 8, 2009, at A1.

[3] *See generally* Catherine Dale, Nina Serafino & Pat Towell, *Organizing the National Government for National Security: Overview of the Interagency Reform Debates* 6-7 (Cong. Res. Serv. RL 34455), Dec. 16, 2008.

[4] *Id.*

to address security requirements that they may be less qualified to satisfy. Although the Department of Homeland Security (DHS) has the responsibility for securing the high-level Internet "gov" domain, it lacks the expertise and capacity of the DoD. National security operations cannot wait while the limitations on civilian capacity are overcome by foreign planning, budgeting, and training. The national security sector must use existing capabilities to address immediate threats. Although the Cyber Command is not currently defending civilian or commercial networks, this option may soon be considered necessary. There are risks to giving the Cyber Command the lead in establishing practices by which critical national security networks can be secured, but that may be the most viable option for the near future.

Whether directed by the Cyber Command or by other government agencies, the employment of U.S. power in the cyber domain requires a rapid paradigm shift uncharacteristic of the DoD. To accelerate this shift, the national security community needs a new doctrine to provide the fundamental principles by which executive branch departments and agencies can ensure the freedom of U.S. action in cyberspace. The DoD controls most of the expertise in computer network operations and is well positioned to lead the national security community in establishing U.S. cyber policies and doctrines. It cannot do this alone, however.

This article argues that a national cyber doctrine is necessary. It is the link between strategy and the execution of the missions of the national security sector. Doctrine may traditionally be a military notion, but agencies are acknowledging the wisdom of establishing guiding principles. A national cyber doctrine can be a vehicle used to define the roles of departments and agencies for the entire U.S. government. In contrast to a presidential executive order or a National Security Council directive, a doctrine is developed in an openly collaborative fashion.

Author David Kilcullen's observations regarding counterinsurgency collaboration are also applicable to the development of a national cyber doctrine: "To be effective, we must marshal not only all agencies of the [U.S. government], but also all agencies of a host nation, multiple foreign allies and coalition partners, international institutions, nongovernment organizations . . . international and local media, religious and community groups, and charities and businesses."[5]

The DoD has developed an extensive collection of doctrines that guide military operations, but there is no doctrine to guide applications of national cyberpower. Cyber Command's missions are being formulated without an adequate doctrine to define the strategic context, establish the fundamentals of cyberpower, or debate issues concerning computer network operations. The Secretary of Defense memorandum ordering the establishment of the

[5] David Kilcullen, Three Pillars of Counterinsurgency, Remarks Delivered at the U.S. Government Counterinsurgency Conference, Washington D.C., at 1-2 (Sept. 28, 2006), *available at* http://www.au.af.mil/au/awc/awcgate/uscoin/3pillars_of_counterinsurgency.pdf.

Cyber Command mandates the synchronization of cyberwar effects "across the global security environment as well as providing support to civil authorities and international partners."[6] Coordination of interagency cyber operations and cooperation with civil and foreign partners are the types of activities for which doctrine is well suited. Other DoD doctrines govern similar activities in the sea, air, land, and space domains.[7]

While the DoD has no authority to enforce military doctrines outside of the Department, sound principles developed with the full participation of interagency partners will be followed due to their utility and effectiveness, not because of coercion. As has been observed, "You cannot command what you do not control."[8] Therefore the doctrine should foster a unified effort across the entire U.S. national security community. Its success will depend "on a shared diagnosis of the problem, platforms for collaboration, information sharing and deconfliction."[9]

The current U.S. counterinsurgency doctrine provides a model of how an inclusive doctrine can gain acceptance throughout the national security community. The development of the counterinsurgency doctrine was directed by then Lieutenant General David Petraeus after his return from his second tour of duty in Iraq in 2004. Petraeus brought together traditional and nontraditional partners to devise fundamental principles by which to address an extremely difficult set of combat circumstances. Some "military officers questioned the utility of the representatives from nongovernment organizations (NGOs) and the media, but they proved to be the most insightful of commentators."[10]

The application of cyberpower is just as complicated as counterinsurgency operations, and in many ways it is more complicated. The success of the counterinsurgency doctrine, produced by a group of collaborators that included those typically excluded from the development of military doctrine, shows the wisdom of an inclusive approach.

By creating a diverse community of interest to draft cyber doctrine, the national security community can more adequately address long-standing questions about U.S. activities in cyberspace: How should the government

[6] Memorandum from Robert M. Gates to the Secretaries of the Military Departments, Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations (June 23, 2009).

[7] *See generally* JOINT CHIEFS OF STAFF, JOINT PUB. 2.0: JOINT INTELLIGENCE (2007), *available at* http://www.fas.org/irp/doddir/dod/jp2_0.pdf; JOINT PUB. 3.0: JOINT OPERATIONS (2006, AS AMENDED IN 2008), *available at* http://ftp.fas.org/irp/doddir/dod/jp3_0.pdf; JOINT PUB. 4.0: JOINT LOGISTICS (2008), *available at* http://www.fas.org/irp/doddir/dod/ jp4_0.pdf; JOINT PUB. 5.0: JOINT OPERATION PLANNING (2006), *available at* http://www.fas.org/irp/doddir/dod/jp5_0.pdf.

[8] Kilcullen, *supra* note 5, at 4.

[9] *Id.*

[10] John A. Nagl, *The Evolution and Importance of Army/Marine Corps Field Manual 3-24 Counterinsurgency*, *in* THE U.S. ARMY/MARINE CORPS COUNTERINSURGENCY FIELD MANUAL xvi (Univ. of Chicago Press ed. 2007).

act to protect privacy while undertaking robust efforts to prevent cyber attacks? How will the Cyber Command support the strategic goal of defending the U.S. economy? What are the likely consequences of and who will be responsible for responding to a successful cyber attack that results in loss of life or destruction of property?

Doctrines are developed by a process that can answer these policy questions, even if only on a temporary basis.

