UNITED STATES
ARMY WAR COLLEGE
PRESS
Carlisle Barracks, PA
STRENGTH ~ WISDOM

DISTINGUISHING ACTS OF WAR IN CYBERSPACE: ASSESSMENT CRITERIA, POLICY CONSIDERATIONS, AND RESPONSE IMPLICATIONS

Jeffrey L. Caton

U.S. ARMY WAR COLLEGE
SSI
STRATEGIC STUDIES INSTITUTE

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations, and Response Implications	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Strategic Studies Institute,47 Ashburn Drive,Carlisle,PA,17013-5010**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**117**	

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

SSI
STRATEGIC STUDIES INSTITUTE

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

CSLD
CENTER for STRATEGIC LEADERSHIP and DEVELOPMENT
U.S. ARMY WAR COLLEGE

The Center for Strategic Leadership and Development contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

PKSOI

The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.

U.S. Army War College
SLDR
Senior Leader Development and Resiliency

The Senior Leader Development and Resiliency program supports the United States Army War College's lines of effort to educate strategic leaders and provide well-being education and support by developing self-awareness through leader feedback and leader resiliency.

SCHOOL OF STRATEGIC LANDPOWER
U.S. Army War College

The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.

The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE

The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

Strategic Studies Institute
and
U.S. Army War College Press

DISTINGUISHING ACTS OF WAR IN CYBERSPACE: ASSESSMENT CRITERIA, POLICY CONSIDERATIONS, AND RESPONSE IMPLICATIONS

Jeffrey L. Caton

October 2014

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5010.

*****

This manuscript was funded by the U.S. Army War College External Research Associates Program. Information on this program is available on our website, *www.StrategicStudies Institute.army.mil*, at the Opportunities tab.

*****

*****

The Strategic Studies Institute and U.S. Army War College Press publishes a monthly email newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on the SSI website at *www.StrategicStudiesInstitute.army.mil/newsletter.*

ISBN 1-58487-643-3

FOREWORD

Currently, there is no internationally accepted definition of when hostile actions in cyberspace are recognized as attacks, let alone acts of war. The goal of this monograph is to provide senior policymakers, decisionmakers, military leaders, and their respective staffs with essential background on this topic as well as to introduce an analytical framework for them to utilize according to their needs.

The examination canvasses existing decisionmaking policies, structures, and influences to provide a holistic context for the assessment that extends beyond limits of the legal and technical communities. Its approach focuses on the synthesis and integration of material from existing experts, deferring the detailed analysis to the many published studies.

Such broad coverage of many complex issues necessarily requires simplification that may negate certain nuances expected by experienced professionals in those fields; but it is hoped that readers understand these limitations. The purpose is not to prescribe or dictate a specific methodology of assessment; rather, it is to introduce decisionmakers and their staffs to a portfolio of options built around the concepts of characterization, assessment criteria, policy considerations, and courses of action consequences.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
U.S. Army War College Press

ABOUT THE AUTHOR

JEFFREY L. CATON is President of Kepler Strategies LLC, Carlisle, PA, a veteran-owned small business specializing in national security, cyberspace theory, and aerospace technology. He is also an Intermittent Professor of Program Management with the Defense Acquisition University. From 2007 to 2012, Mr. Caton served on the U.S. Army War College faculty, including as Associate Professor of Cyberspace Operations and Defense Transformation Chair. Over the past 5 years, he has presented lectures on cyberspace and space issues related to international security in the United States, Sweden, the United Kingdom, Estonia, and Kazakhstan, supporting programs such as the Partnership for Peace Consortium and the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Center of Excellence. His current work includes research on cyberspace and space issues as part of the External Research Associates Program of the Strategic Studies Institute, as well as serving as a facilitator for Combined/Joint Land Force Component Commander courses at the Center for Strategic Leadership and Development. He served 28 years in the U.S. Air Force, working in engineering, space operations, joint operations, and foreign military sales, including command at the squadron and group level. Mr. Caton holds a bachelor's degree in chemical engineering from the University of Virginia, a master's degree in aeronautical engineering from the Air Force Institute of Technology, and a master's degree in strategic studies from the Air War College.

