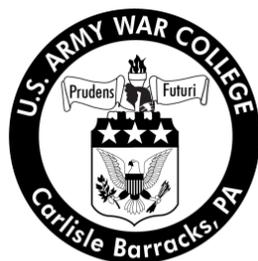


United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?

by

Lieutenant Colonel John W. Brennan
United States Army



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 Senior Service College Fellowship. 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.

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.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YYYY) 15-03-2012		2. REPORT TYPE Civilian Research Paper		3. DATES COVERED (From - To) 19 Aug 11- 15 May 12	
4. TITLE AND SUBTITLE United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) LTC John W. Brennan				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Triangle Institute for Security Studies (Duke University, UNC, NCSU)				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					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT Ten years after the tragedy of 9-11, al-Qa'ida and other international terrorist organizations continue to threaten the United States and its allies through their ever-expanding cyber capabilities. It is clear that numerous national-level civilian and military leaders have duly recognized these menacing terrorist threats--and many officials have also likewise lamented the lack of authority provided them to effectively counter terrorists from within cyberspace. The incongruence between national CT cyber policy, law, and strategy degrades the abilities of federal CT professionals to interdict transnational terrorists from within cyberspace. Specifically, national CT cyber policies that are not completely sourced in domestic or international law, unnecessarily limit the latitude cyber CT professionals need to effectively counter terrorists through the use of organic cyber capabilities. In order to optimize national CT assets and to stymie the growing threat posed by terrorists' ever-expanding use of cyberspace, national decision-makers should potentially modify current policies in order to efficiently execute national CT strategies--albeit within the framework of existing CT cyber-related statutes.					
15. SUBJECT TERMS United States Code, Patriot Act, Counter Terrorism					
16. SECURITY CLASSIFICATION OF: Unclassified			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 34	19a. NAME OF RESPONSIBLE PERSON LTC John W. Brennan
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (include area code) (910) 783-6342

USAWC CIVILIAN RESEARCH PROJECT

**UNITED STATES COUNTER TERRORISM CYBER LAW AND POLICY, ENABLING
OR DISABLING?**

by

Lieutenant Colonel John W. Brennan
United States Army

Professor Charles Dunlap
Project Adviser

This CRP is submitted in partial fulfillment of the requirements of the Senior Service College Fellowship Program

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 John W. Brennan

TITLE: United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?

FORMAT: Civilian Research Project

DATE: 15 March 2012 **WORD COUNT:** 5,809 **PAGES:** 30

KEY TERMS: United States Code, Patriot Act, Counter Terrorism

CLASSIFICATION: Unclassified

Ten years after the tragedy of 9-11, al-Qa'ida and other international terrorist organizations continue to threaten the United States and its allies through their ever-expanding cyber capabilities. It is clear that numerous national-level civilian and military leaders have duly recognized these menacing terrorist threats--and many officials have also likewise lamented the lack of authority provided them to effectively counter terrorists from within cyberspace.

The incongruence between national CT cyber policy, law, and strategy degrades the abilities of federal CT professionals to interdict transnational terrorists from within cyberspace. Specifically, national CT cyber policies that are not completely sourced in domestic or international law, unnecessarily limit the latitude cyber CT professionals need to effectively counter terrorists through the use of organic cyber capabilities.

In order to optimize national CT assets and to stymie the growing threat posed by terrorists' ever-expanding use of cyberspace, national decision-makers should potentially modify current policies in order to efficiently execute national CT strategies--albeit within the framework of existing CT cyber-related statutes.

UNITED STATES COUNTER TERRORISM CYBER LAW AND POLICY, ENABLING OR DISABLING?

“Mass media and the Internet in particular have emerged as enablers for terrorist planning, facilitation, and communication, and we will continue to counter terrorists’ ability to exploit them.”¹

--The National Strategy for Counterterrorism
June 2011

As Al-Qa’ida and its affiliates and adherents have evolved into much more technically savvy terrorist organizations, their ability to threaten to U. S. National Security has likewise increased. The divergence between American national strategies, laws, and policies that govern counterterrorism (CT) operations within cyberspace has hampered the efforts of U. S. CT professionals to keep pace with the transformation of transnational terrorist organizations into more cyber-enabled threats.

Counterterrorism is defined as, “Actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks.”² Due to terrorists’ heavy reliance on cyberspace, it is an operational environment which CT professionals must simultaneously dominate, and effectively deny to these shadowy groups in order to defeat them. CT cyber strategies, law, and policies provide the framework through which CT cyber professionals execute their assigned operations.

Of considerable concern is the fact that current U. S. CT cyber policies are not necessarily completely sourced in domestic or international law, and they inhibit American CT professionals from efficiently implementing the very strategies which they are charged to execute. These restrictive and hierarchical CT cyber policies clearly

hinder the ability of strategic and operational-level military commanders who are deployed in support of Overseas Contingency Operations (OCO) to manipulate cyberspace to their greatest advantage.

In 2010 General David Petraeus, then Commander of United States Central Command (USCENTCOM) accurately described the degree to which al-Qa'ida was operating with impunity in cyberspace to finance, command, and recruit its forces.³ The tactical and operational commanders subordinate to General Petraeus in Iraq and Afghanistan often lamented that they were permitted to drop two-thousand pound bombs on terrorists' homes, but were forced to request from USCENTCOM Headquarters, or even the Secretary of Defense, the approval to attack or manipulate terrorists' computer networks.⁴ This dichotomous situation flies in the face of logic and is caused by a trifurcated divergence between: what is expected of military CT professionals in order kill or capture terrorists; what is permissible under current CT cyber law; and the current policies that actually govern offensive CT operations in cyberspace.