> The Chairman of the Joint Chiefs of Staff has developed specific procedures for the initiation, development, approval, and maintenance of joint doctrine projects. The process requires active involvement by all principal users of joint doctrine. The process also includes a means to work towards consensus among doctrine developers as well as a method for resolving key issues or divergent views.[11]

In the same way that the drafting of the Army Counterinsurgency Field Manual assembled "journalists, human rights advocates, academics, and practitioners of counterinsurgency"[12] – an unusual group to develop an Army doctrine – the development of a national cyber doctrine can encourage horizontal integration of the commercial, government, academic, and civil liberties sectors to enhance the rigor of national security decision making in the cyber domain. It will focus the application of U.S. cyberpower. "Cyberpower" is defined here as "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power."[13]

With the dearth of nonmilitary cyber capacity, the Cyber Command will become the default organization to confront threats affecting the diverse networks on which U.S. defense and the global market rely. Although the command is currently restricted to operations on DoD networks, it is easily foreseeable that the command may be called upon to take action on other networks in times of crisis. With the establishment of the Cyber Command and the prioritization of cybersecurity,[14] national strategy must be effectively communicated and implemented. A doctrine should be in effect before a national crisis occurs so that appropriate constitutional management of U.S. power is maintained. "When strategy is

[11] JOINT CHIEFS OF STAFF, JOINT PUB. 1-01: JOINT DOCTRINE DEVELOPMENT SYSTEM vi (2000), *available at* http://www.bits.de/NRANEU/others/jp-doctrine/jp1-01(00).pdf.

[12] Nagl, *supra* note 10, at xvi.

[13] Daniel T. Keuhl, *From Cyberspace to Cyberpower: Defining the Problem, in* CYBERPOWER AND NATIONAL SECURITY 24, 38 (Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz eds., 2009).

[14] *See generally* OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, THE NATIONAL INTELLIGENCE STRATEGY OF THE UNITED STATES OF AMERICA (2009), *available at* http://www.odni.gov/ reports.htm.

freed from effective political control, it becomes mindless and heedless. . . ."[15]

What was true of nuclear weapons during the Cold War is also true of network attack in the cyber age. Modern technology that

> created the bombs that were dropped on Hiroshima and Nagasaki and the more sophisticated ones that have in the years since 1945 aroused visions of conflict between the superpowers that would end in mutual annihilation, is now, in its restless energy, creating new kinds of weapons that may in time make nuclear war obsolete and recreate the conditions in which the principles of classical strategy were formulated.[16]

Historians Gordon Craig and Felix Gilbert were arguing that point in reference to precision-guided munitions, but cyber war might have a similar potential to make deterrence with nuclear weapons and classic strategic thought obsolete.

Nuclear deterrence during the Cold War contemplated an automated response to attack by the Soviet Union, and similar automated responses to cyber attack are now being debated. Computer network attacks happen at the speed of light, so future threats require an equally rapid and perhaps automatic response. Portals can be programmed to disconnect automatically from the network when known hostile signatures are detected.

The nature of network attacks makes a well reviewed cyber doctrine particularly important, since national security leaders will have little time to consult with the National Security Council or the Commander in Chief when faced with an attack that could devastate the national economy, corrupt the flow of commerce, or disrupt military supply chains. Due to technical challenges, counterstrikes remain a time-consuming proposition. Disruption of a cyber attack is more easily achieved but may not be accomplished in time to protect critical data or national security systems.

The risks in removing human judgment from the network operations decision cycle are significant. For example, in 1988, the automated Aegis computer system on board the *U.S.S. Vincennes* registered Iran Air flight 655 as a hostile Iranian F-14 fighter aircraft.

> Though the hard data were telling the human crew that the plane wasn't a fighter jet, they trusted the computer more. Aegis was in semi-automatic mode, giving it the least amount of autonomy, but

[15] Gordon A. Craig & Felix Gilbert, *Reflections in Strategy in the Present and Future*, *in* MAKERS OF MODERN STRATEGY FROM MACHIAVELLI TO THE NUCLEAR AGE 863, 865 (1986).

[16] *Id.* at 867.

> not one of the 18 sailors and officers in the command crew challenged the computer's wisdom. They authorized it to fire.[17]

This semi-automatic response killed 290 passengers.

Although there are problems associated with attributing the source of cyber attacks, cyber weapons may already be under development. "One can argue plausibly that the autonomy of the political leadership begins to shrink from the moment that it authorizes the expenditure of national resources on this or that kind of weapons research or the production of this or that kind of bomber, missile, or submarine."[18] Some claim that large amounts have already been spent on the research and development of cyber weapons. The current doctrine is inadequate to the task levied on the Cyber Command. Only through a deliberate development process will the risks of applying U.S. cyberpower against cyber threats be mitigated. This process will ensure that the autonomy of U.S. political leadership and the values expressed in the use of U.S. force or influence are maintained.

I. THE CURRENT CYBER DOCTRINE LANDSCAPE

Any employment of U.S. force must be guided by legal and policy determinations. "The President and the national civilian leadership must be sensitive to the legal, political, diplomatic, and economic factors inherent in a decision to further national objectives through the use of force."[19] It is U.S. policy that any application of force must be based on international law "as well as on *domestic* legal authority."[20]

A military doctrine formalizes how the United States conceives of its role in the national security environment and how it acts to accomplish its goals. It codifies how the government should be organized, what tasks it should be prepared to accomplish, and what resources it will need to fulfill its role. When considering the use of cyberpower, the national security community has yet to decide if computer network operations will be directed against human decisionmaking (that is, command and control) or against automated decisionmaking (automated air defense networks).

Joint Publication (JP) 3-13 defines "information operations" (IO) as "the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp

[17] P.W. Singer, *Robots at War: The New Battlefield*, WILSON Q., Winter 2009, at 40, *available at* http://www.wilsoncenter.org/index.cfm?fuseaction=wq.essay&essay_id=4966 13.

[18] Craig & Gilbert, *supra* note 15, at 865.

[19] JUDGE ADVOCATE GENERAL'S LEGAL CENTER AND SCHOOL, OPERATIONAL LAW HANDBOOK 1 (2008).

[20] *Id*. at 1 (emphasis in original); *see generally* War Powers Resolution of 1973, 50 U.S.C. §§1541-1548 (2006).

adversarial human and automated decision making while protecting our own."[21]

In accordance with JP 3-13, information operations – to include CNO – are "primarily concerned with affecting decisions and decision-making processes, while at the same time defending friendly decision-making processes." The mechanisms used to affect these processes are "influence, disruption, corruption, or usurpation."[22] This approach may be consistent with some objectives of power projection, but it unnecessarily constrains U.S. cyberpower advantage by associating it with other activities that target human cognition.

Computer network operations consist of attack, defense, and exploitation, and seek to "disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." Computer network defense seeks to "protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks." Computer network exploitations are "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[23]

These definitions are clear enough, but they are full of deficiencies in the application of the terms. In 2001, the Preventive Defense Project published *Keeping the Edge: Managing Defense for the Future* to provide solutions for "some of the organizational and managerial deficiencies of the national security establishment."[24] This book identified issues with cyber operations that continue to confound the DoD. "The lack of an accepted lexicon has led to much confusion, and the diffusion of responsibility has led to duplication, inefficiency, and increased cost as well as missed opportunity."[25] The recommendation for the national security establishment to develop an information operations strategy and a comprehensive cyber policy was quite prescient, considering the lack of experience and shortage of lessons learned from current cyber operations.

