Program Research Project

# On the Razor's Edge: Establishing Indistinct Thresholds for Military Power in Cyberspace

by

Lieutenant Colonel John A. Mowchan
United States Army

U.S. ARMY WAR COLLEGE
Prudens Futuri
Carlisle Barracks, PA

United States Army War College
Class of 2012

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

| | |
|---|---|
| **REPORT DOCUMENTATION PAGE** | *Form Approved*<br>*OMB No. 0704-0188* |

| | | |
|---|---|---|
| **1. REPORT DATE** *(DD-MM-YYYY)*<br>23-04-2012 | **2. REPORT TYPE**<br>Program Research Project | **3. DATES COVERED** *(From - To)* |

| | |
|---|---|
| **4. TITLE AND SUBTITLE**<br>On the Razor's Edge: Establishing Indistinct Thresholds for Military Power in Cyberspace | **5a. CONTRACT NUMBER**<br>**5b. GRANT NUMBER**<br>**5c. PROGRAM ELEMENT NUMBER** |
| **6. AUTHOR(S)**<br>Colonel John A. Mowchan | **5d. PROJECT NUMBER**<br>**5e. TASK NUMBER**<br>**5f. WORK UNIT NUMBER** |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**<br>Colonel (Retired) Robert Smith<br>Department of Distance Education | **8. PERFORMING ORGANIZATION REPORT NUMBER** |
| **9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**<br>U.S. Army War College<br>122 Forbes Avenue<br>Carlisle, PA 17013 | **10. SPONSOR/MONITOR'S ACRONYM(S)**<br>**11. SPONSOR/MONITOR'S REPORT NUMBER(S)** |

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

Distribution A: Unlimited

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

In the 21st century, the United States will increasingly rely on cyberspace to advance its national interests within a strategic environment characterized by volatility, uncertainty, complexity, and ambiguity. Concurrently, our adversaries are afforded increased opportunities to undermine our efforts by conducting a broad spectrum of nefarious activities in the digital domain. While not all of their acts will pose a direct and imminent threat to the nation's security, some will. Given these challenges, cyber strategists, government leaders, and scholars frequently disagree over whether the U.S. should establish thresholds (or red lines) for using military power when responding to hostile acts in cyberspace against government computer networks. This paper argues that delineating indistinct vice ambiguous or distinct red lines for hostile acts in cyberspace will better protect U.S. government networks and provide policymakers and military leaders ample flexibility to tailor response options in the same manner they are developed for threats in the other global domains.

**15. SUBJECT TERMS**

Cyberspace, Deterrence, Military Power, Cyber Threat and Response

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

USAWC PROGRAM RESEARCH PROJECT

# ON THE RAZOR'S EDGE: ESTABLISHING INDISTINCT THRESHOLDS FOR MILITARY POWER IN CYBERSPACE

by

Lieutenant Colonel John A. Mowchan
United States Army

Colonel (Retired) Robert Smith
Project Adviser

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

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

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

# ABSTRACT

AUTHOR: Lieutenant Colonel John A. Mowchan

TITLE: On the Razor’s Edge: Establishing Indistinct Thresholds for Military Power in Cyberspace

FORMAT: Program Research Project

DATE: 23 April 2012 WORD COUNT: 6,488 PAGES: 30

KEY TERMS: Cyberspace, Deterrence, Military Power, Cyber Threat and Response

CLASSIFICATION: Unclassified

In the 21st century, the United States will increasingly rely on cyberspace to advance its national interests within a strategic environment characterized by volatility, uncertainty, complexity, and ambiguity. Concurrently, our adversaries are afforded increased opportunities to undermine our efforts by conducting a broad spectrum of nefarious activities in the digital domain. While not all of their acts will pose a direct and imminent threat to the nation’s security, some will. Given these challenges, cyber strategists, government leaders, and scholars frequently disagree over whether the U.S. should establish thresholds (or red lines) for using military power when responding to hostile acts in cyberspace against government computer networks. This paper argues that delineating indistinct vice ambiguous or distinct red lines for hostile acts in cyberspace will better protect U.S. government networks and provide policymakers and military leaders ample flexibility to tailor response options in the same manner they are developed for threats in the other global domains.

# ON THE RAZOR'S EDGE: ESTABLISHING INDISTINCT THRESHOLDS FOR MILITARY POWER IN CYBERSPACE

The United States (U.S.) will increasingly rely on cyberspace to advance its national interests within a strategic environment characterized by increased volatility, uncertainty, complexity, and ambiguity.[1] Just as cyberspace provides the U.S. an enhanced ability to realize its security and economic interests, the nation's adversaries are also afforded increased opportunities to undermine our efforts by conducting a broad spectrum of nefarious activities in the digital domain. While not all of their acts will pose a direct and imminent threat to the nation's security, economic well-being, or social stability, some will. Because of this, cyber strategists, government leaders, and scholars frequently disagree over whether the U.S. should establish thresholds (or red lines) for employing military power in response to hostile acts in cyberspace against U.S. government computer systems and networks.

