Strategy Research Project

Defining Cyber and Focusing the Military's Role in Cyberspace

by

Lieutenant Colonel Samuel P. Mowery
United States Marine Corps

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Defining Cyber and Focusing the Military's Role in Cyberspace

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Samuel P. Mowery
United States Marine Corps

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Prentiss O. Baker
Department of Military Strategy, Planning, and Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5,208

14. ABSTRACT

This strategy research paper proposes definitions for cyber crime, cyber war, and cyber terrorism that possess potential for wide adoption throughout the U.S. government, civilian sector, and international community. Using the proposed definitions, more distinct roles for government agencies and civilian sector emerge. The Department of Homeland Security (DHS) retains the lead for overall domestic cyber security with support from the Department of Defense (DoD), Department of Justice (DoJ), Department of State, and the civilian sector. DoD assumes primary responsibility for cyber war, while DHS and DoJ assume primary responsibility for cyber crime and cyber terrorism. The proposed definitions permit DoD to focus on defending, deterring, disrupting, and defeating adversaries that conduct and prosecute cyber war against the U.S. and its allies. The proposed definitions also help to identify cost savings by reducing or eliminating inefficient and duplicative capabilities throughout the government. Lastly, the proposed definitions serve as an aid to decision makers as they work their way through the challenges of Jus ad Bellum and Jus in Bello when responding to cyber threats.

15. SUBJECT TERMS
Definitions, Crime, War, Terrorism, Strategy

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)*
UU	UU	UU	UU	32	

USAWC STRATEGY RESEARCH PROJECT

Defining Cyber and Focusing the Military's Role in Cyberspace

by

Lieutenant Colonel Samuel P. Mowery
United States Marine Corps

Colonel Prentiss O. Baker
Department of Military Strategy, Planning, and Operations
Project Adviser

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

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

Abstract

Title:	Defining Cyber and Focusing the Military's Role in Cyberspace
Report Date:	March 2013
Page Count:	32
Word Count:	5,208
Key Terms:	Definitions, Crime, War, Terrorism, Strategy
Classification:	Unclassified

This strategy research paper proposes definitions for cyber crime, cyber war, and cyber terrorism that possess potential for wide adoption throughout the U.S. government, civilian sector, and international community. Using the proposed definitions, more distinct roles for government agencies and civilian sector emerge. The Department of Homeland Security (DHS) retains the lead for overall domestic cyber security with support from the Department of Defense (DoD), Department of Justice (DoJ), Department of State, and the civilian sector. DoD assumes primary responsibility for cyber war, while DHS and DoJ assume primary responsibility for cyber crime and cyber terrorism. The proposed definitions permit DoD to focus on defending, deterring, disrupting, and defeating adversaries that conduct and prosecute cyber war against the U.S. and its allies. The proposed definitions also help to identify cost savings by reducing or eliminating inefficient and duplicative capabilities throughout the government. Lastly, the proposed definitions serve as an aid to decision makers as they work their way through the challenges of Jus ad Bellum and Jus in Bello when responding to cyber threats.

Defining Cyber and Focusing the Military's Role in Cyberspace

> Does anyone have a common understanding of what's encompassed by the word "cyber" in the first place?
>
> —Jared Serbu[1]

The lack of agreed upon cyber definitions has extensive consequences that affect the U.S. government's policies, roles of agencies, allocation of cyber resources, and cyber funding. Perplexity in the U.S. government is commonplace due to the lack of identifiable lanes in the road for departments, agencies, and civilian sector associated with cyberspace. Most importantly to the Department of Defense (DoD), the lack of definitions forces the department to focus on the entire spectrum of cyberspace operations that spans from countering petty crime to preventing the cyber equivalent of 9/11. The lack of identifiable lanes creates inefficiencies throughout the government that often force the Department of Justice (DoJ) to sort out jurisdiction issues where shared responsibility exists. To respond appropriately to threats in the cyber domain, the U.S. government needs whole-of-government definitions to determine what acts constitute cyber crime, cyber warfare, and cyber terrorism. Once the government develops agreed upon definitions, it can revise the U.S.'s cyber strategy to combat more effectively and efficiently the ever-expanding range of cyber threats. More specifically, a revised cyber strategy based upon the definitions will allow DoD to focus on its war fighting abilities and to step back from attempting to defend the U.S. from the entire spectrum of cyber threats, which Sun Tzu warned against in his statement, "And when he prepares everywhere he will be weak everywhere."[2]

This strategy research paper proposes definitions for cyber crime, cyber warfare, and cyber terrorism that possess potential for wide adoption throughout the U.S.

government, civilian sector, and international community. The layout of the paper begins with a discussion about the lack of definitional guidance across the entire U.S. government and the absence of basic cyber definitions in Joint publications. Next, the paper provides a synopsis of the roles and responsibilities of organizations in cyberspace. The discussion then turns to the identification of actors involved in cyber actions as well as their intent and motives. After proposing definitions for cyber crime, cyber war, and cyber terrorism, the paper reconsiders the roles and responsibilities throughout the U.S. government and civilian sector based upon the proposed definitions. Lastly, the paper examines how the proposed definitions affect the decision process used to determine when the U.S. should respond to acts of cyber crime, cyber war, and cyber terrorism. For purposes of clarity and expectation management, this paper does *not* propose any type of rules of engagement.