This work will analyze the current threat posed by international terrorist organizations from within cyberspace, as well as the inconsistencies between current national security, CT and cyber strategies, and the laws, and policies that permit CT professionals to disrupt and degrade international terrorist organizations through the use of the internet. The results of this analysis reveal that current cyber-related counterterrorism policies constrain military CT professionals, and that before CT cyber strategies can be effectively implemented, they must be in holistic alignment with cyber policies and existing statutes. Furthermore, this work proffers several recommendations

concerning adjustments to current CT cyber policies that are intended to better enable more efficient CT operations, and ultimately prevent future attacks on America and its interests.

The Nature of the Cyber-terror Threat

There is conclusive and irrefutable evidence that terrorist organizations such as al-Qa'ida in Iraq (AQI) not only recruit, propagandize, coordinate attacks, and finance their activities, but these terror organizations are actively seeking the means to initiate casualty-producing kinetic events using the worldwide web as well.⁵ Groups such as the Muslim Hackers Club have developed their own software and tutorials in order to sabotage not only U. S. computer networks, but to also seek to cause the physical destruction of key American infrastructure.⁶ ADM Michael Mullen, then Chairman of the Joint Chiefs of Staff described cyber terrorism as one of two existential threats to U. S. national security, the other being the Russian nuclear threat.⁷ Additionally, the intelligence community (IC) writ large considers cyber attacks as the most prominent, long-term threat to the country.⁸ Deputy Secretary of Defense William J. Lynn III similarly suggests that terrorists are seeking to effectively weaponize cyberspace in order to achieve kinetic effects against key U. S. infrastructure.⁹

Speed matters in stopping potentially calamitous events, and it is of seminal importance as al-Qa'ida and its ilk continue to develop more efficient and effective methods of attack.¹⁰ Current trends indicate that terrorist organizations such as Lashkar e-Tayyibah (LeT) and al-Qa'ida in Iraq (AQI) are investing heavily in the education of select members in the fields of computer and electrical engineering.¹¹ Ayman al

Zawahiri counseled deceased AQI leader Abu Musab al Zarqawi that half of the battle for Islam should be waged on the internet and he constantly stressed to Zarqawi the importance of digital information operations.¹²

In order to pay for their operations, terrorist groups have begun to resort to various forms of computer-assisted robbery and identity theft. Cybercrime has become so important to financing their operations, that it now surpasses drug trafficking as a source of income to fund their operations.¹³ During their investigation into the 2002 Bali bombing by Jemaah Islamiyah, the Indonesian police discovered that the attack was financed through computer credit card fraud.¹⁴

More disturbing than terror financing, is the implementation of a worldwide recruiting drive, launched by al-Qa'ida in order to co-opt computer and electrical engineers who already possess advanced degrees from elite universities. Before their demise, Al-Qa'ida in the Arabian Peninsula (AQAP) leaders Anwar al Awlaki and *Inspire Magazine* editor-in-chief Samir Kahn were posting high-tech want ads in their jihadi circular on the internet in order to elicit acts of terror by homegrown western Muslims. The two also posted numerous want-ads to recruit individuals who possessed high-tech degrees.¹⁵ As we shall learn, the lack of an effective U. S. CT Cyber policy prevented the timely interdiction and/or manipulation of the data on this website--action that could have been used to not only thwart AQAP's cyber efforts, but could have been used to create physical vulnerabilities within the organization as well.

The plots that could be hatched by heavily recruited techno-savvy terrorists are especially horrifying. Imagine if you will, the mayhem that could be unleashed by a terrorist, who using the internet, pilots multiple unmanned aircraft armed with explosive,

chemical, or biological payloads. A hint of this frightening scenario came to pass when the FBI foiled a plot by Rezwan Ferdaus, a young Bangladeshi-American physicist, who was arrested while in the process of developing the means to fly remote-controlled aircraft packed with explosives into the U. S. Capitol and the Pentagon. (Valencia, Milton J. and Ballou, Brian R. 2011, A1) Another terrifying possibility consists of dozens, if not hundreds of improvised explosive devices igniting simultaneously through the instantaneity of the internet. The process of perfecting this method of terrorist attack was proven to be well on its way to fruition, as was evident after the capture of numerous Al-Qa'ida in Iraq (AQI) improvised explosive device (IED) cell members. These individuals were detained while in the possession of hundreds of digital tone multi-frequency (DTMF) boards that were purported to be used to simultaneously initiate multiple IEDs to destroy U. S. and Iraqi security forces.¹⁶

Today these potential threats may seem far-fetched to some, but so did the concept of crashing jet airliners into the World Trade Center and the Pentagon prior to September 11th, 2001. These and other cyber-enabled terror plots are unfortunately far from fiction, as their perpetrators were caught in the acts of planning or executing them. The cyber terror threats which emanate from the various international terrorist organizations around the globe are of a seminal concern to U. S. national decision-makers. Though significant, the task of countering these terrorists' threats within cyberspace is anything but insurmountable, provided that those who are charged with exposing and attacking these networks are given the latitude to act effectively. The concerns of national leaders and their desires to exploit terrorist organizations in

cyberspace are clearly evident in the content of numerous past, and current national security strategy documents.