This paper argues that given the ever-evolving nature of cyberspace with a plethora of threat actors, U.S. interests are better served by delineating indistinct cyber red lines for the effective employment of the military instrument of national power. Indistinct red lines differ markedly from distinct or ambiguous thresholds in that they offer a broad framework for applying military power in a measured way while maximizing the deterrence effect against U.S. adversaries. Indistinct lines also provide policymakers sufficient flexibility to tailor response options in the same manner they are developed for threats in the other global domains. To support these assertions, the scope of this paper focuses exclusively on thresholds for employing military power in response to cyber attacks against U.S. government systems.

The structure of this paper is as follows: first, background information defines cyberspace, select cyber operations, and primary threat actors. A brief review of national-level cyberspace strategies then provide context for the employment of military power and the development of thresholds. Next, ample discussion brings to light key capabilities of the nation's Armed Forces, which sets the foundation for a thorough analysis of three red line frameworks (Distinct, Ambiguous and Indistinct). This paper concludes with a series of recommendations to senior political and military leaders.

## The Digital Domain Defined: Key Characteristics and Threat Actors

Defining cyberspace and identifying cyber threats is a challenging endeavor. Rapid technological changes continue to positively and negatively affect the physical and non-physical aspects of cyberspace causing this digital domain to evolve in many, often unpredictable ways. Cyberspace as the nation knew it in 1994 with dial-up access to the Internet is certainly not the cyberspace of 2012 with e-commerce, the Cloud, and Facebook. Additionally, the availability of advanced technologies and cyber tools, coupled with ease of access to cyberspace give state and non-state actors an enhanced ability to conduct a full range of malicious activities that threaten U.S. government systems and the overall security and economic well-being of the nation.

*Key Definitions*. For the purposes of this paper cyberspace is defined as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2] Other cyberspace-related definitions that help frame this paper include:

- **Computer network attack (CNA) or Cyber Attack.** CNA are actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.[3]

- **Computer network defense (CND).** CND are actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense (DoD) information systems and computer networks.[4]
- **Computer network exploitation (CNE).** CNE are enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.[5]
- **Cyber Deterrence.** The prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action in cyberspace outweighs the perceived benefits.[6]

*Threat Actors*. Threats to U.S. government computers and networks are diverse and growing. As the global community continues to become more digitally interconnected, a broad array of state and non-state actors will be afforded increased opportunity to conduct a full range of malicious activities.

State actors represent the greatest threat to government systems because they possess the necessary resources to acquire the most advanced technologies. Currently, there are over 100 foreign national intelligence organizations conducting operations in cyberspace, many of which target U.S. government networks.[7] Further complicating the situation, these intelligence services likely employ proxies to hide the identity of the responsible state. The most sophisticated threats stem from Russia and China, which continue to make significant advancements in their cyberspace capabilities. For example, in May 2011 China's Defense Minister announced the existence of an elite People’s Liberation Army (PLA) cyber unit called the Blue Army, which while focusing on cyber security likely has a robust offensive cyber warfare capability.[8] Separately, last year Russia’s Director for the Institute of Information

Security Issues at Moscow State University, who is also a member of Russia's National Security Council, admitted Russia is developing offensive cyber capabilities.[9]

Non-state actors include hackers, hacktivists, terrorists, and organized crime groups. Hackers are thrill-seeking individuals, who regard accessing secure computer networks as a challenge while hacktivists use cyberspace to protest or promote their political beliefs. Both usually don't possess the technical skills to attack effectively government networks; however, state actors, seeking to avoid attribution, could provide them with the necessary tools to degrade or damage U.S. government networks. For example, China's PLA has reportedly hired thousands of part-time hackers from the civilian population to target foreign government and corporate computer networks, including those in the United States.[10]

Terrorist organizations and organized crime groups also pose an increasing threat to U.S. government networks. According to Deputy Secretary of Defense William J. Lynn "...the greatest concern... is a terrorist group that gains the level of disruptive and destructive capability currently possessed by nation-states."[11] His concern is likely valid given that in 2010 terrorists with links to Al Qaida acknowledged this group had conducted offensive cyber operations, which included denial-of-service attacks against Israel.[12] Separately, organized crime groups, motivated by profit, could penetrate government networks to steal sensitive defense data and then sell it to U.S. adversaries. According to the Department of Justice (DoJ), "organized crime groups are becoming increasingly involved in cybercrime, which… creates risks to… government computer networks, and undermines worldwide confidence in the international financial system.[13] Taken together, state and non-state actors, given the proliferation of advanced information technologies and the low cost barrier to entry into cyberspace, pose a growing threat to U.S. government computer networks and subsequently, the security of the nation.

U.S. Cyberspace Strategies

To meet the emerging challenges in cyberspace, the U.S. in 2011 released two new national-level strategies for operating in the digital domain—the International Strategy for Cyberspace (ISC) and the DoD Strategy for Operating in Cyberspace (DSOC). The ISC is a landmark policy document that emphasizes a whole-of-government approach and international engagement to "promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, and strengthens international security."[14] While diplomacy is heavily emphasized, military power also plays a critical role as the ISC states...

> "When warranted, the U.S. will respond to hostile acts in cyberspace as we would to any other threat to our country. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values."[15]

In line with the ISC, the Defense Department published the DSOC, which acknowledges hostile cyber operations will be prevalent in any future conflict involving state or non-state actors. With this in mind, the strategy outlines five strategic initiatives. They are:

- Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential.