The U.S. government does not have an official definition of cyber crime, cyber war, or cyber terrorism, nor does one department or agency have sole jurisdiction of cyber crime, cyber war, or cyber terrorism. The terms appear interchangeable in documents and policy, and in many cases, particularly involving cyber crime, federal law enforcement agencies often define cyber crime based upon jurisdiction.[3] Joint Publication 1-02, which provides definitions of military and associated terms for the Joint Force, does not include definitions for cyber crime, cyber warfare, or cyber terrorism. The publication only lists three terms with the word cyber in them: cyber counterintelligence, cyberspace, and cyberspace operations.[4] Until the U.S. acquires a common lexicon or terms of reference, military operations in cyberspace must follow parallel rules to military operations conducted in the physical domains or conventional

world.[5] This parallel approach is not as effective as one tailored to the dynamic nature of cyberspace because cyberspace operations require Joint, interagency, and international cooperation. Although U.S. Cyber Command is diligently adapting and informing policy and doctrine for cyberspace operations, the legal and policy challenges are daunting, as the recent failure of Congress to pass a cyber security bill indicates.[6]

In addition to U.S. Cyber Command, there are a multitude of interagency organizations that possess a role in the cyber domain, which often leads to overlapping authorities. The Department of Homeland Security (DHS) has responsibility for coordinating and orchestrating the nation's cyber defense and is the federal government's lead agency for securing civilian government computer systems and critical infrastructure. DHS leverages its U.S. Secret Service (USSS) and the U.S. Immigration and Customs Enforcement (ICE) to investigate cyber criminals.[7] DoD's role is not only to defend its own networks, but also "to be prepared to defend the nation and our national interests against an attack in or through cyberspace."[8] The National Security Agency (NSA) has responsibility for securing the government's classified networks.[9] DoJ's Federal Bureau of Investigation (FBI) leads the national effort to investigate high-tech crimes, including cyber-based terrorism, espionage, computer intrusions, and major cyber fraud.[10] All agencies and departments work in partnership with DoJ to delineate domestic jurisdictional lines and to prosecute the perpetrators of cyber events.

From an international perspective, the United Nations (U.N.) and The North Atlantic Treaty Organization (NATO) have significant relevance regarding cyberspace operations. The U.N.'s charter advocates that states should "refrain in their international

relations from the threat or use of force" against another state.[11] However, no consensus exists on what constitutes the threat or use of force when it relates to cyberspace. Similarly, from a NATO perspective, there is no consensus on what constitutes an "armed attack" in Article 5 of the Washington Treaty. Article 5 states, "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all."[12] Robert Butler, Deputy Assistant Secretary of Defense for Cyber Policy, best characterized in 2010 the ambiguous nature of cyber events when he said, "We hear a lot of discussion about cyber war and cyber attacks, and there's legal terminology with hostile intent, hostile acts. Making sure everyone understands the taxonomy is really important."[13]

The Council of Europe's Convention Committee on Cybercrime is another international organization that has relevance regarding cyberspace operations. The organization plays a role in achieving international unity of effort to counter the cyber crime threat. On August 4, 2006, the U.S. Senate ratified the Council of Europe's Convention Committee on Cybercrime Treaty (hereafter called the Budapest Convention on Cybercrime).[14] In total, 38 states have ratified the treaty, which aims to achieve three key goals: 1) to establish a list of domestic criminal offenses and conduct that are prohibited by the treaty, 2) to adopt a set of procedural tools and powers to properly and effectively investigate crimes, and 3) to establish strong mechanisms for fostering international cooperation.[15] These goals are essential to keep in mind when definitions of cyber crime, cyber war, and cyber terrorism are discussed later. The Budapest Convention on Cybercrime is important because cyber issues threaten the entire international community, not just the U.S. and Europe.