Each of the armed forces dedicates personnel to computer network defense and computer network attack. They employ thousands of personnel to keep their data secure and their "communications networks flowing."[26] The Defense Information Systems Agency oversees the Global Information

[21] JOINT CHIEFS OF STAFF, JOINT PUB. 3-13: INFORMATION OPERATIONS ix (2006), *available at* http://www.fas.org/irp/doddir/dod/jp3_13.pdf.

[22] *Id.* at I-6.

[23] *Id.* at II-5.

[24] PREVENTIVE DEFENSE PROJECT, KEEPING THE EDGE: MANAGING DEFENSE FOR THE FUTURE xi (Ashton B. Carter & John P. White eds., 2001).

[25] *Id.* at 89.

[26] Noah Shachtman, *U.S. Cyber Command: 404 Error, Mission Not (Yet) Found*, WIRED, June 26, 2009, *available at* http://www.wired.com/dangerroom/2009/06/foggy-future-for-militarys-new-cyber-command/.

Grid (GiG) and provides support for net-centric operations through the Joint Task Force-Global Network operations. The GiG is an interconnected set of capabilities that includes any DoD system, equipment, software, or service that transmits, stores, or processes DoD information.[27]

Not only does each of the military services have its own personnel dedicated to cyber operations, but also – despite the lack of a unified U.S. government cyber doctrine – each of the individual armed forces has a disparate information operations doctrine and elements that manage and defend their information networks. In accordance with the doctrine, all of the armed forces view cyber operations as tools to affect the cognitive processes of adversaries. The majority of soldiers, sailors, airmen, and marines continue to see cyber operations only as an element to be governed by their service information operations doctrine. As noted by Director of the National Security Agency Keith Alexander, "the only doctrine that currently addresses operations within the cyberspace environment is contained within two subsets of information operations (IO) computer network operations and electronic warfare (EW)."[28]

The individual armed forces computer network operations doctrines are incomplete. They fail to delineate the fundamental principles by which the services manage their computer network activities in support of national objectives. This lack of appropriate doctrine has not prevented the Departments of the Army, Navy, and Air Force from establishing individual organizations to address cyberspace issues. Similar to the DoD and the Cyber Command, the services have established these organizations without any governing principles.

This lack of a government-wide cyber doctrine creates a potential for inadequate and ineffective responses to cyber threats. The outdated, maladapted doctrine and the various armed forces doctrines create confusion and could compromise highly sensitive attack techniques. The current doctrine lacks adequate interoperability principles to govern a joint cyber force. "In addition, different organizational structures are being implemented within each service to address this rapidly evolving source of both military opportunity and threat vulnerability. Further complicating the issue, "different voices within the individual Services present diverse visions of the role of cyberpower and of the Service's role . . . within that vision."[29] These different voices may generate incompatible directives and result in the services managing their forces in an entirely inadequate and

[27] Clay Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues* 9 (Cong. Res. Serv. RL31787), Mar. 20, 2007.

[28] Keith B. Alexander, *Warfighting in Cyberspace*, JOINT FORCES Q., 3rd Quarter 2007, at 58, 59, *available at* https://digitalndulibrary.ndu.edu/cdm4/document.php?CISOROOT=/ndupress&CISOPTR=15898&REC=4

[29] Elihu Zimet & Charles L. Barry, *Military Services Overview*, *in* CYBERPOWER AND NATIONAL SECURITY, *supra* note 13, at 285, 299.

incompatible manner. In a time of shrinking budgets and growing threats, cyber coordination must improve within the national security sector.

Without a properly coordinated doctrine, the Cyber Command's capabilities might first be tested during an actual national emergency. Such a crisis may highlight the inadequacy of the command's organizational structure, gaps in its roles and missions, or insufficient intelligence authorities. Critical elements, "such as intelligence, logistics, airspace control, space operations, etc.," have yet to be addressed in any joint authoritative directives.[30] All DoD elements must acknowledge the realities of an environment that provides a powerful advantage but also presents significant vulnerabilities.

First, the U.S. Army's way of conducting combat must adapt to a digital battlefield. It is a well known axiom that the way the Army fights the next war depends on how it prepares to fight in the intervening years. As has been noted, "Peacetime military thought focuses on what the army thinks about past wars, how it interprets current threats of war, and how it anticipates future wars."[31] The Army must assess its martial traditions and lessons from current conflicts in order to seize all opportunities. The world's preeminent ground combat force has yet to fully acknowledge the changing nature of conflict and advantages of network operations.

Notwithstanding this institutional inertia, in the summer of 2008 the Army established the Army Network Warfare Battalion at Fort Meade, Maryland. The battalion's mission is to support the Army and the DoD in "a variety of tasks, ranging from tactical support to Brigade Combat Teams in Iraq through strategic support to the other services, joint commanders, and interagency partners as required."[32] According to the commander of the battalion's parent organization – the Intelligence and Security Command – "In the space of 15 years, networked information systems have become essential to organized human activity across much of the globe. These systems are integral to telecommunications, banking and finance, transportation and energy distribution, human services, government, and all levels of military operations." This new battalion centralizes current Army computer network operations into a single battalion in order to make more efficient use of its resources. "This unit will serve as core for Army network warfare activities that will expand and gain capacity in the coming years."[33]

[30] David A. Sawyer, *The Joint Doctrine Development System*, JOINT FORCE Q., Winter 1996-1997, at 36, 37, *available at* http://www.dtic.mil/doctrine/jel/jfq_pubs/develop.pdf

[31] BRIAN MCALLISTER LINN, THE ECHO OF BATTLE: THE ARMY'S WAY OF WAR 9 (2007).

[32] Army Activates Network Warfare Unit (July 2, 2008), *available at* http://www.army.mil/-newsreleases/2008/07/02/10569-army-activates-network-warfare-unit/.