U. S. Cyber CT Strategies

Even at the onset of the war against terrorism during the early days of the Bush Administration, the threats posed from cyberspace were duly recognized--and the responses to cyber threats to U. S. National Security were publicly stated. In his 2003 National Strategy to Secure Cyberspace, President Bush proclaimed that, "When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U. S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner."¹⁷ As time has passed, the same tact can be seen in President Obama's *International Strategy for Cyberspace*, where he similarly refers to Article 51 of the U. N. Charter in the cyber realm by stating, "Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace."¹⁸ One would assume that this declaration applies to international terrorists who use the internet for malevolent purposes. Both strategies clearly imply that an attack on the United States from cyberspace could lead to a wide range of responses-- not excluding kinetic military operations.

Additionally, in his 2011 *National Strategy for Counterterrorism*, President Obama states that, "...together with our partners, we will degrade the capabilities of al-Qa'ida's local and regional affiliates and adherents, monitor their communications with al-Qa'ida leaders, drive fissures between these groups and their bases of support, and

isolate al-Qa'ida from local and regional affiliates and adherents who can augment its capabilities and further its agenda."¹⁹ Given that al-Qa'ida and its adherents communicate voluminously from within cyberspace, it is inferred that in order to disrupt their communications and isolate the organizations, the U. S. Government should exercise its inherent right to self-defense as stated in Article 51 of the United Nations Charter, and attack al-Qa'ida from within cyberspace.²⁰

The opportunities to adversely impact terrorist organizations through the use of cyber operations are limited only by the imaginations of its executors, and they can be accomplished with only a few key strokes. Classic military doctrine would label such activities as deception, defined by DoD as: "Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission."²¹ Intercepting al Qa'ida digital communications and modifying them in order to obtain possible locations of its members is potentially a highly effective CT tactic. Unfortunately, due to the current state of play that is promulgated by current cyber policies, executing this type of action in Afghanistan requires the approval of a major general.²² Although most international terrorists do not typically disclose their personal information on social media sites, they do, however; use social media (albeit using pirated or anonymous accounts) and thereby leave their digital fingerprints in cyberspace. This window into terrorists' computer networks provides CT professionals with ample opportunity to manipulate their devices, accounts and information in ways which causes them to expose both individual and collective organizational vulnerabilities to CT cyber professionals. A

preview of the use of cyber deception is indicated within DoD's own cyber strategy documents.

The DoD Strategy for Operating in Cyberspace clearly recognizes the threat posed by transnational terrorists to DoD personnel and systems and declares that terrorists have already attacked DoD networks and will continue to do so in the future. The strategy states that "...non-state actors (i.e. terrorists) increasingly threaten to penetrate and disrupt DoD networks and systems. We recognize that there may be malicious activities on DoD networks and systems that we have not yet detected."²³ The strategy further stipulates, "As directed by the *National Security Strategy*, DoD must ensure that it has the necessary capabilities to operate effectively in all domains- air, land, maritime, space, and cyberspace."²⁴ This dictum would imply that just as U. S. military forces conduct deception operations on the sea, land or in the air, they are similarly permitted to execute them in cyberspace as well. Furthermore, the DoD document unveils the five strategic initiatives that create a comprehensive framework to address cyber operations--to include the development and training of cyber forces.²⁵(United States Department of Defense 2011) These cyber forces, if properly leveraged, could serve as key enablers in the conduct of effective CT operations.

Finally, the 2011 *National Strategy for Counterterrorism* professes that the United States is at war (albeit an undeclared one) with al-Qa'ida, which would imply that military computer network operations (CNOs) should be governed by the same policies, laws, and rules of engagement as operations in other domains, such as war on the land, sea, or in the air, but this is not the case.²⁶ Perhaps a reason for this phenomenon, even though cyber operations are not a new tactic, is that CNOs can potentially cause

unintended political, economic, or even kinetic effects.²⁷ Due to this possibility of cyber-initiated collateral damage, key national decision-makers feel obliged to personally analyze the political risks involved, thereby withholding execution authority at higher levels of command.

Through its own strategy documents, the national security apparatus demonstrates there are seemingly no limits on how the U. S. Government could respond to acts of cyber terrorism. So what is missing from these key strategy documents concerning cyberspace? Nowhere in any public policy or national strategy document, does the government address actually attacking terrorist organizations from within cyberspace. Though not completely specific concerning cyber operations, these documents do not prohibit offensive or deception operations within cyberspace.