Cyber actors, a collective term used in this paper to describe those committing acts of cyber crime, cyber war, and cyber terrorism, include a number of diverse actors with different objectives and motives. Secretary of Defense Panetta stated on October 11, 2012, that when people think of the cyber threat, they have a limited vision of "criminals who prowl the Internet and steal people's identities, sensitive business information, or even national security secrets."[16] Secretary Panetta acknowledged the list of cyber actors goes well beyond this limited vision when he warned a cyber event perpetrated by a state or violent actor could be as destructive as the terrorist attacks of September 11, 2001.[17]

In general, criminals, nation-states, non-state actors, violent extremist groups, organized crime groups, and corporations conduct cyberspace operations, but they do so for reasons that normally fall into three different categories: individuals and criminal organizations interested in stealing for monetary gain, "hactivitsts" intent on furthering their own agendas, and foreign governments or their agents aiming to steal information or lay the groundwork for subsequent operations.[18] According to the FBI, monetary gain motivates organized crime groups to prey on the financial sector; ideology motivates violent extremist groups and non-state actors to disrupt or harm the viability of dissimilar ways of life; and the acquisition of intellectual property motivates corporations to engage in espionage.[19] The motivation of nation-states varies. The acquisition of intellectual property motivates some nation-states just like corporations. Other nation-states are trying to obtain a profit, while others are identifying exploitable digital weaknesses, possibly for a future attack.

In addition to the aforementioned external actors threatening the U.S.'s security in cyberspace, two types of internal actors exist. First, malicious insiders possess the capability to exploit their access to government, public, or private cyber networks on their own initiative or at the behest of foreign governments, terrorist groups, criminal organizations, or unscrupulous associates.[20] Devastating effects to national security could result regardless of the malicious insider's intent, which might range from committing espionage, making a political statement, or expressing disgruntlement. Second, complacent insiders pose a threat as real as malicious insiders. Dr. James A. Lewis from the Center for Strategic and International Studies candidly addressed the passivity of complacent insiders during his statement before Congress on April 24, 2012:

> "In the Internet community, there are many who still believe that the Internet can heal itself, that civil society and multi-stakeholder Internet governance will ultimately provide adequate security. They say that threats in cyberspace are exaggerated and that better cyber security puts privacy and the alleged virtues of an open Internet for innovation at risk. This is simply naïve and outdated. This sort of approach has never worked anywhere else, and it is not working now in cyberspace."[21]

Internal actors complicate the U.S. government's challenge of achieving security in cyberspace operations by adding another layer of malicious actors and complacent insiders to an already abundant amount of external actors.

The sheer number of potential actors threatening the U.S. in cyberspace, pervasiveness of the Internet, low cost of computer technology, and availability of malware provide challenges to the U.S.'s ability to counter cyber threats. These challenges come in the form of attribution, jurisdictional, and technological challenges. In addition to providing access to a plethora of rich targets, the Internet provides cyber actors access to anonymity and lack of traceability, which complicates the process of

determining attribution. According to Dr. Lewis, attribution is difficult, but not impossible.[22] Attribution is a necessary step in the process to determine motivation, which victims of cyber actions then use to determine how to respond to the event. Further complicating the matter, actions that constitute a crime in one state might not constitute a crime in another state. Some state, city, and local law enforcement agencies may not have the technological capabilities to keep pace with cyber actors. Worse yet, when an incident crosses geographic boundaries, particularly international boundaries, jurisdictional issues regarding case investigation and prosecution may cause significant impediments to effective law enforcement. Even when cyber actors leave a trace, victims must decide whether or not to pursue the trace. Hackers like Anonymous routinely boast about uncovering vulnerabilities, but victims often conceal information to preserve company reputations and investor confidence.[23] General Alexander, the Commander of U.S. Cyber Command and Director of the NSA, supports legislation that would *require* private companies to report cyber events. Additionally, General Alexander feels such reporting needs to happen before an incident is complete. He said, "We have to have the ability to work with industry—our partners—so that when they are attacked, they can share that with us immediately."[24]

DHS and DoD already share an ability to work together, which is exemplified by a Memorandum of Agreement (MOA) between the two departments. The MOA charges DHS and DoD to provide personnel, equipment, and facilities in order to increase interdepartmental collaboration in strategic planning for the nation's cyber security, mutual support for cyber security capabilities development, and synchronization of current operational cyber security mission activities.[25] The aim of the MOA is to focus

effort and increase capacity and capability while providing integral protection for privacy, civil rights, and civil liberties. The sharing of information between government and the civilian sector potentially affects issues of privacy, civil rights, and civil liberties, which are some of the most contentious issues preventing recent passage of congressional legislation regarding cyber security.[26] The aforementioned challenges of attribution, jurisdiction, and technology only begin to describe the dynamic nature of cyberspace operations.