[33] *Id.*

Army Field Manual 3-13 *Information Operations: Doctrine, Tactics, Techniques, and Procedures* addresses computer network operations in the same way that the inadequate Joint Staff doctrine does: as a subset of information operations. This approach conceives of a network as a weapon or a tool for cognitive influence, rather than as a domain in and through which power may be projected:

> Information superiority *creates conditions* that allow commanders *to shape the operational environment* and *enhance the effects of all elements of combat power*. [Information operations (IO)] has two categories, offensive IO and defensive IO. Commanders conduct IO by synchronizing IO elements and related activities, each of which may be used either offensively or defensively. Army IO doctrine supports joint IO doctrine, supplementing it where necessary to meet the conditions of land operations.[34]

This text from the Army Field Manual distinguishes information operations – and by definition computer network operations – from combat power. The Manual defines "network operations" as an enhancement of combat power, not as an essential modern element. Given the capabilities of today's networks, this approach is inadequate.

The U.S. Navy has a long history of using cryptology and network operations. The Navy should formalize the lessons learned over decades of successful cryptologic operations. In 2002, the Navy combined multiple commands – including Naval Space Command, Naval Computer and Telecommunications Command, Fleet Information Warfare Center, and Navy Component Task Force-Computer Network Defense – to form the Naval Network Warfare Command (NETWARCOM) to focus on enabling access to foreign information networks and defending the Navy's networks from penetration.[35] NETWARCOM is assigned to generating fleet and joint warfighters' readiness, providing decision makers with superior information to gain advantage over adversaries, developing a workforce to meet current and future requirements, and providing capabilities.[36]

NETWARCOM's strategic plan mandates the development of a CNO strategy, with action plans to achieve freedom of maneuver in cyberspace.[37] This strategy should be developed concurrently with or derived from the new national cyber doctrine necessary for the focused application of national cyberpower.

[34] U.S. ARMY, ARMY FIELD MANUAL 3-13: INFORMATION OPERATIONS 1-1 (2003) (emphasis added).

[35] U.S. Navy, Naval Network Warfare Command, NETWARCOM – Our History, *available at* http://www.netwarcom.navy.mil/about-us/history.htm.

[36] NAVAL NETWORK WARFARE COMMAND, NAVY NETWARCOM STRATEGIC PLAN 2009-2013: A FRAMEWORK FOR DECISION-MAKING 6 (2009), *available at* http://www.netwarcom.navy.mil/about-us/StrategicPlan.pdf.

[37] *Id.* at 12.

Complicating the task of drafting a naval network operations strategy and action plan is the order from the Chief of Naval Operations to merge the intelligence and communications network elements of the Navy staff. This merger is intended to facilitate the establishment of a Fleet Cyber Command to provide a maritime component force to the Cyber Command. The memorandum of the Chief of Naval Operations directing the merger implies that a new naval cyber doctrine may ultimately have to be developed: "the [reorganization] team shall also identify governance mechanisms across the Navy to optimally align and manage Navy's information capabilities."[38]

This reorganization may bode well for the Navy staff, but the Navy IO doctrine, in contrast, remains insufficient. It does not adequately describe the Navy's role in the protection of its networks or offensive cyber operations. The establishment of the Fleet Cyber Command will not resolve the problems presented by a lack of national cyber doctrine. Without the doctrinal star to guide the Navy's Cyber Fleet, it will lack purpose and direction. The Navy may have the advantage of worldwide access and a tradition of network operations, but it cannot realize its full potential without the strategic direction that a national cyber doctrine would provide. The Navy needs to define its role in cyberspace.

Within the Department of the Navy, the Marine Corps has chosen not to establish an organization dedicated to network operations. The Marines, rather, focus on the war fighting elements of IO, such as signals intelligence and electronic warfare. Their IO doctrine does provide adequate guidance for these functional tasks.

Marine Corps War-fighting Publications (MCWPs) contain the tactics, techniques, and procedures utilized by the Marine Corps in the prosecution of their assigned mission. MCWP 2-1 *Intelligence* discusses IOs and their intelligence support requirements, but it does not address how expeditionary forces may capitalize on cyberpower to succeed in their missions. "The Marine Corps has focused its cyberpower vision on network-centric operations and warfare (NCOW) and is developing a Marine Air-Ground Task Force Information Operations (MAGTF-IO) strategy for operational implementation."[39] Just as the Army must adapt to the new techniques of ground combat, so too must the Marines. They would be wise to create a partnership with the Army in the development of their new cyber doctrine, similar to the way all the armed units collaborated in 2007 to develop the counterinsurgency doctrine.

Like the Navy, the U.S. Air Force has made some efforts to adjust its structures and organization to provide a dedicated cyber force. After an

[38] Memorandum from the Chief of Naval Operations to the Director of Naval Intelligence (N2), Reorganization of the Office of the Chief of Naval Operations (OPNAV) Staff (June 26, 2009), *available at* http://therealnavy.com/IWOInterestItems.aspx.

[39] Zimet & Barry, *supra* note 29, at 304.

initial attempt in July 2008, the Air Force established a provisional cyberspace command under the Air Force Space Command. According to the Air Force Cyberspace Command, the provisional 24th Air Force is supposed to enhance global reach, power, and vigilance with war fighting cyberspace forces and integrate the Air Force's global capabilities in support of the combatant commander through the full range of military operations. The Command is required to align "Air Force train and equip organizations the way best suited to prepare for and, in some cases conduct, war-fighting operations (for example, defense of cyberspace)."[40]

The 24th Air Force, like the Army Network Warfare Battalion, was established without any appropriate doctrine to direct how the Air Force will protect its own networks and conduct operations in and through cyberspace. A useful Air Force cyber doctrine would delineate how the 24th Air Force will interact with other interagency elements such as DoD's Cyber Command, the National Security Agency, and the Department of Homeland Security.

The Air Force cyber doctrine should describe network architectures for which the Air Force is responsible. Air Force Doctrine Document 2-5 describes network warfare as the "the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the interconnected analog and digital network portion of the battlespace."[41] The doctrine wisely includes radio networks, "satellite links, tactical digital information links, telemetry, digital track files, telecommunications, and wireless communications networks and systems" as examples of networks subject to exploitation and attack.

The Air Force doctrine does not adequately address computer network operations, but it does encourage an effects-based approach to information operations. This approach suggests that computer network operations should continue to be directed toward human decision making. Unfortunately, the document uses a strategic, operational, and tactical framework for its effects-based approach, and these levels of war may prove to be just as irrelevant in cyberwarfare as they are becoming in traditional warfare. At best, it would give policy makers a false sense of intellectual security when considering the proportionality or collateral effects of national security decisions with cyber operations elements.