U. S. CT Cyber Law

One of the key (and most difficult) tasks in destroying terrorist organizations overseas is identifying and physically locating the individual leaders and members of these shadowy networks.²⁸ This laborious task within the cyber realm is conducted primarily by the Intelligence Community (IC), largely under the intelligence authorities granted in Title 50 of the U. S. Code and in accordance with the Foreign Intelligence and Surveillance Act (FISA).²⁹ FISA has been amended several times, most recently in 2008 by the 110th Congress, and it now permits surveillance of a foreign power, (e.g. international terrorist) or an agent thereof, that is reasonably believed to be located abroad, without the previously-required, and laborious process of obtaining a FISA order from the Foreign Intelligence Surveillance Court (FISC). The FISC consists of a

group of eleven judges who sit in *ex parte* status and are not always readily available in time-sensitive situations.³⁰

This virtual electronic collection capability that is utilized by the IC to target terrorists overseas, however, becomes immediately problematic if the monitoring of a foreigner's communications connects the foreign power to a U. S. citizen, or if the target in question is believed to be within the United States.³¹ If one of the latter two conditions exists, then the law forces cyber counterterrorism experts to obtain court orders to continue to monitor terrorists' electronic communications.(McConnell) Although FISA is now a much more streamlined process than during the pre-9/11 era, the primary negative effect of the requirement to seek surveillance orders from the FISC, is that terrorists could potentially get a head start on their pursuers. As then Director of National Intelligence (DNI), Mike McConnell described it, the overriding issue is that the, "law has not been changed to reflect technological advancements, we are missing potentially valuable intelligence needed to protect America."³² Mr. McConnell made this statement in the press prior to the passage of the 2008 FISA Act, which now contains a provision for the Attorney General and the DNI to immediately begin electronic surveillance in an emergency situation, provided that the FISC is notified within seven days after the surveillance is ordered.³³

Even in the event that a FISA order is required, the provisions of the amended FISA do provide CT intelligence professionals with adequate legal provisions to monitor terrorists' communications traffic. This access does come at a price, however; as Congress levied an immense oversight requirement upon all of the primary organizations involved in counterterrorism, namely DoJ, DoD, ODNI, CIA, and the

NSA.³⁴ The FISA Amendments Act of 2008 (H. R. 6304) is now the unequivocal electronic surveillance law of the land, but many of its provisions will expire in 2013 if it is not reauthorized.³⁵ The magnitude of the foreign surveillance program is clear, as the number of FISA orders has grown to over 1,700 per year, but since 2001 only 4 requests have been denied by the FISC. This trend indicates that U. S. counterterrorism electronic surveillance laws provide intelligence experts with wide latitude to collect intelligence against members of international terror organizations.³⁶

Although identifying international terrorists in cyberspace is critical to successful counterterrorism operations, it is only half of the battle in bringing them to justice. Monitoring terrorists' electronic communications is extremely important, but further work is required by the CT community to isolate, and eventually kill or capture the terrorists overseas. Manipulation or disruption of a terrorist organization's computer networks is a potential means to this end, and it is also a possible tactic that is employed to preempt a cyber or kinetic terrorist attack.³⁷ The laws that govern the actual manipulation of terrorists' electronic accounts and devices in order to make them more targetable, are not explicit or simply do not exist. The primary document that gives the President of the United States the authority to conduct offensive CT cyber operations overseas is the 2001 Authorization of the Use of Military Force, which gives the president the authority to "use all necessary and appropriate force" to protect the country for further attacks.³⁸ The extrapolation of this authority which permits the targeting of al-Qa'ida and its adherents, was employed in order to legally kill Anwar al Awlaki (an American citizen) in Yemen, and was invoked in permitting the planned (but not executed) computer network attack against his online magazine, *Inspire*.³⁹

Regardless of these authorities, General Keith B. Alexander, the Commander of U. S. Cyber Command, has expressed similar misgivings as Mr. O'Connell in response to Congressional inquiries concerning the efficacy of cyber laws. During his confirmation hearings that resulted in his appointment to the post of the commander of U. S. Cyber Command in 2010, General Alexander stated that there is a, "mismatch between our technical capabilities to conduct operations and the governing laws and policies."⁴⁰

When he assumed the mantle of command of this first-ever joint and interagency cyber unit, General Alexander retained his title and position as the Director of the National Security Agency (DIRNSA). This dual command role placed him in the unique position to not only locate and intercept enemy internet communications, but to also conduct computer network attacks on the terrorists' networks as well.⁴¹ The essence of this new command permits a more efficient cyber warfare capability which can theoretically operate seamlessly under both Titles 10 and 50 of the U. S. Code.⁴²

With over 1.8 billion Internet users and 4.6 billion cellular phone subscribers who generate approximately 90 trillion emails per annum, the establishment of U. S. Cyber Command from within the NSA was an extremely useful beginning.⁴³ A subordinate command to the United States Strategic Command (USSTRATCOM), Cyber Command was delegated Title 10 authority over military operations in cyberspace.⁴⁴ On the other hand, Cyber Command also possesses the ability to conduct covert actions within cyber space under Title 50.⁴⁵ This duplicitous legal framework is a result of current cyber policies and can create confusion over who is permitted to actually authorize a cyber operation.⁴⁶ In the end, this policy friction can translate into delays while the required

approvals are garnered, and could result in missing a fleeting opportunity to kill or capture a terrorist.