- Employ new defense operating concepts to protect DoD networks and systems.
- Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cyber security strategy.
- Build robust relationships with U.S. allies and international partners to strengthen collective cyber security.
- Leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation.[16]

While DoD's strategy is somewhat rudimentary (only 12 pages), it provides language that U.S. military power will be used if necessary stating "the Department… reserve[s] the right to defend vital national assets as necessary and appropriate."[17]

When considered holistically, the ISC and DSOC are generally ambiguous. Neither defines a hostile act in cyberspace nor is there language that explicitly states when, how, and to what extent the U.S. will respond to such acts. These strategies do acknowledge the inherent complexities of cyberspace where there are no simple, unitary solutions to the strategic challenges of the day. However, both do not specifically articulate the role of military power in a response leaving its employment open for consideration. Furthermore, the DSOC primarily focuses on the .mil domain giving lip service to cooperative efforts with other government agencies and the private sector.

## Military Power in Cyberspace

To employ military power effectively in response to a hostile act in cyberspace against government networks, one must understand the key lethal and non-lethal capabilities of the nation’s armed forces. Currently, U.S. Strategic Command (USSTRATCOM) is responsible for building DoD capacity and capabilities in cyberspace. U.S. Cyber Command (USCYBERCOM), under USSTRATCOM, “plans, coordinates, integrates, synchronizes, and directs activities to operate and defend DoD computer information systems and conducts full-spectrum military cyberspace operations to ensure U.S. freedom of action in cyberspace, while denying the same to our adversaries."[18] For simplicity, military power in response to hostile acts in cyberspace is divided into defensive and offensive capabilities.

*Defensive Military Power*. There are three key defensive capabilities. First, DoD has the capacity to surge CND operations to protect government computer systems. Currently, DoD via Army Forces Cyber Command (ARCYBER), 24th Air Force (AFCYBER), Fleet Cyber Command (FLTCYBERCOM), and Marine Forces Cyber Command (MARFORCYBER) can monitor, analyze, detect, and respond to unauthorized activity against .mil systems. Due to legal authorities under Titles 6, 10, 18, 44, and 50, these efforts extend minimally to other government agencies; however, some progress is being made as the Commander, USCYBERCOM, General Keith Alexander notes, "Cyber [security] is a team sport [and] DoD must work with other agencies as a team… to strengthen our public-private partnerships."[19]

Second, despite focusing primarily on military networks, DoD can also provide Defense Support to Civil Authorities (DSCA) to protect U.S. government computers in the .gov domain. In late 2011, the House Cybersecurity Task Force recommended that the federal government establish a "proactive process for DSCA as they relate to cyber and that DoD needed to better leverage technology transition mechanisms and training opportunities for the entire federal government."[20] For example, DoD can deploy Computer Emergency Response Team (CERTS) to assist other agencies bolster cyber defenses. DoD can also "provide technical assistance to gather and analyze information to characterize the attack and to gain attribution of the cyber threat, offer mitigation techniques, and perform network intrusion diagnosis."[21] However, to date these efforts have proven largely ineffective since current authorities and legal constraints prevent DoD from using all its capabilities to defend the .gov domain.

Third, with a lion's share of the intelligence budget, DoD possess a robust intelligence collection, processing, analysis, and dissemination capability. The co-location of USCYBERCOM with the National Security Agency gives it excellent access to time-sensitive intelligence on threat actors' illicit activities against government networks. Key here is that the timely sharing of cyber threat intelligence allows all government agencies to proactively bolster cyber defenses or modify operations to avert a breach in their network systems.

*Offensive Military Power*. There are three key offensive capabilities. First, DoD can conduct CNE against a cyber perpetrator to collect intelligence on the adversary's vulnerabilities or identify external technical support elements and financiers. This information could subsequently support follow-on lethal or non-lethal operations designed to degrade or destroy the adversary's cyber warfare capabilities. Additionally, this information could be used as evidence that allows the DoJ, in concert with the domestic and international law enforcement agencies, to arrest the perpetrators.

Second, DoD can, with appropriate authorization, conduct CNA against an adversary that initiates a cyber attack against U.S. government networks. Currently, DoD is developing offensive cyberweapons that will target a wide array of threat actors. These cyberweapons may eventually be able to "target offline military systems… by harnessing emerging technologies that use radio signal to insert coding into networks remotely."[22] Additionally, USCYBERCOM intends to deploy Cyber Support Elements

(CSEs) to each Geographical Combatant Command (GCC), which will purportedly "provide technical capability and expertise… to improve the integration of [DoD's] cyber attack capabilities."[23] Taken together, DoD is attempting to build its capacity to nullify an adversary's cyber attack and potentially proactively prevent future assaults against government networks before the exploits are initiated.

Third, the nation's armed forces can use kinetic force following a cyber attack. In line with the President's ISC, "DoD will ensure that the U.S. military continues to have all necessary capabilities in cyberspace to defend the United States and its interests, as it does across all domains."[24] For example, following a cyber attack that was attributed to a state actor, DoD could conduct cruise missile strikes, deploy special operating forces, or use unmanned drones against the adversary's cyber warfare command and control (C2) facilities to prevent it from conducting future attacks.