Thus, the need for defining cyber crime, cyber war, and cyber terrorism is paramount to the refinement of a cyber strategy that more effectively delineates roles and responsibilities of organizations in the U.S. government and civilian sector. The lack of definitional clarity is problematic as it impacts every facet of cyber strategy. Definitions provide a common language that is necessary for sound collaboration and meaningful discussion, as well as effective deterrence and defense against cyber events.[27]

The first term that needs a clear definition is cyber crime. Definitions of cyber crime vary, but most resemble a "crime that is enabled by, or that targets computers."[28] This common definition does not provide nearly enough detail to help jurisdictional issues or facilitate collaboration among governments or departments. The European Commission understands cyber crime as "criminal activity committed using electronic communications networks and information systems or against such networks and systems," but its practical application of the term cyber crime goes into more detail. Its practical application states cyber crime as the following: 1) traditional forms of crime such as fraud or forgery, though in a cyber crime context relates specifically to crimes

committed over electronic communication networks and information systems (hereafter called electronic networks); 2) publication of illegal content over electronic media (e.g., child sexual abuse material or incitement to racial hatred); 3) crimes unique to electronic networks (e.g., attacks against information systems, denial of service and hacking).[29] This type of definition is more rigorous and appropriately scoped to apply given the dynamic nature of cyber threats.

However, the U.S. needs to amend the details of the European Commission's definition before adoption. First, the example, "incitement to racial hatred," provided under the second part of the definition implies that a restriction on free speech is lawful. The First Amendment to the U.S. Constitution guarantees the right to free speech; therefore, the example for the second portion of the definition should list "child sexual abuse material" only. Second, "computer systems and electronic networks" should replace "electronic communication networks and information systems" throughout the proposed definition of cyber crime to capitalize on the European Commission's recent adoption of an expanded meaning of "computer systems," which encompasses devices such as smart phones, tablets, and other forms of technology that produce, process, or transmit data.[30] Third, the definition of cyber crime should not use the word "attacks" because of legal implications that could invoke collective defense agreements like NATO's Treaty. In summation, the proposed definition now reads as follows: *cyber crime consists of 1) traditional forms of crime such as fraud or forgery, though in a cyber crime context relates specifically to crimes committed over computer systems and electronic networks; 2) publication of illegal content over electronic media (e.g., child sexual abuse material); 3) crimes unique to computer systems and electronic networks*

(e.g., intrusion of computer systems and electronic networks, denial of service and hacking). This revised definition is in line with the spirit of the original definition promulgated by the European Commission but on terms that abide by U.S. laws. The revised definition neatly complements the aforementioned Budapest Convention on Cybercrime, a treaty to which the U.S. signed and obligated itself. The Budapest Convention on Cybercrime provides more detail on cyber crimes such as offenses against the confidentiality, integrity, and availability of computer data and systems; forgery and fraud; child pornography; and infringements of copyright and related rights.

Unlike cyber crime, the definition of cyber war is not neatly defined or scoped by a similar "Budapest Convention on Cyber War" (no such convention exists), and significant controversy over the term cyber war exists. For instance, Howard Schmidt, the Cyber Czar for the Obama administration in 2010, questioned whether cyber war could exist and stated, "Cyber war is just something we can't define."[31] When General Alexander took command of U.S. Cyber Command in 2010, he said cyber war existed but he avoided defining the term. Information warfare, asymmetric warfare, electronic warfare, cyber crime, and cyber terrorism relate to cyber war, but those terms are either too broad or too narrow to appropriately define cyber war.

To construct a useful definition of cyber war that advances the end goals of clarifying jurisdictional issues and assisting the formulation of an appropriate response to an event, this paper considered the following definition from Richard Clarke and Robert Knake in their book, *Cyber War*, and another definition from the Institute for Security Technology Studies at Dartmouth College: 1) cyber war involves units organized along nation-state boundaries, in offensive and defensive operations, using

computers to attack other computers or networks through electronic means with the overall intent to seek advantage over an adversary by comprising the integrity, confidentiality, or availability of a computing device, and 2) actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.[32] The first definition starts to provide the detail necessary to align actions and roles of government agencies to properly prepare for and conduct cyber war. For consistency with terms used in the previously proposed definition of cyber crime, one should use “computer systems and electronic networks” when considering adoption of the first definition of cyber war. The second definition is more concise, but it implies offensive action and does not address specifically the issue of defensive actions. An amalgam of both definitions produces the following definition: *cyber war is offensive or defensive actions taken by a nation-state to penetrate or attack another nation-state’s computer systems or electronic networks for the purposes of causing damage or disruption*. This definition addresses offensive and defensive actions, differs from the definition of cyber crime because penetration of an enemy’s electronic network has a specific purpose of causing damage or disruption, and unambiguously introduces the term nation-state. The inclusion of the term nation-state will help differentiate cyber war from cyber terrorism.