U. S. Computer Network Operations Policy

As a matter of current U. S. policy, the decision to label a computer network operation (CNO) as a traditional military activity (TMA), thereby falling under the purview of Title 10 of the United States Code (USC), or as a covert action under Title 50 of the USC, has spurred a great deal of discussion at the highest levels of the U. S. Government.⁴⁷ Although cyber warfare is only one aspect of the overall current Title 10/50 debate that is raging within Congress and the various departments within the executive branch, one cannot legitimately discuss the policies that govern the approvals to conduct CNOs without touching upon this current source of friction.⁴⁸ Much of the policy concerning the details of computer network operations is classified, but is gaining in importance such that many policy experts are speaking about it, some albeit from under the cloak of anonymity.⁴⁹ As Andru E. Wall suggests, the confusion over Title 10 and Title 50 authorities appears to have, "...more to do with congressional oversight and its attendant internecine power struggles than with operational or statutory authorities," despite the fact that by design, Title 10 and 50 authorities are mutually supporting and were not intended to be competing.⁵⁰ Retired Admiral Dennis C. Blair (former ODNI) proclaimed that, "This infuriating business about who's in charge and who gets to call the shots is just making us look muscle-bound." ADM Blair went on to bemoan the "over-legalistic" approach to CT cyber--despite the fact that current cyber

laws are woefully inadequate to address the, ...”complexity of the global information network.”⁵¹(Wall 2011101)

Current media reports indicate that the use of specially-designed cyber tools in order to target states or non-state actors requires presidential approval. An example of this approval policy was seen last year when media reports indicated that the Stuxnet cyber-worm was allegedly implanted in an Iranian nuclear facility, an act that American military cyber warriors will not publicly confirm.⁵² This computer virus subtly attacked the computers that controlled the enormous Iranian nuclear centrifuges and caused them to self-destruct. Although the Stuxnet infestation in Natanz was a major attack with immense international political consequences, media reporting suggests that less contentious operations against terrorists’ computer networks have taken on a similarly hierarchical approval process, even though these computer network operations support the local war fighters in Afghanistan or Iraq.⁵³ For instance, in the early years of the Iraq war, numerous attempts to hack into terrorists’ email accounts and send erroneous information from them, in order to expose other members of AQI or cause potential organizational rifts was strictly forbidden without the approval of the CENTCOM Commander.⁵⁴

The reasoning behind this elevated approval policy centers upon the fact that terrorists frequently use American or allied internet service providers (ISPs) to access and manipulate the internet during the conduct of their own cyber operations.⁵⁵ The consequences of this arrangement, which could ultimately involve the U. S. Government manipulating an American or allied server network in order affect a terrorist

organization, makes many national leaders leery of employing the capability in the first place.⁵⁶

The ongoing debate between elements of the DoD, who feel that certain cyber operations are a traditional military activity and should be governed by the laws of armed conflict and Title 10 of the U.S. Code, and leaders within the Intelligence Community (IC) who contend that any and all cyber operations are inherently covert and should be under the purview of Title 50, shows no signs of abating. An example of this conundrum occurred in June, 2010 when the U. S. was allegedly contemplating a cyber attack on Inspire Magazine.⁵⁷ The U. K.'s GCHQ Intelligence Service actually conducted an attack, dubbed "Operation Cupcake" while the CIA and Cyber Command were reportedly still haggling over whether attacking the site was a traditional military activity (TMA), thereby considered a Title 10 action, or a covert action under Title 50.⁵⁸ Although this operation had little kinetic effect, it was disruptive as GCHQ managed to effectively replace the bomb-making recipes on the Inspire site with actual cupcake baking recipes.⁵⁹ The delay caused by the policy debate within the executive branch ultimately led to a missed opportunity. The effect of a potential delay could have been much more significant had the stakes been higher, particularly if the purpose of the proposed CT cyber operation was to thwart an impending attack.⁶⁰

Another potential genesis for the policy debate is the inconsistent verbiage used between the Military and the IC when categorizing operations in cyberspace. For example, if any data within an enemy computer network is modified, then the operation is labeled a Computer Network Attack (CNA) by the military.⁶¹ The IC considers data manipulation as an Offensive Cyber Operation (OCO), a title which is much more

palatable to CT lawyers than the term Computer Network Attack, even though the intent and outcome of the operations are identical.⁶² The differences between these labels are frequently referenced in policy debates, which ultimately slow down the process of finding and interdicting terrorists.

Current CT Cyber Legal and Policy Initiatives

The confusion surrounding the current CT cyber policy and laws caused the House Armed Services Committee to attempt to address the conundrum in the drafting of the National Defense Authorization Act (NDAA) for Fiscal Year 2012.⁶³ Section 961 of the House bill (HR 1540) stipulated that military activity is not confined to a physical domain, and provided the Secretary of Defense the authority to conduct clandestine (read Title 10) offensive operations in cyberspace. HR 1540 further directed that clandestine CNO authority was to be granted to the Secretary of Defense to execute cyber operations against a CT target, provided that the target is located outside of the United States and is pursuant to the Authorization for the Use of Military Force (AUMF).⁶⁴ According to HR 1540, the SECDEF was also granted de facto Title 10 CNO authority when defending against cyber attacks on DoD assets. Although this bill determined that a presidential finding was not required, as it is to conduct a covert action, it did dictate that the Secretary of Defense would inform Congress of DoD's CNO activities every 120 days.⁶⁵

HR 1540 passed a full vote in the House, but the Senate drastically modified the cyber portion of the bill in their version of the 2012 NDAA (S. 1867) which contained completely different verbiage concerning military operations in cyberspace than what

was resident in HR 1540. The cyber warfare clause in the House bill was replaced by the Senate version in Sections 931-932 with language that was more concerned with the establishment and implementation of enhanced cyber defense measures, rather than offensive cyber operations.⁶⁶ Despite being stalled in negotiations after it was approved by the Senate Armed Services Committee (SASC) in June of 2011, S. 1867 eventually passed the Senate with a vote of 93 to 7 on December 1st, 2011, and was signed into law by President Obama on December 31st, 2011.⁶⁷

The 112th Congress missed a potential opportunity to enhance the efficacy of cyber CT operations through the legislative process. Many members of the House Armed Services Committee (HASC) and the Senate Armed Services Committee (SASC) agree that military cyber operations are critical to counter terrorism efforts and to protect U. S. troops abroad.⁶⁸ The newly-enacted 2012 NDAA completely avoids the subject of offensive CT cyber operations altogether. Ultimately, the NDAA could have served as a forcing function to cause national decision-makers to potentially craft more comprehensive CT cyber policies that are better aligned with domestic and international cyber laws and national strategies.