The relevant and useful elements of the current armed forces information operations manual should be preserved in a new national cyber doctrine. The first priority, however, should be to assemble an inclusive group of cyber stakeholders – including each of the armed forces – to

[40] *See generally* Paul Berg, *Air Force Cyber Command: What Will It Do and Why We Need It*, *available at* http://www.au.af.mil/au/cadre/aspj/apjinternational/apj-s/2007/1tri07/bergeng.html.

[41] U.S. AIR FORCE, AIR FORCE DOCTRINE DOCUMENT 2.5 5 (2005), *available at* http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_5.pdf.

debate and develop a national cyber doctrine applicable to the entire national security community.

A new cyber doctrine, developed under a sound national security strategy, will enable the DoD and non-DoD institutions to tailor their cyber activities and manage their capabilities in cyberspace. "[P]rotection against cyber attack through cyberspace is a new task for the military," and the U.S. military resists adjustment to new combat realities. The advantages of a novel cyber doctrine may motivate the defense establishment – and the entire national security community – to embrace cyberpower as the next critical element with which to protect U.S. interests.

II. ADVANTAGES OF A NEW DOCTRINE

A new doctrine that treats cyberspace as an essential war fighting domain will enable the capabilities of each of the armed forces to be better directed, managed, and trained. For example, each branch of the armed service has training programs to provide computer network personnel to the combatant commands and national agencies. A national cyber doctrine could help to focus this training in areas such as network architecture design, in-depth network defense, and weaponization of network devices.

Some argue that none of the services is qualified to produce or manage a cyber force. The cultures of the "Army, Navy, and Air Force are fundamentally incompatible with that of cyberwarfare."[42] The service elements that manage cyber activities are "ill-fitting appendages that attempt to operate in inhospitable cultures where technical expertise is not recognized, cultivated, or completely understood."[43] A national cyber doctrine can bring discipline to these training efforts and begin to build a skilled cyber cadre across the national security community. Under the current construct, however, "information warfare in the form of computer network attack has a long way to go before it is fully fit for the front."[44]

To create a mature network operation that is "fit for the front" requires a doctrine applicable to all elements of the national security community. The doctrine must acknowledge that the DoD may not be the only institution exercising U.S. cyberpower. Just as Army Field Manual 3-07 acknowledges the roles of the U.S. Department of State, U.S. Agency for International Development, and U.S. Department of the Treasury in stability operations, so the new national cyber doctrine should acknowledge the roles of non-DoD organizations, including the private sector.

[42] Gregory Conti & John Surdu, *Army, Navy, Air Force, and Cyber – Is It Time for a Cyberwarfare Branch of Military?* 12-1 IA NEWSLETTER 15 (Spring 2009), a*vailable at* http://iac.dtic.mil/iatac/download/Vol12No1.pdf .

[43] *Id.*

[44] MARTIN C. LIBICKI, CONQUEST IN CYBERSPACE: NATIONAL SECURITY AND INFORMATION WARFARE 100 (2007).

Today's military and intelligence communities rely on commercial networks, but the nodes, access points, and traffic are controlled by the DoD. For example, the Secret Internet Protocol Router Network and the Secure Telephone Units are examples of information system partnership between the military and commercial networks.[45] Public-private partnerships are necessary to protect and make effective use of U.S. cyberpower. The entire national security sector, including military, government, and commercial network providers, must learn to collaborate in the same way that our cyber adversaries do.

There is currently no guidance for the national security sector to resolve conflicts or encourage collaboration between the government and the private sector when faced with network defense or attack. If a cyber attack occurred today, there is little that the DoD could do if the attack came across a commercial network. A national cyber doctrine can help the relevant organizations to resolve conflicts concerning the protection of critical domestic infrastructure when the networks to be protected by the Cyber Command belong to a commercial entity.

Potential conflicts arising from U.S. government activities on commercial networks can be mitigated by assembling a cyber task force to develop a national cyber doctrine that includes network service providers.. Specifically, by engaging in such a process, commercial providers can address their concerns and develop solutions to allow a U.S. government organization, such as the Cyber Command, to operate on their networks.

A cyber doctrine task force can draw on established DoD procedures for doctrine development. During the analysis phase, "all relevant sources [of information] have been explored, including international agreements, lessons learned, extant and emerging joint, multinational, and Service doctrine and procedures, interviews [with stakeholders], meetings, and working groups; and other sources as appropriate."[46] There are procedures for addressing and voting on doctrine proposals, debating key issues, and maintaining awareness of interagency perspectives and positions. Recommendations that receive a majority vote of the attending permanent members of the cyber task force will become part of the national cyber doctrine. In this way, the doctrine development process can be used to help resolve conflicts not by authority, but by consensus – much like the way that the Internet has developed.

Any cyber doctrine developed in this inclusive manner can apply to all organizations within the U.S. government. Much like the development of the counterinsurgency doctrine drove policy in Iraq, a new national cyber doctrine can drive policies concerning cyberpower in areas such as civil liberties and public-private partnerships. If collaborative mechanisms are developed and tested as part of the development of a national cyber doctrine, this work can serve as the foundation of new regulations and

[45] Zimet & Barry, *supra* note 29, at 287.

[46] JOINT CHIEFS OF STAFF, *supra* note 11, at III-3.

statutes to govern cybersecurity. In this way, theoretical models can be tested before they get enacted into law.

A recent workshop report issued jointly by the American Bar Association Standing Committee on Law and National Security and the National Strategy Forum recognized the importance of developing a national cyber doctrine. The report noted that the U.S. government most often looks to law enforcement to address illicit cyber activity. "But the truth is that applying the criminal law is of limited utility."[47] Knowledgeable cyber criminals, terrorists, and foreign operatives are difficult to identify using traditional law enforcement methodologies. The report continues:

> Moreover, the organic method of developing doctrine through executive consideration seems to be the only one available at the moment. Given the complexity of this area of law and the practical challenge of finding political will to motivate Congress to legislate on this issue, this is unlikely to change in the near future.
>
> To the extent possible, discussions about cyberlaw, doctrine, and policy should not be classified. While in some instances the disclosure of doctrine may be impossible (lest sources and methods be disclosed), for the most part the public revelation of our response doctrine will be to our benefit. Doing so will create international norms for behavior and then, collaterally, attach a stigma to those who fail to conform. Moreover, a robust doctrine can serve as a deterrent.[48]

The current process by which military doctrine is conceived, drafted, and reviewed provides the mechanism to develop a common understanding of computer network operations.[49] Those experienced with classified networks in the U.S. government might well agree that there is a need to incorporate best practices for the protection of the DoD's top-level domain "mil" networks, the Non-Secure Internet Protocol Router Network, and Secret Internet Protocol Router Network is needed. Although much is known about network protection techniques, the national security apparatus needs a fresh set of principles to formalize the best network security approaches for more agility and faster dissemination of security protocols and virus signatures.[50]

[47] *National Security Threats in Cyberspace*, report of a *Workshop Jointly Conducted by the ABA Standing Committee on Law and National Security and National Strategy Forum* 18 (Sept. 2009), *available at* http://www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf.