Cyber terrorism is another cyber event that commonly gets used interchangeably with cyber crime and cyber war. One journalist puts the minimum number of magazine and journal articles written on cyber terrorism at 31,000.[33] Yet like cyber crime and cyber war, a widely accepted definition of cyber terrorism does not exist. The FBI defines cyber terrorism as the “premeditated, politically motivated attack against information,

computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents."[34] Dr. Dorothy Denning, from Georgetown University, provides a prolific definition found in the work of researchers and journals: “unlawful attacks or threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.” [35] She further states that the actions should result in violence against persons or property, or cause enough harm to generate fear.[36] By using the term, “computer,” both definitions run into the same minor faults of which previously proposed definitions in this paper were guilty. The term “premeditated” occurs in the FBI’s definition but not Dr. Denning’s definition. Premeditated applies to traditional terrorism, but cyber terrorism does not necessarily require detailed planning in the age of widespread computers, Internet access, and the immediacy of cyber space. The term “fear,” an intuitively important element of cyber terrorism, does not appear in the FBI’s definition like it does in Dr. Denning’s definition. Her definition does not specify actions or threats executed through the electronic network. A blend of these definitions produces the following definition: *cyber terrorism is a politically motivated attack or threat of attack using computer systems or electronic networks to intimidate, generate fear, or coerce a government or its people*. This definition is more concise and distinguishes cyber terrorism from cyber war by avoiding use of the word state or nation-state. The definition also specifies the motives of generating intimidation, fear, and coercion, further separating it from an act of cyber war.

By no means does the application or use of the three proposed definitions provide a silver bullet to fix inter-agency turf disputes or inefficiencies in cyber strategy. However, the subtle yet distinct differences between the proposed definitions of cyber crime, cyber war, and cyber terrorism serve to underpin the differences of roles and responsibilities between departments and institutions of the U.S. government. Disputes will continue to occur but adoption of the definitions will start to focus agencies on their primary roles.

Under the proposed definitions, DHS would still maintain overall responsibility for coordinating and orchestrating cyber defense. DoD, DoJ, and the Department of State (DoS) would play major supporting roles. As advocated in the introduction of this paper, DoD's primary responsibility should focus on cyber war. Within DoD, U.S. Cyber Command should focus on the execution of cyber war policy and strategy, and NSA should focus on the providing appropriate intelligence information to the department. How DHS and DoJ organize or assign sub-agencies, like the FBI and USSS, to tackle the issues of cyber crime and cyber terrorism is beyond the scope of this paper. DoS should employ diplomacy with other states to forge a consensus about the roles and responsibilities of states to help prevent cyber crime, cyber war, and cyber terrorism.[37]

The effectiveness of the U.S. government's cyber defense strategy, allocation of resources, and recognition of manpower and resource shortfalls are all reasons for the need to focus departments on cyber crime, cyber war, and cyber terrorism. Undoubtedly, some areas of cyber capabilities will overlap across cyber crime, cyber war, and cyber terrorism, but in today's environment of fiscal austerity, the U.S. government cannot afford excessive and duplicative spending. DoD needs to focus on

cyber war and get out of the business of being overly vigilant about cyber crime and cyber terrorism.

Previous paragraphs outlined the roles of the government in cyber strategy, but the role of the private sector is equally as important. The National Strategy to Secure Cyberspace states that a partnership between government and the private sector regarding cyber security is critical.[38] The partnership is necessary for a number of reasons. First, a significant amount of the country's cyber talent resides outside of government. The severe shortfall of cyber talent in DHS led to a DHS Cyber Skills Task Force report in the fall of 2012 that identified best practices to enable DHS to recruit and retain the cyber force it needs.[39] Second, the government needs the private sector to maintain standards of cyber capabilities to uphold a layered defense of the nation's infrastructure. The lack of cyber security legislation forces the government to rely on the private sector to *voluntarily* maintain minimum cyber defense capabilities. Third, the U.S. government needs the private sector's help to safeguard the privacy of the American people. In order to defend against cyber events, the U.S. government needs to share information with the private sector, and vice versa, without violating the privacy of American citizens. Privacy issues served as one of the stumbling blocks that prevented the passage of recent cyber security legislation. Having DHS in the lead of the government's cyber security allows for a level of transparency the American people expect in this area.[40] Until Congress passes legislation or the President issues an executive order regarding cyber security legislation, the government will face difficulty forging a long-lasting and functional partnership between government and the cyber

industry, facilitated by the Department of Homeland Security, to make cyberspace more secure.

Not only will the proposed definitions for cyber crime, cyber war, and cyber terrorism help establish a foundation for an effective strategy to make cyberspace more secure, but also the definitions will assist formulation of the mental framework by which the U.S. responds to cyber events. Granted, it is impossible to precisely or universally state a level to which the U.S. should respond to a cyber event, even if this paper assumed the highest level of classification. Publicly divulging rules of engagement would likely expose the U.S. to a deluge of cyber events that came just short of qualifying for required response. Of course, the U.S. always reserves the right *not* to respond in any situation. However, the definitions assist in development of an appropriate and proportional response to cyber crime, cyber war, and cyber terrorism.