While Congress was pursuing legislative change, DoD leadership began to codify a list of pre-approved cyber weapons that can be employed on foreign networks without garnering the nod from national decision-makers. Although the details of this policy directive are classified, it is potentially a step in the right direction to put a valuable capability into the hands of the commanders who are engaged in combat operations. Anonymous media sources have described the general theme of the proposed DoD

approach as one that more closely models the law of armed conflict, as opposed to one that resembles a policy to govern the use of weapons of mass destruction.⁶⁹

Recommendations

The bulk of the recommendations provided below concern possible modifications to existing CT cyber policies in order to bring them better into alignment with existing laws and strategies. Through its key cyber strategy document, DoD has determined that cyberspace is a military domain similar to the those of land, sea, and air; therefore as the overarching framework, CT cyber operations within an AOH should be governed by the law of armed conflict (LOAC).⁷⁰ For those targets (and supporting cyber infrastructure) that lie outside of the current AOH, military CT cyber operations should be utilized only in the execution of targets that are pursuant to the current AUMF.

The first step in rectifying the CT cyber policy should be for the IC and DoD to accurately define and properly name CT cyber operations. This may be effectively accomplished through the merger of both the IC and DoD cyber lexicon. The names given to CT cyber operations should be derived on the basis of the desired effects of the operation. If a cyber operation produces a kinetic effect that is intended to destroy terrorists or their equipment, then it should be labeled a “CT cyber attack (CCA).” If the desired effect of a CT cyber operation is to manipulate terrorists’ data, equipment, or minds (i.e. cyber deception), then the operation should be dubbed an “offensive CT cyber operation (OCCO).” Standard intelligence collection of terrorists’ cyber networks in support of either a military commander or the IC should simply be labeled “CT cyber collection (CCC).”

Next, the above CT cyber capabilities and operations should be appropriately matched to their approval level, and the resources to conduct such operations should likewise be provided to that approving authority. At least on the tactical U. S. military level, the approvals to conduct cyber operations that only effect a limited population or area of operation within an AOH, should be governed by a much lower level of command than current policies dictate. For that matter, the capability to conduct low-level, localized CT cyber operations that anticipate little or no international repercussions (Offensive CT Cyber Operations and CT Cyber Collection) should be provided down the O6 (Colonel) level of command or whatever level of command is authorized to conduct offensive kinetic operations of similar size and scope. Brigade Combat Team (BCT) commanders are assigned large swaths of battlespace in Afghanistan, and their ability to leverage CT cyber capabilities and approve OCCOs and CCCs would definitely increase the efficacy and pace of CT operations within the AOH. The authorities to conduct CT Cyber Attacks (CCA) should be retained by the AOH theater commander or his designated representative. If the effects of a CCA will likely spill outside of the AOH, then the Geographical Combatant Commander or his designated representative should be the approving authority to the same extent that they approve traditional kinetic operations. In each instance, the overriding theme should be to delegate execution authority down to the lowest level feasible in order to maximize the effects of CT cyber operations.

Cyber operations are not exclusively a military capability, despite the fact that the great preponderance of cyber operations are conducted by the NSA (a DoD Agency), and they have proven to be a key enabler to the success of many overseas CT

operations. If DoD and the greater IC continue to refuse to come to an agreement on which agency should execute which types of cyber operations, then the White House should settle the issue through the drafting of a comprehensive CT cyber policy. This policy should generally outline which agencies have primacy for certain types of operations, which will at least settle the matter of who is in charge.

In order to avoid the time-consuming task of attempting to rewrite the U. S. Code (that does not require revision), the next set of recommendations will serve to attempt to generally delineate which authorities should be employed, under which circumstances, in the conduct of CT cyber operations. If a CT cyber operation is conducted in support of a military commander, and/or as a part of, or in advance of, a larger military operation, then Title 10 authorities should be employed, even in the event that 3rd party data systems are manipulated outside of an AOH. The data manipulation should be permissible so long as the manipulation does not destroy or disrupt the service or equipment of civilians uninvolved in the conflict concerned. Conversely, if a cyber operation is conducted as, or in support of, a covert action completely independent of, or outside of an existing AOH, then Title 50 authorities should be leveraged in accordance with appropriate congressional oversight. In order to perform their tasks, CT cyber professionals may be required to access servers or equipment that is not located within an AOH, and is frequently located within a friendly country. As long as that equipment or the individuals that operate it are not harmed, then the operations should not necessarily be deemed a covert action. The logic behind this recommendation is due largely to the fact that most cyber operations are by their very nature, deniable.