SUMMARY

The monograph is comprised of four main sections:

- Characterization. This section provides the notional foundation necessary to avoid any devolution of the analysis to mere semantic arguments. It presents how cyberspace is defined and characterized for this discussion, as well as how this compares to existing concepts of the traditional domains of land, sea, air, and space. Also, it identifies some of the unique technical challenges that the cyberspace domain may introduce into the process of distinguishing acts of war.
- Assessment Criteria. This section explores the de jure and the de facto issues involved with assaying cyber incidents to determine if they represent aggression and possible use of force; and, if so, to what degree? It reviews the traditional legal frameworks surrounding military action to include the United Nations (UN) Charter and the Law of Armed Conflict. It also examines how these compare to the recently published Tallinn Manual on the International Law Applicable to Cyber Warfare. From these sources, it proposes a cyberspace incident assessment methodology.
- Policy Considerations. Having identified viable criteria to aid with the assessment of cyber-space incidents, this section looks at the policy considerations associated with applying such principles. First, it examines the relevant U.S. strategies; next, it investigates the strategies of other key countries and international organizations and how they compare to U.S. tenets; and finally, it evaluates how nonstate actors may affect U.S. deliberations.

- Courses of Action. This section examines the influences that course of action development and implementation may have on the assessment of cyberspace incidents. It first looks at the President's role as the primary decisionmaker in U.S. national matters regarding cyber-space. It then surveys key influences affecting subordinate decisionmakers and their staffs that may be advising the Commander-in-Chief: reliable situational awareness, global and domestic environment considerations, and options and their related risks and potential consequences.

Any reader expecting a perfect solution for this conundrum will be disappointed, as the examination is more about the journey than the destination. In the end, many of the challenges with this issue are common with those of the traditional domains; however, the complex and dynamic character of the cyberspace domain introduces unique vexations for senior policymakers and decisionmakers.

The conclusion of this monograph includes recommendations that the author hopes will aid in the positive evolution toward a better understanding and mitigation of the fog and friction surrounding the distinction of acts of war in cyberspace.

DISTINGUISHING ACTS OF WAR IN CYBERSPACE: ASSESSMENT CRITERIA, POLICY CONSIDERATIONS, AND RESPONSE IMPLICATIONS

Currently, there is no internationally accepted definition of when hostile actions in cyberspace are recognized as attacks, let alone acts of war. The goal of this monograph is to provide senior policymakers, decisionmakers, military leaders, and their respective staffs with essential background on this topic as well as introduce an analytical framework for them to utilize according to their needs. The examination canvasses existing decisionmaking policies, structures, and influences to provide a holistic context for the assessment that extends beyond limits of the legal and technical communities. Its approach focuses on the synthesis and integration of material from existing experts, deferring the detailed analysis to the many published studies. Such broad coverage of many complex issues necessarily requires simplification that may negate certain nuances expected by experienced professionals in those fields. The author respectfully requests that readers understand these limitations. The purpose is not to prescribe or dictate a specific methodology of assessment; rather, it is to introduce decisionmakers and their staffs to a portfolio of options built around the concepts of characterization, assessment criteria, policy considerations, and courses of action consequences.

CHARACTERIZATION

This section provides the notional foundation for the dialogue on this issue necessary to avoid any devolution of the analysis to mere semantic arguments. It presents how cyberspace is defined and characterized for this discussion, as well as how this compares to existing concepts of the traditional domains of land, sea, air, and space. Also, it identifies some of the unique technical challenges that the cyberspace domain may introduce into the process of distinguishing acts of war.

Assessment Context.

The popular concept of an "act of war" is that of a single event or incident of violence and aggression that could justifiably drive one nation to legally declare war on another. In a November 2011 report to Congress, the Department of Defense (DoD) termed an act of war simply as "an act that may lead to a state of ongoing hostilities or armed conflict,"[1] and it is this definition that is used for this monograph.

*Acts of War and the Military Domains***.**

On October 11, 2012, then Secretary of Defense Leon Panetta warned of a possible "cyber Pearl Harbor" during a speech in New York City, repeating a warning that has floated around the Washington, DC, area from more than 2 decades. In reporting this event, a *Washington Post* article asserted that "we all know what an act of war looks like on land or sea," implying that distinguishing acts of war in the traditional domains is a simple matter. Certainly, there

are clear cut historical examples such as Pearl Harbor (for the air and sea domains) and the 1990 invasion of Kuwait by Iraq (for the land domain) that would support this view. But what other, perhaps lesser, actions by one nation against another constitute acts of war? What are the thresholds of force and violence for this distinction, and are they universally recognized? The same article later concedes that "deciding what amounts to an act of war is more a political judgment than a military or legal one" and noted incidents such as the 1979 attack and seizure of the U.S. Embassy in Tehran did not cause the United States to go to war.[2] Noted author Thomas Rid observes that this is consistent with the Clausewitzian concept of war as a continuation of politics by other means and he posits that "any act of war has to have the potential to be lethal; it has to be instrumental [i.e., have clear means and ends]; and it has to be political."[3]