These military capabilities lead to several key observations. First, offensive military power is problematic because it can produce unexpected negative second- and third-order effects. For example, U.S. missile strikes against terrorists that also kill innocent civilians could elicit broad international condemnation, which may erode U.S. influence abroad. Such acts may also compel threat actors to form temporary alliances that allow them to leverage each other's strengths resulting in additional, more damaging attacks. Second, offensive military operations have the potential to escalate the situation. For example, a CNA against Iran could trigger a counter-counter attack from Tehran that includes kinetic-based strikes against U.S. military forces in the Middle East. Third, defensive power is less problematic and will not likely bring about negative repercussions. Defensive power also preserves the ability of the U.S. to conduct offensive military operations if warranted. Finally, as currently arrayed, DoD military power focuses almost exclusively on protecting the .mil domain. While DHS is charged with protecting the .gov domain, it currently does not possess the necessary resources and capacity to do so effectively.

### Threshold Options: Distinct, Ambiguous, Indistinct

Strategists, government leaders, and scholars frequently disagree over whether the U.S. should establish thresholds for employing military power following a cyber attack against U.S. government computer networks. Currently, there are three frameworks to consider.

*Distinct Thresholds.* Distinct thresholds for employing military power are specific, unambiguous statements that frame how the U.S. will respond to a hostile act in cyberspace against government networks. Delineating explicit thresholds in cyberspace via national strategies, policy documents, or Presidential speeches send a clear message to our adversaries that if you do “x” the U.S. will do “y” or “z” or both. Distinct thresholds are also narrowly focused and prescriptive in nature. For example, a distinct threshold may state the U.S. will employ kinetic military force against any non-state actor who conducts a cyber attack against government networks that kills three or more U.S. citizens. As a result, cyber actors, most particularly nation states, decide not to act out of fear of the potential consequences stemming from a military response that may include a kinetic component.

*Ambiguous Thresholds.* A diametrically opposed position for employing military power focuses exclusively on ambiguity in U.S. policies and strategies. Ambiguous red lines posit that if an adversary does “x” the U.S. may do “y” or “z”. Current U.S. policies and strategies like the ISC and DSOC contain ambiguous thresholds on employing military power. Both documents use the words “reserves the right” or “when warranted” that allude to the potential employment of military power following a cyber attack. The National Military Strategy for Cyberspace Operations is even more ambiguous asserting “DoD will execute the full range of military operations in cyberspace to defeat, dissuade, and deter threats against U.S. interests.”[25] Key here is that ambiguous thresholds do not explicitly state when and where military power will be employed. Furthermore, ambiguous thresholds are neither prescriptive in nature nor specifically frame how exactly offensive or defensive military power will be used, if at all.

*Indistinct Thresholds*. Indistinct thresholds differ from ambiguous and distinct red lines in three ways. First, indistinct thresholds are generally broad in nature but not too ambiguous so as to guide the employment of military power while maximizing the deterrence effect against U.S. adversaries. That is, indistinct red lines more clearly frame when military power will be used following a cyber attack. Second, unlike clearly delineated red lines, indistinct thresholds are not too narrowly focused or prescriptive, which helps to avoid automatic and frequently problematic triggers in the applications of military power. Third, indistinct thresholds rest on a singularly important premise that defensive military power will always be employed in preventing and responding to cyber attacks against U.S. government networks. That is, regardless of the perpetrator, the attack vector, the attack type, and the subsequent effects, defensive military power is always in play. Fourth, given the preceding characteristics, indistinct thresholds are tied almost entirely to the employment of offensive military power. Examples of indistinct thresholds include, but are not limited to the following examples:

1. The U.S. will always employ defensive military power to protect, respond to, and recover from hostile cyber attacks against U.S. government networks.
2. The U.S. will employ military power in a suitable and measured way as part of a whole-of-government response to any hostile cyber attack against government networks that results in…
    a. The death of U.S. citizens.
    b. The destruction or degradation of U.S. critical infrastructure and key resources.
    c. Penetration of classified government networks.
    d. Theft of sensitive, unclassified government data that could undermine U.S. national security.
    e. The theft of large sums of money that have the potential to negatively affect the nation's financial standing.

Threshold Analysis: Why Indistinct Thresholds are Optimal

Determining the optimal threshold approach is fraught with many challenges since each framework possesses several notable advantages. To guide a constructive analysis of all three frameworks, the following evaluation criteria are used: degree of ambiguity, flexibility to tailor response options, deterrence effect, response time, and risk.