The first response to consider using the proposed definitions is the response to cyber crime. For the most part, law enforcement deals with cyber incidents that fall into the cyber crime definition. DHS should exercise due diligence to apply resources to investigate and prosecute, in consultation with DoJ, cyber crimes using the existing legal framework. Cyber crimes would rarely, if ever, elicit a physical response from DoD. However, DHS should maintain dialogue and information exchanges with DoD to help identify trends, tactics, techniques, and procedures that cyber criminals use so that if the same type of events meet the definition of cyber war, DoD can respond from an informed perspective.

Responses to incidents that fall under the proposed definition of cyber war may or may not necessitate a DoD response. In consultation with DoJ and DHS using

applicable international law, DoD must provide the Commander-in-Chief with response options. Only the Commander-in-Chief can authorize a response. The difficulty of developing response options is astounding. As mentioned previously, the difficulty lies in acquiring sufficient confidence of attribution and determining the motivation behind an act of cyber war. Before responding, the U.S. must cross check to make sure the cyber event constitutes a "threat or use of force" as phrased in Article 2(4) of the U.N. Charter.[41] Under this paper's proposed definition of cyber war, however, personnel or property damage is a necessary element to constitute an act of cyber war. The damage also fulfills the "Just Cause" portion of *Jus ad Bellum* ('justice in going to war").[42] Unless the act of cyber war produced damage so minimal that the public was unable to recognize the damage, the government should refrain from acting as though the event did not happen or produced no damage. In any case, the U.S. should respond proportionally in accordance with *Jus in Bello* ("law during war") to gain acceptability of its wartime conduct.[43]

The decision process that goes into responding to an event that falls into the cyber terrorism definition could entail more difficulty than responding to an event that falls into the cyber war definition. If an act of cyber terrorism produces damage, the response process is identical to an act of cyber war. However, unlike an act of cyber war, an act of cyber terrorism does not have to produce physical damage. Therefore, on a case-by-case basis, the U.S. must consider what level of threat or fear necessitates a response to an act of cyber terrorism and whether the response satisfies *Jus ad Bellum*. The "state on state" guidance from Article 2(4) of the U.N. Charter might not apply perfectly to an act of cyber terrorism because a non-state actor could serve as the

aggressor. Nonetheless, the rules of proportionality apply and although cyber terrorism does not fall under the primary role of DoD, the U.S. can respond via DoD actions, if directed by the Commander-in-Chief and in accordance with *Jus in Bello*.

Whether speaking about cyber crime, cyber war, or cyber terrorism, answering questions about *Jus ad Bellum* and *Jus in Bello* is difficult. In 2009, the Vice Chairman of the Joint Chiefs of Staff asked, "What's proportionality look like in cyber? What does attribution look like in cyber? How do you understand sovereignty in the cyber domain?"[44] These questions remain unanswered in a universally acceptable manner, but this paper aims to propose definitions that underlie the answers to them. Application of the proposed definitions of cyber crime, cyber war, and cyber terrorism more clearly defines the role of DoD and frames appropriate responses.

Using the proposed definitions, clearly DoD is currently out of its cyber war lane. If the situation of DoD executing the roles of other departments of the government sounds familiar, it should. In 2007 during a speech to Kansas State University students, former Secretary of Defense Gates spoke about DoD's assumption of burdens that civilian agencies normally handled in the past, like building schools and mentoring city councils in Iraq and Afghanistan.[45] After making a joke about traveling halfway across the country to make a pitch to increase the budget of other agencies, he said civilian participation is necessary to making military operations successful and "having robust civilian capabilities available could make it less likely that military force will have to be used in the first place, as local problems might be dealt with before they become crises."[46] Admittedly, Secretary Gates was speaking about DoD's assumption of additional roles in a counterinsurgency environment. However, Secretary Gates's

remarks are equally applicable to today's volatile, uncertain, complex, and ambiguous cyber environment. DoD needs to focus on cyber war and let other civilian agencies and departments take the lead in cyber crime and cyber terrorism. DoD needs to stop protecting, and seemingly expanding, its turf to obtain cyber funding and to relax its requirement of "right to know and need to know" when dealing with the DHS and DoJ. DoD should keep in mind that the Secretary of Defense claimed DHS "has the lead for domestic cyber security," and then he said, "The Department of Defense also has a role. It is a supporting role."[47]