For the time being, let us assume we can distinguish acts of war in cyberspace using the same criteria and analysis used to determine war in the traditional domains. How do we characterize this new domain? A simplified model of cyberspace offered by information warfare expert Dr. Dan Kuehl consists of three elements: information content, electromagnetic connectivity, and human cognition.[4] Recent Army conceptual models follow parallel logic in their three layers: the Physical Layer (geographic components and physical network components); the Logical Layer (logical network components), and the Social Layer (persona components and cyber persona components).[5] One could argue from these models that the domain of cyberspace has existed in war for well over a century (for example, consider the use of telegraphs in the Civil War). Over the last 50 years, the content and connec-

tivity elements of cyberspace have been transformed with the introduction of electronic transistor-based data processing devices. Hence, this monograph will focus on the modern incarnation of cyberspace created largely by the convergence of three events—the introduction of the personal computer (circa 1975), the Internet (circa 1982), and the worldwide web protocol (circa 1989).[6]

For practical discussion of military matters, let us use the current joint staff definition of cyberspace as:

> a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[7]

Note that this definition emphasizes the content and connectivity portions of the Kuehl model (i.e., the information technology aspects), but fails to include any mention of cognition.[8] Also, this definition is unclear regarding the roles of the electromagnetic (EM) spectrum and electronic warfare (EW) within the cyberspace domain. There are still doctrinal debates and differences among service components regarding the relationship.[9] With this definition of cyberspace in hand, let us now consider how conflict may manifest there.

Conflict in Modern Cyberspace.

Secretary Panetta's remarks in October 2012 reiterated some themes of his testimony before the Senate Armed Service Committee in March 2011. In fact, his statement that "the next Pearl Harbor we confront

could very well be a cyber-attack" caught the attention of the committee chairman and ranking member. They reminded the Secretary of several key issues that needed to be resolved to comply with legislative provisions:

> During the Committee's examination of the proposal to establish U.S. Cyber Command as a sub-unified command under U.S. Strategic Command, it became evident that a number of critical questions with respect to legal authorities and policy would need to be resolved, including the relationship between military operations in cyberspace and kinetic operations; the development of a declaratory deterrence posture for cyberspace; the necessity of preserving the President's freedom of action in crises and confrontations in the face of severe vulnerabilities in the Nation's critical infrastructure; the rules of engagement for commanders; the definition of what would constitute an act of war in cyberspace; and what constitutes the use of force for the purpose of complying with the War Powers Act.[10]

Further, they clarified that the recent DoD efforts did not fulfill their expectations:

> Despite the release last week [July 14, 2012] of the "Department of Defense Strategy for Operating in Cyberspace," the requirements of Section 934 [of Senate report] . . . remain unmet. The continued failure to address and define the policies and legal authorities necessary for the Pentagon to operate in the cyberspace domain remains a significant gap in our national security that must be addressed.[11]

The content and scope of the committee's questions demonstrate that its interest is not limited merely to what and how military forces operate in cyberspace. Rather, the committee is also concerned with how these operations integrate with existing U.S. policy, as

well as executive guidance and direction. Thus, while considering cyberspace as a domain may be sufficient for analyzing warfighting issues, a broader construct of cyberspace is necessary to include other elements of national power. Admiral Arthur Cebrowski, the DoD transformation lead under Secretary of Defense Donald Rumsfeld, offered a view of cyberspace as "a new strategic common, analogous to the sea as an international domain of trade and communication."[12] This more holistic definition includes not only military forces but also the national elements of diplomacy, information, and economy. Kuehl developed this concept further and termed its aggregate as "cyberpower," which he defined as "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power."[13]

How has conflict revealed itself during the first 25 years of modern cyberspace? Jason Healey, director of the Atlantic Council's Cyber Statecraft Initiative, contends that there is already a rich history of cyber conflict in the last quarter century with significant historical lessons that can be applied to future activities. Consistent with the commons paradigm of cyber power, he notes that "the more strategically significant the cyber conflict, the more similar it is to conflicts on the land, in the air, and on the sea," with the interesting caveat that "governments rarely play a central role in mitigating them." [14] Despite this assertion, he depicts that modern cyber conflict entered its current phase of militarization in 2003 with well-documented cases such as Estonia (2007),[15] Georgia (2008),[16] and BUCKSHOT YANKEE (2008),[17] among many others. More importantly, he predicts that future trends are toward more destructive cyber conflicts with more disruptive, covert, and offensive cyber operations.