*Distinct Thresholds.* Distinct thresholds that delineate when and how military power will be employed following a hostile cyber attack have several advantages. First and foremost, distinct thresholds eliminate ambiguity in U.S. strategies and policies, which can dramatically reduce the time it takes to respond to a cyber attack. Distinct thresholds in essence become an automatic trigger for employing military power, which can be advantageous in the cyber realm where adversaries move at light speed and can quickly disappear. Distinct thresholds also maximize the deterrence effect against

U.S. adversaries because cyber threat actors know there will be a military response. This reality directly affects an adversary’s strategic calculus whereby they believe that there is more to lose than gain for taking a specific action that may be deemed hostile to the target state. Representative Jim Langevin (D-R.I.) likely sees the advantages of clearly stated thresholds. Following the release of the DSOC, he asserted that the U.S. is too ambiguous with regard to how it will respond to cyber attacks. While the Congressman believes the DSOC and the ISC represented a good start, they were still deficient in several key areas including its fixation on the defense and the identification of acceptable red lines for a response in cyberspace.[26]

Despite these advantages, distinct thresholds have several inherent and problematic disadvantages. First, if distinct red lines are established, then the U.S. will be compelled to act every time a threat actor crosses that line, which it cannot realistically do since U.S. government networks are subjected to millions of probes, scans, and attacks on a daily basis and there are not enough resources to respond effectively. In addition, distinct, clearly articulated thresholds may give cyber threat actors a green light for certain illicit acts that do not cross a red line. While one nefarious act below this threshold may not be harmful to government networks, what if 100 million are? Next, because cyberspace is a global domain that emphasizes open access, the free flow of information, and anonymity, it is extremely difficult to attribute responsibility for a hostile act. As a result, a majority of these perpetrators are never identified, less a computer IP address or a one-time user alias. When thinking about attribution, General Alexander, highlighted this challenge saying “too often, the military discovers through forensics that network probes have been successful [and] as a consequence, response becomes policing up after the fact versus mitigating it real time."[27] If distinct red lines demand a timely response and there is no one to pin responsibility on, then how can a response be implemented?

Finally, even if attribution is acquired in a timely manner, automatic triggers for a response, particularly those that employ military force, could create negative second and third-order effects that make a bad situation even worse. Given nation states pose the greatest threat to U.S. networks, thresholds that automatically result in a kinetic response could escalate an already volatile situation. For example, if Russia and/or China, two nuclear powers, were found responsible for a cyber attack that killed U.S. citizens, a lethal-based counter attack could elicit a similar if not stronger counter-counter attack that may eventually result in the use of nuclear weapons if the situation were to spiral out of control. Clearly the diplomatic, information, and economic instruments of national power vice military force would receive more emphasis with

When weighing the advantages and disadvantages, establishing distinct thresholds carries a high degree of operational risk. Automatic triggers that set in motion offensive military power against a state or non-state actor can escalate a crisis thereby requiring the commitment of additional military forces to safeguard U.S. interests. Establishing a long laundry list of distinct thresholds could minimize this risk; however, since not every situation following a cyber attack against government systems can be adequately predicted, such thresholds could in the end constrain t

he application of military power.

*Ambiguous Thresholds.* Ambiguous thresholds offer several advantages for employing military power following a hostile cyber attack against government networks.

First, not establishing red lines allows government leaders the flexibility to tailor response options based on the hostile act, the perpetrator (state or non-state), its effects in the physical and digital world, and how they relate to the current state of affairs in the international system. As such, the employment of military power against a state-based threat would be much different than one against a non-state actor that conducted the same type of attack thus validating the necessity for ambiguous thresholds. For example, in 2009 individuals in China and Russia penetrated computer networks that operate parts of the U.S. electrical power grid.[28] These individuals reportedly inserted malware that could destroy infrastructure components. Although the identities of the perpetrators or their associations with the Russian and Chinese governments were not disclosed, it validates the point that response options must be tailored since a response against hackers or hacktivists would be different from a response against the Chinese or Russian governments.

A second advantage is that the U.S. does not disclose all facets of its strategy to its adversaries. If cyber threat actors know what the U.S. will do in response to particular hostile acts in cyberspace, they will adjust their strategic approaches, modify their doctrine, and develop new cyber tactics, techniques or procedures that skirt the red line. Because neither the national nor the defense strategy for cyberspace explicitly defines a hostile act in cyberspace or how exactly the U.S. will respond, this leaves it open to interpretation. In 2009 General Kevin Chilton, Commander U.S. Strategic Command, stated, "I don’t think you take anything off the table when you provide [response] options to the president. Why would we constrain ourselves on how we would respond [to hostile acts in cyberspace]?"[29] Such an approach is no different than how the U.S.

addresses hostile acts in the other global domains. Hostile actions in cyberspace should be no different.

Finally, ambiguous thresholds keep the adversary guessing on how the U.S. will respond. As was brought out by one unidentified military official, "If you shut down our power grid, maybe we will put a missile down one of your smokestacks,"[30] Again, ambiguity in when, how, and to what extent to use military power gives political and military leaders maximum latitude in developing a response.

There are three key disadvantages to ambiguous thresholds. First and foremost, there are no overarching guidelines that steer offensive or defensive military power following a hostile cyber attack against government networks. Without some discernable guideposts for using military power, there is increased risk that the nation's military capabilities will stand idle thereby making government networks more susceptible to attack. Senator John McCain understands this risk when he wrote a letter to General Alexander on 29 March 2012 stating "I am deeply concerned by your [General Alexander] endorsement of the Administration's proposal to appoint the Department of Homeland Security (DHS) as the lead agency responsible for ensuring domestic security against cyber attacks and that I do not understand why DHS can more effectively protect our nation's critical infrastructure better than USCYBERCOM."[31] Senator McCain clearly realizes not only the inadequacy of DHS to protect government networks but the failure of DoD to use its capabilities in the same endeavor.