Lastly, in order to maintain synergy, and to prevent fratricide, cyber operations should be de-conflicted on a constant basis. The personnel, skills, and tools used in cyber collection are nearly identical to those to conduct offensive cyber operations.⁷¹ This would indicate that perhaps a centralized fusion center is required between the IC and U. S. Cyber Command which would not only de-conflict CT cyber missions between the disparate organizations, but it would also rapidly provide needed capabilities to customers in a responsive fashion as well. The reaction time between the discovery of a terrorist on the worldwide web, and the need to manipulate his or her computer systems is extremely limited, and the future security of the United States depends upon the ability of CT cyber professionals to operate within this narrow gap to the maximum extent possible.⁷²

Conclusion

The effective fusion of inter-agency intelligence and the military operational aspects of CT has proven to be as necessary as it is effective in both in Iraq and Afghanistan. The congressional mechanisms that fund and oversee the military and the IC however, have been anything but fused since 9-11.⁷³

Despite a key recommendation of the 9-11 commission to the contrary, the built-in stovepipes between how Congress organizes and funds the IC and the DoD have been maintained through 10-plus years of constant CT operations.⁷⁴ The lessons learned from the early days of OPERATION ENDURING FREEDOM should be heeded in that, CT operations and those who conduct them should not be held hostage by the negative perceptions of legislators that military and IC operations are virtually

indistinguishable. CT cyber operations are no different and should be judged only by their efficacy, so long as they are conducted within the confines of the law.⁷⁵ Due to the increased digitization of the current threat posed by international terrorist organization, now is the time to coalesce national CT cyber policy, law, and strategy into an effective triumvirate—and not after a “digital mushroom cloud” has appeared on the horizon.

Endnotes

¹ Barrack Hussein Obama, *National Strategy for Counterterrorism* (Washington D. C.: The White House, June 2011), 9.

² Department of Defense, "DoD Dictionary of Military Terms," http://www.dtic.mil/doctrine/dod_dictionary/data/c/10082.html (accessed January 9, 2012).

³ Senate Armed Services Committee, *Posture of the U. S. Central Command*, 2010, 49. Charles Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly*, no. Spring (2011), 81.

⁴ Brennan, John, *Author's Personal Experiences in Iraq and Afghanistan from 2001-2011*.

⁵ Gabriel Weimann, *Special Report 116: [Www.Terror.Net](http://www.terror.net) how Modern Terrorism Uses the Internet* (Washington, D. C.: United States Institute of Peace, March 2004), 5.

⁶ *Ibid.*, 7.

⁷ Rockefeller, Jay and Chertoff, Michael, "A Step Toward Improving Cybersecurity," *The Washington Post*, November 18, 2011 (accessed November 21, 2011).

⁸ *Ibid.*

⁹ Aliya Sternstein, "Pentagon Concerned about Terrorists' Cyberwar Capabilities," NextGov Technology and the Business of Government, http://cybersecurityreport.nextgov.com/2011/06/pentagon_concerned_about_terrorists_gaining_cyberwar_capabilities.php (accessed January 9, 2012).

¹⁰ Weimann, *Special Report 116: [Www.Terror.Net](http://www.terror.net) how Modern Terrorism Uses the Internet*, 9.

¹¹ *Ibid.*, 9.

¹² Theohary, Catherine A. and Rollins, John, *Terrorist use of the Internet: Information Operations in Cyberspace* (Washington D. C.: Congressional Research Service, 2011), 3, www.crs.gov (accessed November 17, 2011).

¹³ Ibid., 2.

¹⁴ Ibid., 2.

¹⁵ Schone, Mark and Cole, Matthew, "American Jihadi Samir Khan Killed with Awlaki," ABC News, <http://abcnews.go.com/Blotter/american-jihadi-samir-khan-killed-awlaki/story?id=14640013#.TrRjfPTXo-0> (accessed 11/3, 2011).

¹⁶ Valencia, Milton J. and Ballou, Brian R., "Rezwan Ferdaus Indicted for Alleged Plot to Attack Capitol, Pentagon," *The Boston Globe*, 29 September 2011, <http://www.boston.com/Boston/metrodesk/2011/09/alleged-terror-plotter-indicted-federal-grand-jury/OevOhHc4o1VwcQABMplHIN/index.html> (accessed 17 October, 2011).

¹⁷ Brennan, *Author's Personal Experiences in Iraq and Afghanistan from 2001-2011*.

¹⁸ Jason Healey, *Bringing a Gun to a Knife Fight: US Declaratory Policy and Striking Back in Cyber Conflict*, <http://www.acus.org/publication/us-declaratory-policy-and-striking-back-cyber-conflict> ed. (Washington, D. C.: Atlantic Council at 50, 21 September, 2011), 2.

¹⁹ Barrack Hussein Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington DC: The White House, May 2011), 10.

²⁰ Obama, *National Strategy for Counterterrorism*, 9.

²¹ United Nations General Assembly, *United Nations Charter, Chapter 7, Article 51* (San Francisco, CA, June 25, 1945).

²² Department of Defense, *DoD Dictionary of Military Terms*, 1.

²³ *Interview with a Confidential Source.*, December 14, 2011).

²⁴ United States Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011), 1.

²⁵ Ibid., 5.

²⁶ United States Department of Defense, *Department of Defense Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934* (Washington, D. C.: United States Government, 2011), 1.

²⁷ Obama, *National Strategy for Counterterrorism*, 2.

²⁸ Welch, General Larry D. USAF (Ret), "Cyberspace-the Fifth Operational Domain," *IDA Research Notes-Challenges in Cyberspace*, no. Summer (2011), 2-4.