Warfare including Cyberspace versus Cyberspace War (or Cyber War).

Accepting that the potential for cyber attack among nations is increasing, is the concern over a devastating surprise attack in or through cyberspace valid? A review of literature over the past few years reveals a dialectic of views among authors. The popular thesis is that cyber war will definitely occur, supported by such writers as Richard Clarke and John Stone, versus an antithesis that cyber war will not occur, espoused with some controversy by Rid.[18] Rid clarifies his argument by focusing on the enduring and evolving nature of war, asserting that "not one single cyber offense on record constitutes an act of war *on its own* [emphasis added]," and further contends that the incidents of sabotage, espionage, and subversion using cyberspace are "sophisticated versions of three activities that are as old as warfare itself."[19]

In practical terms, one can argue that preparing for cataclysmic attack conducted solely through cyberspace—popularly coined **cyber war**—represents the worst case for planning and that a force organized and prepared to handle such an event could also mitigate any lesser events. The more likely cases involve incorporation of cyberspace activities into existing joint force operations, that is, the evolutionary integration of **cyberspace warfare** with the established land, sea, and air warfare. This concept is consistent with the current joint doctrine definition of cyberspace operations as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[20] What are some unique challenges of incorporating cyberspace into the conventional aspects of warfare?

Technical Challenges.

This section focuses on some of the exceptional tactical concepts of cyberspace operations that may present technical challenges to planners and warfighters. The purpose is not to investigate these matters in detail, but rather to provide an appreciation and proper foundation to support subsequent analysis for strategic decisionmakers.

*Methods, Targets, Effects, and Intentions***.**

Traditional military operations involve the application of kinetic force to produce kinetic effects that can be directly observed in the physical environment, such as a bullet or bomb hitting a target. In contrast, cyberspace operations use nonkinetic means of exchanging coded information using the electromagnetic spectrum at levels well below that of human perception to produce nonkinetic or kinetic effects. The practitioners in cyberspace ("cyber warriors") have both common core competencies, as well as specialized skill areas that may be task organized to accomplish objectives.[21] Some of the promised advantages of cyberspace operations are that they can be direct, immediate, and predictable in method and effect. However, since the cyberspace domain is much more dynamic in its content and structure than the traditional domains, these promises are often not realized. Targets and their lines of approach in cyberspace are not static and may depend on multiple pivot points in networks to be compliant in the passage of the cyber payload.[22] However, the actual path of the electronic package may change by the re-routing of data

to compensate for failed network servers or possible intentional interference.[23] Once delivered, the code may cause immediate collateral damage as well as nth-order effects beyond the intentions of its designers. For example, the software weapon called Stuxnet is often touted as the epitome of precise delivery of cyberspace effects, allegedly zeroing in on unique industrial control devices in Iranian nuclear refinement facilities. But in reality, less than 2 years after the attack, software security corporation Symantec reported that the malware had spread to over 100,000 hosts in over 25 countries, including the United States.[24]

Attribution: Tactical and Strategic.

One of the most difficult challenges in cyberspace operations is the timely and accurate attribution of their means and source. At the tactical level, if damage or other negative effects to some system are discovered, one must determine if the effects were caused by cyber means. Often, the effects themselves may not be discovered for days or weeks, thus making the forensics more difficult, as many other factors may have influenced the same system in the interim. Without delving into technical digressions, suffice it to say that merely discovering the effects and root cause of a cyber attack is not a trivial affair.[25]

But even if the mechanics of determining the effects and causes are perfected, there remains a challenge of determining the source and intentions of the attack. Even in the land domain, this may be a challenge. Consider a vignette where the president of country A is shot by a uniformed sniper in the army of country B. On the surface, it may be very simple—direct effects and clear identities of aggressor and target.

However, attribution quickly becomes complicated if the vignette occurred during the visit of the president to country C with the sniper, a dual citizen of countries A and E, shooting across a river from country D. Given these further stipulations, who does country A hold accountable for this violent act?