Second, with ambiguous thresholds, the time it takes to respond effectively with military power will be greatly increased allowing cyber adversaries to escape. Building on Senator McCain's comments in the preceding paragraph, one of the most significant challenges for the interagency (IA) will be determining which government organization is the lead federal agency (LFA). This is no simple feat since there is much confusion about whether a cyber attack against government computers is a crime or act of war. If it is a crime, perhaps the DoJ or DHS will be the lead. If it is an act or war, DoD would lead.

Third, ambiguous thresholds, because they lack clarity, could erode U.S. public confidence in the government to protect its citizens from cyber attacks. Critics of ambiguous policies and strategies like the ISC and DSOC argue the U.S. is taking ambiguity too far. Now retired General James Cartwright, the former Vice Chairman of the Joint Chiefs of Staff may have recognized the benefits of being less ambiguous with respect to our offensive approach in cyberspace. Following the release of the DSOC, he remarked the strategy was too defensive stating “we are supposed to be offshore convincing people if they attack, it won’t be free…[and that] disabling computerized patient records at a hospital such that the patients cannot be treated would be a violation of the law of armed conflict… [which could] then [trigger a] …proportional response.”[32] General Cartwright went on to emphasize the nation will need stronger deterrents. Although he did not articulate what deterrents should be or what instruments of national power would be used, his words lend support for greater specificity in U.S. policies, greater clarity on what is a hostile act in cyberspace, and thresholds that signal U.S. resolve to act.

Ambiguous thresholds as articulated in current U.S. policy and strategy represent a positive step forward in framing the potential use of military force in response to hostile cyber attacks; however, such an approach is too ambiguous and therefore problematic given the noted disadvantages. Additionally, there exists an unacceptable level of force management risk where military power has the potential to stand idle in the face of a large-scale cyber attack against U.S. government networks. Given current authorities and DoD's primary emphasis on the .mil domain, it is plausible U.S. military power could not be brought to bear in defense of the .gov domain or in an offensive manner against the perpetrator. As a result, the entire Federal Government and the nation remain at risk and vulnerable to cyber attack.

*Indistinct Thresholds.* The establishment of indistinct thresholds for employing military power in U.S. national strategies affords the nation a marked advantage over the current construct (ambiguity) or any approach that gravitates toward distinct thresholds. Four reasons support this assertion. First, indistinct thresholds convey to the American public and the nation's enemies that the full gamut of U.S. military capabilities will "defend the United States against all adversaries and serve the Nation as a bulwark and the guarantor of its security and independence"[33] in all the domains, including cyberspace. More importantly, indistinct thresholds convey the U.S. <u>will</u> use military power in response to hostile acts against <u>all</u> government networks; however, they do not explicitly state how and to what extent military power will be employed. From one perspective, measured ambiguity via indistinct thresholds strikes an appropriate balance between complete ambiguity and distinct red lines. The net benefit here is all government networks are more adequately protected, the American public reassured, and deterrence maximized because the nation's adversaries know there will be a price to be paid for their nefarious acts.

Second, indistinct thresholds do not disclose fully all facets of U.S. cyber strategies. While indistinct thresholds guide the employment of military force, measured ambiguity will certainly keep the adversary guessing on how the U.S. will exactly respond militarily. An extremely important corollary here is that senior political and military leaders are still afforded flexibility to tailor how military power will be employed. For example, a cyber attack by a terrorist cell that kills one, ten or 100 U.S. citizens will trigger the employment of military power; however, political and military leaders decide how such power is fused into a whole-of-government response. In one instance, (e.g. the death of a single U.S. citizen), military power via CNE may provide intelligence that leads to the arrest of cell members. In another case where ten citizens die, perhaps CNA against the group's computers and intelligence (derived from CNE) sharing lead to the take-down of the cell by host-nation law enforcement.

Third, the time for a military response is decreased significantly because there are clearly understood lines that trigger action by DoD and the interagency. Given military power will always have a role in a whole-of-government response removes or at least minimizes the "debate" that often accompanies IA deliberations on the military's role. While IA discussions on using offensive military power will certainly still need to occur, knowing the military's defensive power will be automatically employed will bolster cyber defenses, minimize the adversary's cyber attack, and ensure networks recover more quickly thereby lessening the damage. In essence, indistinct thresholds help to streamline the IA process ensuring the timelier and effective application of the military instrument of national power following a cyber attack against government networks.

Fourth, in a resource constrained environment, indistinct thresholds for employing military power can better align finite DoD resources with national priorities to protect government networks from cyber attacks. Currently, ambiguous thresholds are open to interpretation and risk misaligning monies to lower priorities. Meanwhile, distinct thresholds are too narrow and risk wasting monies on priorities that are no longer at the top of the list. Although indistinct thresholds frame the application of offensive military power, emphasis is given to the defense. As Martin Libicki notes, “the best defense [in cyberspace] is not necessarily a good offense; it is usually a good defense.”[34]