²⁹ Brennan, *Author's Personal Experiences in Iraq and Afghanistan from 2001-2011*.

³⁰ United States Congress, *Title 50, U. S. Code-War and National Defense*, trans. United States House of Representatives (Washington, D. C., 2010), Chapter 36, http://www.law.cornell.edu/uscode/50/usc_sec_50_00001802----000-.html (accessed November 9, 2011).

³¹ Silvestre Rep Reyes, *FISA Amendments Act of 2008*, ed. Lamar Rep Smith and Peter Rep Hoekstra, trans. United States House of Representatives, Intelligence ed., Vol. Public Law No: 110-261 (Washington, D C: Federal, 2008), 105.

³² Stephen Dycus, *Counterterrorism Law*, ed. William C. Banks and Peter Raven-Hansen (New York: Aspen Publishers, 2007), 122.

³³ Mike McConnell, "A Law Terrorism Outran: We Need a FISA for the 21st Century," *The Washington Post*, May 21, 2007.

³⁴ Ibid.

³⁵ Rep Reyes, *FISA Amendments Act of 2008*, Sec. 105.

³⁶ Ibid., Sec 101.

³⁷ Ibid., Sec 101.

³⁸ H. L. Pohlman, *Terrorism and the Constitution: The Post-9/11 Cases* (Lanham, Maryland: Rowman & Littlefield Publishers, 2008), 71.

³⁹ Shanker, Thomas and Schmitt, Eric, "U.S. Military Goes Online to Rebut Extremists' Messages," *The New York Times*, November 18, 2011 (accessed November 21, 2011).

⁴⁰ 107th United States Congress, *Authorization for use of Military Force*, trans. Joint Session, Joint Resolution ed., Vol. 107-40 (Washington, D. C., 2001).

⁴¹ Ellen Nakashima, "List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare," *The Washington Post*, May 31, 2011.

⁴² Thomas Shanker, "Cyberwar Nominee Sees Gap in Laws," *The New York Times*, April 14, 2010, <http://www.nytimes.com/2010/04/15/world/15military.html> (accessed November 9, 2011).

⁴³ Ibid.

⁴⁴ Robert Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of National Security Law and Policy* 5, no. 539 (January 24, 2012), 58, <http://www.jnslp.com/2012/01/24/military-intelligence-convergence-and-the-law-of-the-title-10title-50-debate-3/> (accessed February 9, 2012).

⁴⁵ *Statement of General Keith B. Alexander, Commander United States Cyber Command before the House Committee on Armed Services*, 3.

⁴⁶ Ibid., 5.

⁴⁷ Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 57.

⁴⁸ Ellen Nakashima, "Pentagon's Cyber Command Seeks Authority to Expand its Battlefield," *The Washington Post*, November 6, 2010.

⁴⁹ Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 58.

⁵⁰ *Ibid.*, 72.

⁵¹ Nakashima, *List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare*, A1-A2.

⁵² Andru E. Wall, "Demystifying the Title 10 - Title 50 Debate: Distinguishing Military Operations, IntelligenceActivities & Covert Action," *Harvard National Security Journal* 3, no. 1 (2011), 101.

⁵³ Nakashima, *Pentagon's Cyber Command Seeks Authority to Expand its Battlefield*, A2.

⁵⁴ Nakashima, *List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare*, A1-A2.

⁵⁵ Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 59.

⁵⁶ Brennan, *Author's Personal Experiences in Iraq and Afghanistan from 2001-2011*.

⁵⁷ Nakashima, *List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare*, A1-A2.

⁵⁸ Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 59.

⁵⁹ Duncan Gardham, "MI6 Attacks Al-Qaeda in 'Operation Cupcake'," *The Telegraph*, June 2, 2011.

⁶⁰ Nakashima, *List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare*, A1-A2.

⁶¹ Gardham, *MI6 Attacks Al-Qaeda in 'Operation Cupcake'*.

⁶² Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 75.

⁶³ Department of Defense, *DoD Dictionary of Military Terms*, 1.

⁶⁴ Wall, *Demystifying the Title 10 - Title 50 Debate: Distinguishing Military Operations, IntelligenceActivities & Covert Action*, 118.

⁶⁵ Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 59.

⁶⁶ *National Defense Authorization Act for Fiscal Year 2012*, HR 1540, 1st Session, 112th Congress, , no. HR 1540, (May 26, 2011): 962.

⁶⁷ *Ibid.*

⁶⁸ *National Defense Authorization Act for Fiscal Year 2012*, S. 1867, 1st Session, 112th Congress, , no. S. 1867, (June 22, 2011): 931, <http://www.ng.mil/II/analysisdocs/FY2012/S1253SASC.pdf> (accessed November 15, 2011).

⁶⁹ E. D. Kain, "President Obama Signed the National Defense Authorization Act - Now what?" *Forbes*, <http://www.forbes.com/sites/erikkain/2012/01/02/president-obama-signed-the-national-defense-authorization-act-now-what/> (accessed January 16, 2012).

⁷⁰ Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 59.

⁷¹ Nakashima, *List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare*, A1-A2.

⁷² Dunlap, *Perspectives for Cyber Strategists on Law for Cyberwar*, 81.

⁷³ Wall, *Demystifying the Title 10 - Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action*, 121.

⁷⁴ *Ibid.*, 121.

⁷⁵ *Ibid.*, 122.