In summary, this strategy research paper proposed the following three definitions to rectify the lack of agreed upon definitions for common words that government and industry use on a routine basis. First, *Cyber crime* consists of 1) traditional forms of crime such as fraud or forgery, though in a cyber crime context relates specifically to crimes committed over computer systems and electronic networks; 2) publication of illegal content over electronic media (e.g., child sexual abuse material); 3) crimes unique to computer systems and electronic networks (e.g., intrusion of computer systems and electronic networks, denial of service and hacking). Second, *Cyber* war is offensive or defensive actions taken by a nation-state to penetrate or attack another nation-state's computer systems or electronic networks for the purposes of causing damage or disruption. Third, *Cyber terrorism* is a politically motivated attack or threat of attack using computer systems or electronic networks to intimidate, generate fear, or coerce a government or its people. Using the definitions, more distinct roles for government agencies and the civilian sector emerged. DHS retained the lead for overall domestic cyber security with support from DoD, DoJ, DoS, and the civilian sector. More

specifically, DoD assumed primary responsibility for cyber war, while DHS and DoJ executed primary responsibility for cyber crime and cyber terrorism. The proposed definitions permit DoD to focus on defending, deterring, disrupting, and defeating adversaries that conduct and prosecute cyber war against the U.S. and its allies. From a DoD perspective, the proposed definitions make intuitive sense as they allow DoD to extricate itself from cyber crime and cyber terrorism as much as possible while focusing on cyber war. The proposed definitions help to identify cost saving options by reducing or eliminating inefficient and duplicative capabilities throughout the government. Lastly, the proposed definitions also serve as an aid to decision makers as they work their way through the challenges of *Jus ad Bellum* and *Jus in Bello* when responding to cyber threats.

Endnotes

[1] Jared Serbu, "Air Force role just 1 piece of DoD's cyber puzzle," *Federal News Radio*, December 3, 2012, http://www.federalnewsradio.com/395/3140801/Air-Force-role-just-1-piece-of-DoDs-cyber-puzzle (accessed December 5, 2012).

[2] Sun Tzu, *The Art of War*, trans. Samuel Griffith (New York: Oxford University Press, 1963), 98.

[3] Kristin M. Finklea and Catherine A. Theohary, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement* (Washington, DC: U.S. Library of Congress, Congressional Research Service, July 20, 2012), available at http://www.fas.org/sgp/crs/misc/R42547.pdf (accessed December 12, 2012).

[4] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010), 77.

[5] Based on remarks by Rear Admiral Margaret Klein, U.S. Cyber Command's chief of staff, at the second annual U.S. Cyber Command Inter-Agency Legal Conference on September 18, 2012. Edited excerpts are available at http://www.military-information-technology.com/mit-home/445-mit-2012-volume-16-issue-9-october/6066-cyberspace-and-the-law.html (accessed December 5, 2012).

[6] "Daily Report: Cybersecurity Bill Stalls," *The New York Times*, November 15, 2012, available at http://bits.blogs.nytimes.com/2012/11/15/daily-report-cybersecurity-bill-stalls/ (accessed December 5, 2012).

[7] Janet Napolitano, "Homeland Threats and Agency Responses," *Congressional Record* (September 19, 2012), available at http://www.dhs.gov/news/2012/09/19/written-testimony-secretary-napolitano-senate-committee-homeland-security-and (accessed December 17, 2012).

[8] Leon Panetta, "Defending the Nation from Cyberattack," *Business Executives for National Security*, October 11, 2012, available at http://www.bens.org/document.doc?id=188&erid=20257 (accessed December 12, 2012).

[9] Kim Zetter, "DHS, Not NSA, Should Lead Cybersecurity, Pentagon Official Says," *Wired,* March 1, 2012, available at http://www.wired.com/threatlevel/2012/03/rsa-security-panel/ (accessed December 10, 2012).

[10] *The Federal Bureau of Investigation's Cyber Crime Page*, http://www.fbi.gov/about-us/investigate/cyber/cyber (accessed December 10, 2012).

[11] United Nations, *Charter of the United Nations: Chapter 1: Purposes and Principles*, http://www.un.org/en/documents/charter/chapter1.shtml (accessed December 10, 2012).

[12] North Atlantic Treaty Organization, "What is Article 5?" http://www.nato.int/terrorism/five.htm (accessed December 18, 2012).

[13] Jim Garamone, "Official Details DOD Cybersecurity Environment," *American Forces Press Service*, October 20, 2010, available at http://www.defense.gov/news/newsarticle.aspx?ID=61356 (accessed December 10, 2012).

[14] Declan McCullagh and Anne Broache, "Senate ratifies controversial cybercrime treaty," *cnet.com*, August 4, 2006, available at http://news.cnet.com/Senate-ratifies-controversial-cybercrime-treaty/2100-7348_3-%206102354.html (accessed December 12, 2012).

[15] Dan Robel, "International Cybercrime Treaty: Looking Beyond Ratification," *SANS Institute*, August 15, 2006, available at http://www.sans.org/reading_room/whitepapers/honors/international-cybercrime-treaty-ratification_1756 (accessed December 12, 2012); a list of signatories to the International Cybercrime Treaty is available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (accessed December 12, 2012).

[16] Panetta, "Defending the Nation."

[17] Ibid.

[18] Robert L. Mitchell, "After Stuxnet: The new rules of cyberwar," *Computerworld*, November 5, 2012, available at http://www.computerworld.com/s/article/9233158/After_Stuxnet_The_new_rules_of_cyberwar?taxonomyId=17&pageNumber=2 (last accessed December 12, 2012).