In cyberspace, attribution can have such levels of intricacy as attacks may be directed through multiple persona using multiple computers connected by multiple networks residing in multiple countries. Given this thorny mix of possibilities, how can strategic decisionmakers ensure they are receiving the proper and sufficient foundation of situational understanding by which to determine and judge appropriate responses? Waxman offers three questions to help assess the reliability of attribution:

> What level of certainty is sufficient from an intelligence perspective to convince policy-makers as to the perpetrator? What level is sufficient to satisfy the legal requirements of self-defense? And what level is demonstrable publicly (or perhaps privately when necessary) to attain diplomatic and political support for responses?[26]

Applying this model of technical-legal-political attribution requires a balanced approach to prevent each of the communities involved from following their favorite rabbit hole. Healey advances that "the international security community must focus on the policymakers' warning that too much time has been wasted obsessing over which particulate villain pressed the *ENTER* key." He further refines this concept to a proposed spectrum of state responsibility for cyber attack that ranges in 10 steps from state-prohibited to state-integrated. To illustrate this, he observes that analysts

were successful in tracing elements of the 2007 Estonia incident back to 178 countries, including the United States. However, this impressive technical tracking of "cyber stones" being thrown from numerous locations detracted from efforts of Western authorities to engage the likely culprit (Moscow).[27] In later writing, Healey develops 14 criteria for analyzing nation responsibility for cyber attacks:

- Attack traced to a nation?
- Attack traced to a state organization?
- Attack written or coordinated in national language?
- State control over the Internet?
- More technical sophistication than normal?
- More targeting sophistication than normal?
- Little popular anger at target?
- No direct commercial benefits?
- Direct support of hackers?
- Attack correlated with public statements?
- Lack of state cooperation during investigation?
- Attack correlated with specific national policy?
- *Cui bono* (who benefits)?
- Attack strongly correlated or even integrated with physical force?

We will discuss these in concert with existing international legal frameworks in the Assessment Criteria section of this monograph.

*Speed, Perception, and Complexity – the Role of Chance***.**

In testimonies before a congressional committee, General Keith Alexander, former Commander, U.S. Cyber Command, stated that the U.S. military needs a "pro-active, agile cyber force that can 'maneuver'

in cyberspace at the speed of the Internet" and mentioned that the interagency and international exercise Cyber Flag "introduced new capabilities to enable dynamic and interactive force-on-force maneuvers at net-speed."[28] The speeds of weapon systems movement and tempo of operations are essential considerations for military planners and commanders. How the "speed of cyber" compares to activities in other operational domains should be of interest to modern military decisionmakers.

Although there are many ways to depict this, Figure 1 illustrates typical speeds of executing operations in each domain versus the distance traveled in the domain in 20 milliseconds, which is the average time for an information payload to transverse to an Internet node halfway around the world and return. Each axis of the graphic is logarithmic, which means that each mark on the axis is an order of magnitude greater than the previous mark. Examining this, one can see that cyberspace operations occur in a realm of speed that is over 20,000 times faster than operations in the space domain; over 200,000 times faster than the air domain, and 10 million times faster than the land and sea domains.[29] Why is this significant? Granted, the manifestation of any kinetic effects in the physical world will propagate at about the same rate independent of the method of delivery. But the increased pace of cyberspace activities means that a weaponized software payload may be delivered on target in less time than your brain can perceive the visual content of this page. In the time it takes for a trained mind to comprehend it as a potential threat, there may be numerous cycles of cyber fires and maneuver. These factors may reduce the time frame for the observe-orient-decide-act (OODA) loop for tactical operators to a realm that

may be described as ultra-tactical.[30] Such cyber warfare exchanges may create even larger problems for military operations requiring permissions and authorities of higher headquarters.