[48] *Id.* at 19.

[49] *See generally* Alexander, *supra* note 28.

[50] Antivirus programs search incoming data for known virus patterns called virus signatures. A signature is a characteristic byte pattern that is part of a certain virus or family

A new cyber doctrine will provide guidance on the application of cyberpower in response to a physical attack or as part of a computer network attack initiated by the U.S. government. Under the existing doctrine, a computer network attack "is not integrated with overall [warfare] planning because of the highly compartmented classification that cyber activities receive."[51] A major objective of assembling an interagency team to establish a national cyber doctrine is to improve the integration of cyber defense and offense into joint interagency operational planning. Operations in cyberspace must be "synchronized and coordinated with other operations, just as land and air operations . . . must be synchronized and coordinated."[52] With their current classification, network attack capabilities are misunderstood and not widely employed.

A national cyber doctrine should be unclassified to the maximum extent possible. As with other doctrines, a classified annex may be necessary to delineate sensitive capabilities, operations, or relationships. While it is foolish to disclose all the elements of U.S. cyberpower, the foundational principles that govern the applications of cyberpower should be widely disseminated. The development of this doctrine would de-mystify the domain for the national security community and the American people. Federal agencies should participate in the debate to establish this doctrine and help institutionalize its principles across the entire government. This debate can inform the decision on what information must remain classified and what does not need to be classified.

Although the doctrine should include as much unclassified detail as possible, the national cyber doctrine may require a classified annex to document U.S. offensive computer network capabilities. Other unclassified doctrines do not disclose specifications of weapons systems but do include a classified annex for a variety of purposes. Cyber weapons should be viewed as having little distinction from traditional weapons or techniques available to the U.S. Government. "Cyber weapons simply provide the operational planner with another option, in addition to the air-delivered, laser-guided bomb and the Special Operations force with demolition charges."[53] Given the nature of cyberwarfare, it is more important that details of specific weapons or techniques remain classified. As noted in a recent study, "As a general rule, [computer network] tricks exhaust themselves to the extent . . . that their existence and thus the need to protect

of viruses. *See generally* DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY (1999).

[51] Franklin D. Kramer, *Cyberpower and National Security: Policy Recommendations for a Strategic Framework, in* CYBERPOWER AND NATIONAL SECURITY, *supra* note 13, at 3, 14.

[52] NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 163 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009).

[53] *Id.*

against their recurrence is obvious and . . . that counters to their recurrence are straightforward to implement."[54]

This issue of overclassification must be addressed if U.S. national security organizations are to benefit from cyberpower. According to Andrew Krepinevich, the "cyberwarfare competition is so shrouded in secrecy that it is difficult to determine the United States' level of vulnerability, let alone options for addressing it."[55] The development of a national cyber doctrine would clarify the nation's capabilities to those who are responsible for projecting U.S. power. The highly classified nature of computer network operations capabilities has prevented computer networks from being fully integrated into traditional war fighting exercises conducted by combatant commands. "[A]n unclassified and authoritative statement of current joint doctrine for the use of computer network attack is unavailable" and is still evolving.[56]

The national security sector needs to debate cyberpower publicly, rather than just hold classified conversations.[57] An open debate about the application of power and the circumstances that warrant a doctrinal response would clarify and further develop the general understanding of not only the capabilities but also the limitations of network operations.

According to General James E. Cartwright, the Vice Chairman of the Joint Chiefs of Staff, "the integration of cyberspace capabilities across the full-range of military operations" is fundamental to assuring U.S. freedom of action in cyberspace.[58] Strategy, policy, and doctrine on the use of other instruments, such as nuclear weapons, are publicly debated even while the exact capabilities and technical details of the weapons themselves remained secret.[59] Similar to these discussions, the various perspectives concerning cyber weapons, techniques, and capabilities can be reviewed and validated by knowledgeable representatives from a cyber community of interest from across the national security community.[60] If properly structured, the interagency group will include representatives from the intelligence community to provide expertise on the proper classification of sections of the cyber doctrine.

In addition to classification, another issue that can be resolved through interagency development of a national cyber doctrine is the interaction between the U.S. government and the private companies that operate

[54] MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 57 (2009).

[55] Andrew F. Krepinevich, Jr., *The Pentagon's Wasting Assets*, FOREIGN AFFAIRS, July/Aug. 2009, at 30-31.

[56] NATIONAL RESEARCH COUNCIL, *supra* note 52, at 161-162.

[57] Shaun Waterman, *U.S. Takes Aim at Cyberwarfare: Data Sharing, Defense Against Unknown Attackers Among Issues*, WASH. TIMES, July 2, 2009, at B1.

[58] *Id.*

[59] Shaun Waterman, *Analysis: New Army Cyber Task Force*, Oct. 27, 2008, *available at* http://www.spacewar.com/reports/Analysis_New_Army_cyber_task_force_ 999.html.

[60] *See generally* JOINT CHIEFS OF STAFF, *supra* note 11, at II-8.

commercial networks over which DoD data flow. Because the vast majority of U.S. commerce is conducted through the Internet, the DoD acknowledges that the DoD must have the capability to protect it. The DoD already relies on private and academic institutions to "assist commercially owned telecommunications networks, communications satellite systems, and other civilian critical infrastructure systems" through the Computer Emergency Response Team.[61]

The initiation of the doctrine development process within the national security community will force the U.S. government to establish roles and delineate responsibilities for the public and private sector concerning network defense and the use of private networks for offensive operations and intelligence collections. Without a structured forum to debate the concerns over government action on commercial information systems, national security organizations are forced to continue their individual *ad hoc* solutions that may not hold up in times of crisis. Commercial entities may not cooperate when the U.S. Government requests authority to control portions of their network during national emergencies or during a computer network attack by a foreign force. Jurisdictional arguments or debates about statutory interpretation should not delay national defense during times of national emergencies.