[19] Federal Bureau of Investigation, "The Cyber Threat: Part 1: On the Front Lines With Shawn Henry," March 27, 2012, http://www.fbi.gov/news/stories/2012/march/shawn-henry_032712/shawn-henry_032712 (accessed December 11, 2010).

[20] U.S. Department of Defense, *Strategy for Operating in Cyberspace*, July 2011, available at http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf (accessed December 12, 2012).

[21] James A. Lewis, "America is Under Attack: Why Urgent Action is Needed," Congressional Record (April 24, 2012), available at http://csis.org/files/ts120424_lewis.pdf (accessed December 12, 2012).

[22] Speech by James A. Lewis at Sasakawa Peace Foundation in Tokyo titled "Rethinking Cybersecurity – A Comprehensive Approach for Cyberwar," September 12, 2011, available at http://csis.org/publication/rethinking-cybersecurity-comprehensive-approach (accessed December 11, 2012).

[23] Ibid.

[24] Lisa Daniel, "DOD Needs Industry's Help to Catch Cyber Attacks, Commander Says," American Forces Press Service, March 27, 2012, available at http://www.defense.gov/news/newsarticle.aspx?id=67713, (accessed December 13, 2012).

[25] The Memorandum of Agreement between DHS and DoD is available at http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf (accessed December 13, 2012).

[26] For a more expansive look at the issues regarding Congressional cybersecurity legislation, see Paul Rosenzweig's "Issue Brief" at http://thf_media.s3.amazonaws.com/2012/pdf/ib3685.pdf (accessed December 13, 2012)

[27] Sarah Gordon and Richard Ford, "On the definition and classification of cybercrime," *Journal of Computer Virology*, vol. 2 (July 2006): 17.

[28] Clay Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* (Washington, DC: U.S. Library of Congress, Congressional Research Service, January 29, 2008), available at http://www.fas.org/sgp/crs/terror/RL32114.pdf (accessed December 13, 2012).

[29] Commission of the European Communities, "Towards a general policy on the fight against cyber crime," May 22, 2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF (accessed December 13, 2012).

[30] Alexander Seger, "Cooperation against cybercrime: Progress made in 2012," January 21, 2013, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Docs2013/cyber_AS_review2012_flyer_v5.pdf (accessed February 7, 2013).

[31] Sean Lawson, "General Alexander's Confirmation And The Failure of Cyberwar Transparency," *Forbes*, May, 13, 2012, http://www.forbes.com/sites/firewall/2010/05/13/general-alexanders-confirmation-and-the-failure-of-cyberwar-transparency/ (accessed December 13, 2012).

[32] Charles Billo and Welton Chang, Institute for Security Technology Studies at Dartmouth College, *Cyber Warfare: an analysis of the means and motivations of selected nation states*, November 2004, http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf (accessed December 11, 2012); Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010), 1.

[33] P. W. Singer, "The cyber terror boogeyman," *Armed Forces Journal*, November 2012, http://www.armedforcesjournal.com/2012/11/11530198 (accessed December 9, 2012).

[34] Mudawi Mukhtar Elmusharaf, "Cyber Terrorism: The new kind of Terrorism," April 8, 2004, http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism/ (accessed December 13, 2012).

[35] Dororthy E. Denning, "Cyberterrorism," Congressional Record (May 23, 2000), available at http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (accessed December 13, 2012).

[36] Ibid.

[37] Panetta, "Defending the Nation."

[38] George W. Bush, *The National Strategy to Secure Cyberspace*, (Washington, DC: The White House, February 2003), http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (accessed December 16, 2012).

[39] The DHS Cyber Skills Task Force report is available at https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf (last accessed December 13, 2012).

[40] Cheryl Pellerin "U.S. Leaders Cite Partnership as Key to Cybersecurity," American Forces Press Service, October 2, 2012, available at http://www.defense.gov/news/newsarticle.aspx?id=118074 (accessed December 13, 2012).

[41] United Nations, *Charter of the United Nations*.

[42] Martin L. Cook, "Ethical Issues in War: An Overview," http://www.au.af.mil/au/awc/awcgate/army-usawc/strategy2004/03cook.pdf (accessed December 18, 2012).

[43] Ibid.

[44] Jim Garamone, "Questions Abound in Cyber Theater of Operations, Vice Chairman Says," American Forces Press Service, June 9, 2009, available at http://www.defense.gov/news/newsarticle.aspx?id=54709 (accessed December 12, 2012).

[45] Robert M. Gates, “Landon Lecture (Kansas State University),” November 26, 2007, http://www.defense.gov/speeches/speech.aspx?speechid=1199 (accessed December 16, 2012).

[46] Ibid.

[47] Panetta, “Defending the Nation.”