Critics would argue that indistinct thresholds are no better than the current approach (e.g. ambiguous thresholds) or an approach that focuses on creating distinct thresholds. Proponents of ambiguous thresholds would argue that any attempt to add clarity to response thresholds is untenable and could undermine U.S. credibility. For example, if an indistinct threshold states the U.S. will use military power to respond to a cyber attack that kills U.S. citizens, the first time this does not happen it will signal that U.S. does not mean what it says thereby diminishing the deterrence effect of the nation’s other capabilities. Meanwhile, pundits for unambiguous thresholds would argue that indistinct thresholds don’t go far enough in framing how military power will be used and that responses will eventually succumb to “red tape” in the IA leading to a time-late response. Both counterarguments are invalid because they fail to acknowledge that “defensive” military power <u>is always in play</u> and that regardless of the situation, DoD, either as the LFA or in support, can provide intelligence, bolster cyber defenses or deploy some other form of defensive power following the incident. While the nation or its adversaries may not overtly see its application because of classification restrictions, The overarching conclusions presented above make it clear that neither distinct nor ambiguous thresholds for employing military power are optimal for the U.S. today. Both approaches fall short in many respects and more importantly, fail to acknowledge that the world is neither black nor white but various shades of grey. Given this reality, the U.S. needs a different framework—one that fuses the positive aspects of distinct and ambiguous thresholds into a more balanced approach that allows for the timely, tailored, effective, and measured application of military power. As such, the U.S. will be better served in the long-run by establishing indistinct thresholds for employing military power in response to hostile acts in cyberspace against U.S. government networks.

In the 21st Century, the U.S. will increasingly rely on cyberspace to advance its national interests. Given the preceding analysis and to ensure the government is properly positioned to employ military power in response to hostile acts against government networks, senior political and military leaders should enact the following recommendations.

*1. Establish indistinct response thresholds to cyber attacks.* Delineating indistinct cyber red lines, such as the ones articulated in this paper, for the effective employment of the military instrument of national power in U.S. policies and strategies will increase the deterrence effect against current and future adversaries. Additionally, when employing the military instrument of national power, national leaders are permitted ample flexibility to tailor timely response options in the same manner they are developed for threats in the other global domains.

*2. Focus on defensive military power.* Although offensive cyberweapons and the kinetic force may be required, their application is problematic and could make a bad situation worse. Because of this, the U.S. government should devote more budgetary allocations to defensive cyber security efforts. For instance, of the $3.4 billion DoD is seeking in fiscal year 2013[35], devoting approximately 75 percent towards defense will help ensure networks have the necessary resiliency and ability to detect an intrusion before it penetrates government systems. Maintaining a strong defense also allows other instruments of national power to take precedence over military options thereby minimizing the risk associated with using offensive military power. This defensive focus applies not only to DoD but the entire Federal Government.

*3. Expand DoD responsibility in the .gov domain.* The overarching mission of the United States Armed Forces is to protect and defend the nation against all enemies. Current authorities constrain DoD's ability to accomplish fully this vitally important mission. By updating authorities to allow DoD an increased role in defending the .gov network will better secure not only government networks but the entire nation. Admittedly, the U.S. public may perceive this as the militarization of cyberspace and a threat to civil liberties; however, given the global interconnectivity of government, public, and private networks in cyberspace, employing the full range of the nation's military capabilities to protect the nation and its citizens is an imperative that cannot be comprised.

*4. Increase cyber intelligence operations.* Given the nation's growing reliance on cyberspace and the increased number of state and non-state actors, the Intelligence Community (IC) must increase intelligence operations designed to identify emerging cyber threats to government networks. While emphasis should be devoted to indications and warning, the IC must do a better job of sharing classified intelligence with all stakeholders, especially those that do not have mature classified networks. This is best accomplished by quickly declassifying intelligence and “pushing” timely and relevant classified information vice waiting for a request from another government agency on a cyber threat that probably has already penetrated the system. This proactive approach improves cyber defenses and allows political leaders to enact decisions on cyberspace in a timelier manner. Furthermore, it allows military leaders to develop appropriate, measured options for employing military power, prior to an adversary's cyber attack.

### Future Research

Given the ever-evolving nature of cyberspace and the rather narrow focus of this paper, there is ample opportunity for continued research on this topic. Not fully considered is DoD’s role in protecting private networks from cyber attacks and the accompanying concerns over civil liberties. From an organizational perspective, the use of military power and DoD’s leading role in protecting all government networks calls into question DHS responsibilities for cyber security.

### Conclusion

The 21st century strategic environment will become more and more grey owing to globalization and the impact cyberspace has on the dynamic interplay of political, economic, religious, and social factors in the international system. With a multitude of threats facing the U.S. both in the physical and digital realm, measured ambiguity via indistinct thresholds can serve as a powerful tool to shape the actions of U.S. adversaries in cyberspace. By establishing indistinct thresholds, the U.S. can bolster deterrence and give the nation’s leaders enough latitude to tailor effectively how and when military power will be employed following a hostile act against government networks in cyberspace.

## Endnotes

[1] This PRP represents an expansion of previously published paper on the topic of establishing thresholds for responding to hostile acts in cyberspace against the United States. Some of the concepts, ideas, sources, and text presented in this paper are that of the authors from the following source: Lieutenant Colonel John A. Mowchan, "Don't Draw the [Red] Line," *Proceedings*, October 2011, 16-20.

[2] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military Terms,* Joint Publication 1-02, (Washington, DC: U.S. Joint Chiefs of Staff, 08 November 2010 (As amended through 15 February 2012)), 83.