New statutes and regulations may be required. Existing partnerships between the federal government and commercial entities, such as the Federal Aviation Administration, the National Oceanographic and Atmospheric Administration, and the National Institute for Standards and Technology have not presented the same concerns as those raised by government activities in commercial cyberspace. Concerns over privacy, network service availability, criminal and civil liability risks, and intellectual property protections make government cyber operations a sensitive topic. New regulations governing U.S. cyberpower must be debated before becoming law.[62]

Determining the responsibilities of the national security community during cyber emergencies is a broad task. Just as the term "national security" is too broad to be discussed in adequate detail, cybersecurity is too broad to be covered without further delineation of how the U.S. government plans to establish the roles of the private and public sectors to implement policy. The Joint Doctrine Development System requires that any new proposal include recommended chapters to be covered by the new document.[63] Issues such as government interactions with private information networks, overclassification, foreign relationships in the cyber domain, and others must be addressed in a clear and concise manner in the chapters of the new doctrine. The doctrine must translate current national

[61] Wilson, *supra* note 27, at 10.

[62] *See generally National Security Threats in Cyberspace, supra* note 47, at 12-19.

[63] *See generally* JOINT CHIEFS OF STAFF, *supra* note 11.

cyber strategies into objectives and desired effects to be achieved by the Cyber Command and the other elements of the U.S. government.

The new doctrine must include a definitions and descriptions chapter so that U.S. cyberspace actors have common terms of reference. The chapter should describe various networks, the access these networks provide to various traditional and non-traditional military targets, and the combat effects network operations can achieve. It should also describe – in as much detail as proper classification will allow – the nature of cyber operations and the current governance of each activity. The doctrine may include a classified annex to describe the more sensitive elements of U.S. cyberpower.

Another critical chapter should discuss intelligence support. The chapter should describe the various military and government organizations that provide data on networks and adversary network architecture and management. It should include guidance on how best to work with combat support agencies, service intelligence centers, and the defense intelligence enterprise to achieve the desired effect, including cyber tactics, techniques, and procedures. Some information may have to be documented in a classified annex, but the representatives to the development process must resist the temptation to overclassify the majority of cyber capabilities.

The new doctrine must include a chapter on the interagency relationships and the network advantages that each organization offers. In the memo establishing the new Cyber Command, Secretary Robert Gates called for a plan that would "delineate [its] mission, roles and responsibilities" and its "command and control, reporting and support relationships with combatant commands, [military] services and U.S. government department and agencies."[64]

These relationships are critical because there are myriad sets of authorities within the U.S. government.[65] Each organization brings its own authority to conduct cyber operations, and the relationships between the military, the non-DoD cyber elements, and the private sector must be well understood.

These linkages are so significant that any new doctrine should include a chapter dedicated to identifying the DoD and non-DoD elements that defend the national cyber infrastructure. This section of the new doctrine should outline the fundamental principles by which the U.S. government, particularly the DoD, interact with commercial service providers to educate

[64] Waterman, *supra* note 57.

[65] The authorities of the defense and intelligence agencies are established by the National Security Act of 1947, as amended, codified beginning at 50 U.S.C §401. Intelligence activities are extensively regulated by the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12,333, as amended, *United States Intelligence Activities*. *See generally* 50 U.S.C §§401, 413-414; 50 U.S.C. §§1801-1871 (2006), *as amended by* Pub. L. No. 110-261, 122 Stat. 2436 (2008), and other measures; Exec. Order No. 12,333, 46 Fed Reg. 59,941 (Dec. 4, 1981); Exec. Order No.12, 139, 3 C.F.R. 398 (1979).

each other. The risks and vulnerabilities accompanying the government's increased dependence on military and civilian networks "need careful assessment to be effectively managed."[66] According to an independent policy institute:

> U.S. military operations are very dependent on commercial land-based information infrastructure. If cyber attacks inflicted substantial damage commercial networks or corrupted the data on those networks, not only would great economic turmoil ensue; much of the military capability of the United States could prove to be the modern equivalent of the Maginot Line.[67]

In other words, all the investment in cyberpower may be moot.

Another chapter should cover planning and coordination, including standards for the commander's objectives, target development, weaponeering assessment, force execution, and battle damage assessments. This chapter should provide the means by which national policy and civilian control are translated into boundaries of action and the use of force is managed in accordance with U.S. national security.

A chapter on multilateral coordination should describe how the DoD envisions working with foreign governments to defend common networks and gateways. The deployment of various combined enterprise regional information exchange systems provides common standards but prevents unauthorized information exchange based on information sharing agreements with foreign partners.[68] Although these non-interconnected networks provide adequate data sharing among coalition partners, common network security standards will require more sophisticated information sharing agreements and technology.

Any doctrine that describes how the U.S. government will employ cyberpower must also describe how international partners will contribute. This chapter would enable closer relationships with our foreign partners in both computer network exploitation and attack.

The final chapter of a new joint cyber doctrine should guide the training and professionalization of an interagency cyberforce. Acquisition of the technical expertise required for an advanced cyberforce – and the knowledge and experience to understand how it is to be applied – requires extensive training in both technical and policy disciplines.[69] The new doctrine's mandate for manpower allocations would enable the armed services and the civilian agencies to invest in such training.

[66] Zimet & Barry, *supra* note 29, at 285.

[67] Krepinevich, *supra* note 55, at 25 (referring to the Center for Strategic and Budgetary Assessments).

[68] Zimet & Barry, *supra* note 29, at 287.

[69] *See generally* Victor A. DeMarines, *Exploiting the Internet Revolution*, *in* KEEPING THE EDGE: MANAGING DEFENSE FOR THE FUTURE, *supra* note 24, at 98.

III. TARGET AUDIENCE

Because a joint doctrine "is authoritative and applies to joint force operations or when significant forces of one Service support forces of another Service,"[70] the new doctrine will inform the organizational structure, the lines of operation, and the manning of the new Cyber Command. If the doctrine is properly developed by all elements of the national security community, then non-DoD elements may use it to inform their organizational structures, functions, and staffing as well.

The emerging discipline of network operations is a highly technical arena that few civilian or military leaders over the age of 30 adequately understand. The highly classified nature of cyber operations has prevented candid discussion about the consequences or effects of operations. The new doctrine will enable the entire U.S. government to grasp the power and the dangers of actions on the global grid. As interest in cyber operations grows and skills of non-DoD agencies are developed, government reliance on the national cyber doctrine will increase.

The authorities of the Cyber Command, a sub-unified command, have not been determined. Although the U.S. Strategic Command retains authority for computer network operations, JP3-13 allows other commands to execute cyber operations. As the Secretary of Defense or STRATCOM delegates cyber authority, the Cyber Command may become less the launcher of cyber weapons and more the developer or overseer of network exploitation and attack. Joint publication 3-13, *Information Operations*, already permits cyber operations by other combatant commanders:

> [Commander, U.S. Strategic Command's] specific authority and responsibility to coordinate [information operations] across [areas of operation] and functional boundaries do not diminish the imperative for the other combatant commanders to coordinate, integrate, plan, execute, and employ [information operations]. These efforts may be directed at achieving national or military objectives incorporated in [Theater Security Cooperation Programs], shaping the operational environment for potential employment during periods of heightened tension, or in support of specific military operations.[71]

The common understanding is that the Cyber Command will have the lead for all uses of military force in cyberspace. As cyberpower becomes better known and understood, all the combatant commands or other elements of the U.S. government may be called on to conduct operations either individually or as part of a unified effort under the authority of the DoD or military computer networks.

[70] JOINT CHIEFS OF STAFF, *supra* note 11, at v.

[71] JOINT CHIEFS OF STAFF, *supra* note 21, at iv-2.

Because the armed forces provide the personnel and organizational units to the combatant commands, each of them is responsible for executing the mission within the combatant commands. Cyber doctrine will focus efforts to better utilize the personnel, training, and tools within the cyber arsenal. The new doctrine will help determine the size of the cyber forces for each service and the funding to be directed to cyber capabilities.

Other elements of the national security apparatus depend on the intelligence community to define threats to U.S. interests and to guide the appropriate response to those threats. According to JP 3-13:

> Through the intelligence directorate of a joint staff (J-2), [information operations] planners and supporting joint organizations have access to intelligence from the national and combatant command-level intelligence producers and collectors. At the combatant command level, the theater joint intelligence center supports [information operations] planning and execution and provides support to [joint Task Forces] through established joint intelligence support elements. In multinational operations, when appropriate, the J-2 should share information and assessments with allies and coalition partners.[72]

All cyber operations require multi-disciplined intelligence, much of which will be beyond the reach of the defense intelligence enterprise and the intelligence agencies. The new security environment may require data previously excluded from intelligence collection to be provided by government agencies outside of the intelligence community and the private sector. Such is the nature of a networking world. A national cyber doctrine must be developed by a group that includes the intelligence community and other organizations with broader insights into cyberspace. This doctrine development process will improve collaboration among intelligence community organizations, nontraditional government partners, and the private sector.

In the development of doctrine, foreign partners are almost as important as the intelligence community in offering particular knowledge, expertise, and intelligence capabilities. It is unlikely that any future crisis will be met solely by the United States. Foreign countries and the United States are together on battlefield of Iraq and Afghanistan, and they will be in cyber space as well.

Joint Publication 3-13 states:

> Allies and coalition partners recognize various [information operations] concepts and some have thorough and sophisticated doctrine, procedures, and capabilities for planning and conducting IO. The multinational force commander (MNFC) is responsible to resolve potential conflicts between each nation's IO programs and

[72] *Id*. at III-5.

> the IO objectives and programs of the multinational force. . . . It is vital to integrate allies and coalition partners into IO planning as early as possible so that an integrated and achievable IO strategy can be developed early in the planning process.[73]

Foreign partners are critical to the success of U.S. military operations in all the domains. A new cyber doctrine will clarify the U.S. policy in cyberspace for all allies.

IV. OTHER CONSIDERATIONS

The most significant policy issues facing any cyberpower projection is the applicability of the Law of War (LOW). The legal questions must be examined and resolved in detail.[74] The relationship between the laws of war and cyber operations will evolve, but a baseline policy position must involve the entire U.S. government.

Scrutiny should focus on the definitions of "armed attack," as well as "distinction" and "proportionality" as applied to cyber operations.[75] The U.N. Charter provides guidance for responses to armed attacks. The proper classification of cyber activity as an armed attack is much more difficult than the drafters of the U.N. Charter ever envisioned. These issues are ripe for debate and could be addressed in drafting the guiding principles for a national cyber doctrine.

There is a presumption that the rules of engagement in cyber doctrine "will follow the [L]aw of Armed Conflict, meaning a response taken after receiving an electronic or cyber attack will be scaled in proportion to the attack received, and distinctions will be maintained between combatants and civilians."[76] This presumption may be significant because adversaries using cyber attacks may not distinguish between civilian and military targets. "Security experts warn that all U.S. federal agencies should now be aware that in cyberspace some malicious actors consider that no boundaries exist between military and civilian targets."[77]

The law frequently lags behind technology, but the consequences of adversarial actions against the United States and the responses of the Cyber Command illustrate the importance of establishing legitimate legal bases

[73] *Id.* at VI-1.

[74] For detailed discussion of legal questions raised by cyber operations, see Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SECURITY L. & POL'Y 63 (2010).

[75] Regarding the question of when cyber attack may be considered an "armed attack" under the LOW, see David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87 (2010).

[76] Wilson, *supra* note 27, at 11.

[77] Clay Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* (Cong. Res. Serv. RL 32114), Jan. 29, 2008, at 15.

for defensive and offensive cyber operations. "The potentially nonlethal nature of cyber weapons may cloud the assessment of an attack's legality, leading to more frequent violations of the principle of distinction in this new form of warfare than in conventional warfare."[78]

For these reasons, legal experts in the national security sector must engage in the development of the new cyber doctrine. Now is the time for the United States to demonstrate its leadership in establishing the proper doctrine for a governmental approach in accordance with the civil and military principles that have led to U.S. freedom of action.

CONCLUSION

The U.S. Cyber Command was established to defend DoD networks against cyber attacks and to develop offensive cyber capabilities. The creation of this command is a legitimate response to the growing capabilities of nations such as China and Russia as well as non-state actors such as al Qaeda and Hamas. The command was established without an adequate cyber doctrine to guide the application of joint forces in protecting U.S. freedom of action in cyberspace. Only by adopting a comprehensive government approach can the United States bring its full intellectual might to bear on the challenging domain of cyberspace.

The joint doctrine development process will allow interagency elements to resolve many issues that currently complicate the U.S. approach to cyberpower. The joint doctrine must distinguish computer network operations from their current framework and embrace cyberspace as a war fighting domain. The process will allow debate and resolution of issues such as the training required for a cyber force, the proper classification of U.S. cyber capabilities, the authorities under which computer network attacks may be executed, and actions in cyberspace that implicate the laws of war. This new doctrine will enhance U.S. national security by normalizing cyberspace as a domain through which the United States can express national values and protect national interests.

[78] Jeffrey T.G. Kelsey, *Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, MICH. L. REV. 1427, 1446-1447 (2008).