[3] U.S. Joint Chiefs of Staff, *Information Operations,* Joint Publication 3-13, (Washington, DC: U.S. Joint Chiefs of Staff, 13 February 2006), GL-5.

[4] Ibid, GL-5

[5] Ibid, GL-6

[6] U.S. Joint Chiefs of Staff, *Joint Operations,* Joint Publication 3-0, (Washington, DC: U.S. Joint Chiefs of Staff, 11 August 2011), V-10.

[7] Deputy Secretary of Defense William J. Lynn III speech at USAF-Tufts Institute for Foreign Policy Analysis Conference, 21 January 2010, 3.

[8] Zhang Jiawei, "China Confirms Deployment of Online Army," *China Daily*, May 26, 2011, http://www.chinadaily.com.cn/china/2011-05/26/content_12583698.htm, accessed 16 July 2011.

[9] Kathryn Stevens and Larry K. McKee Jr., "International Cyberspace Strategies," Improving the Future of Cyberspace...Issues, Ideas, Answers, June 28, 2010, 8.

[10] "George H. Wittman, "China's Cyber Militia," *The American Spectator*, 21 October 2011, http://spectator.org/archives/2011/10/21/chinas-cyber-militia, accessed 07 January 2012.

[11] RSA 2011: Terrorist groups pose most dangerous cyber threat, *Info Security Online*, 16 February 2011, http://www.infosecurity-us.com/view/16005/rsa-2011-terrorist-groups-pose-most-dangerous-cyber-threat/, accessed 21 July 2011.

[12] Alex Kingsburg, "Documents Reveal Al Qaeda Cyberattacks," *U.S. News and World Report Online*, 14 April 2010, http://www.usnews.com/news/articles/2010/04/14/documents-reveal-al-qaeda-cyberattacks, accessed 01 August 2011, 2.

[13] Lanny A. Breuer, "Statement of Assistant Attorney General Lanny A. Breuer before the Senate Judiciary Subcommittee on Crime and Terrorism," 01 November 2011, http://www.justice.gov/criminal/pr/testimony/2011/crm-testimony-111101.html, accessed 04 April 2012.

[14] Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011), 8.

[15] Ibid, 14

[16] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, (Washington DC: U.S. Department of Defense, July 2011), 5-10.

[17] Ibid, 10.

[18] U.S. Strategic Command, "Fact Sheets: U.S. Cyber Command," http:/ /www.stratcom.mil/factsheets/Cyber_Command/, accessed 13 March 2012.

[19] Donna Miles, “Alexander cites need for greater cyber defense,” *American Forces Press Service*, 13 September 2011, http://www.defense.gov/news/newsarticle.aspx?id=65321, accessed 04 April 2012.

[20] Representative Robert Aderholt and others, “Recommendations of the House Republican Cybersecurity Task Force,” 05 October 2011, 16.

[21] Department of Homeland Security (DHS), National Cyber Incident Response Plan (NCRIP), Interim Version, September 2010, C-2.

[22] Ellen Nakashima, “Pentagon Ups Ante on Cyber Front,” *Washington Post*, 19 March 2012, 1.

[23] Zachary Fryer-Biggs, “U.S. Military Goes on Cyber Offensive,” *Federal Times*, 26 March 2012, http://www.federaltimes.com/article/20120326/DEPARTMENTS01/203260301/, accessed 26 March 2012.

[24] Department of Defense, “DoD Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November 2011, 9.

[25] U.S. Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations*, (Washington, DC: U.S. Joint Chiefs of Staff, December 2006), 2.

[26] Ellen Nakashima, “U.S. Cyber Approach ‘Too Predictable’ for One Top General,” Washington Post, July 14, 2011, http://www.washingtonpost.com/national/national-security/us-cyber-approach-too-predictable-for-one-top-general/2011/07/14/gIQAYJC6EI_story.html, accessed 15 July 2011.

[27] William Mathews, “CyberCom: U.S. Lacks Online Situational Awareness,” *Defense News*, 03 June 2010, http://www.defensenews.com/story.php?i=4655216, accessed 01 August 2011.

[28] Siobahn Gorman, “Electricity Grid in U.S. Penetrated by Spies, *Wall Street Journal*, April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html, accessed 02 August 2011.

[29] Robert Lemos, “Cyber attack could bring US military response-No options removed from table,” *The Register Online,* 13 May 2009, http://www.theregister.co.uk/2009/05/13/us_cyber_attack_response/, accessed 12 August 2011.

[30] Chris Carroll, “DoD: Cyberattack on U.S. could warrant deadly response,” *Stars and Stripes*, May 31, 2011, http://www.stripes.com/news/dod-cyberattack-on-u-s-could-warrant-deadly-response-1.145183, accessed 01 August 2011.

[31] Senator John McCain, “Letter to General Keith B. Alexander, 29 March 2012,” United States Senate, Committee on Armed Services, Washington D.C. 20510, 1.

[32] Ibid

[33] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States,* Joint Publication 1, (Washington, DC: U.S. Joint Chiefs of Staff, 02 May 2007 (Incorporating Change 1, 20 March 2009)), i.

[34] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, RAND Project Airforce (Santa Monica, CA: RAND Corporation, 2009), 176.

[35] Nakashima, 2.