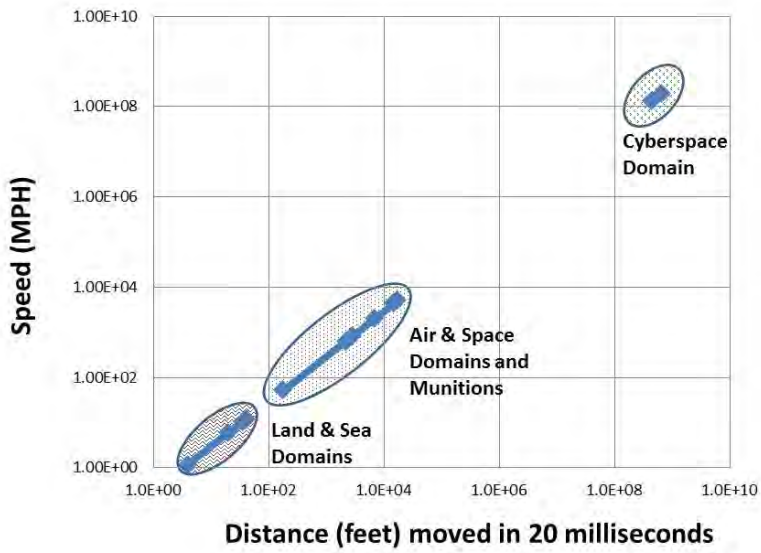

Figure 1: A Comparison of Operational Speed and Distance in Military Domains.

The dynamic nature of cyberspace adds more conceptual hurdles for decisionmakers trying to make sense of activities. The cyberspace domain can be modeled as a complex adaptive system—a system of systems with a complex macroscopic collection of similar and partially connected microstructures formed to adapt to a changing environment.[31] The intricate interactions within such systems may lead to spontaneous self-organization and synchronization that produce emergent and unanticipated macroscopic behavior. Such behavior may be exacerbated when there is a

high degree of homogeneity and integration in microscopic structures, such as the widespread use of standard operating systems.[32] A controversial report on Microsoft in 2003 posited that use of a "single dominant operating system in the hands of all end users is inherently dangerous."[33] To facilitate that full range of operations for U.S. Cyber Command, the Defense Information Systems Agency (DISA) is developing the Joint Information Environment with enterprise-wide architectures and standardized identity and access management.[34] While this may enhance the capability of cyberspace operations, it may be prudent to realize that these same characteristics also increase the prospect of emergent behavior in the warfighter operations, perhaps initiated by natural phenomena such as geomagnetic storms. Thus, planners should realize that any cyber weapon must traverse an ever-changing terrain to deliver its payload, and that its effects may trigger mechanisms in the domain that produce emergent events that are unpredictable, and possibly undesirable, in consequence and severity.

Clearly, the result of the combined aspects of speed, perception limitation, and system complexity may have far-reaching implications for the reliability of information presented to support decisionmaking in the cyberspace domain. In the traditional Clausewitzian trinity, such operations gravitate toward the "chance" apex with normal and emergent cyberspace activity (e.g., Internet activities), enabling the spread of "cyber fog and friction." But is such drastic behavior of a system realistic or mere theory? Consider the recent events of April 23, 2013, where automated trading algorithms on Wall Street triggered a temporary drop of 130 points (worth approximately $134 billion) based on false information from a hacked Associ-

ated Press Twitter account. The Tweet indicated that President Barack Obama had been injured in an explosion at the White House.[35] What if a similar emergent event occurred in a military cyberspace common operational picture? Imagine what could happen if the physical or cyber equivalent of the May 2013 missile tests by North Korea[36] were monitored as indicators in an attack assessment system. What if a natural event akin to the February 2013 Chelyabinsk meteor[37] released mega-tonnage of blast effects near any of the missile impact zones—how would this be assessed and reported by the system? What criteria would senior decisionmakers use to determine if an attack had occurred?

ASSESSMENT CRITERIA

The section explores the *de jure* and the *de facto* issues involved with assaying cyber incidents to determine if they represent aggression and possible use of force; and if so, to what degree? At this point, we will assume for the purpose of this monograph that the information gathered regarding a potential negative incident in cyberspace is fully accurate. Certainly, this is not a trivial task, but once the information is received, evaluated, and passed to the proper authorities—what happens next? What criteria may they use to determine the severity of the incident as well as the appropriateness, necessity, and urgency to respond?

Legal Frameworks.

The purpose here is to describe what exists in international law regarding cyberspace activities and to establish a foundation for criteria contained therein; it

will not discuss any issues regarding legal adequacy. Readers interested in a more detailed analysis should explore some of the seminal works in this field by experts like Walter Gary Sharp, Sr., and Thomas C. Wingfield.[38]

United Nations Charter.

There are many publications that delve into the details of how the existing Charter of the United Nations (UN) may apply to activities in cyberspace among sovereign nations. Most focus on the following articles of the charter when addressing this issue[39] (see Appendix 1 for the full text of these articles):

- Article 2(1): Establishes "the principle of sovereign equality" for member countries.
- Article 2(4): Requires members to "refrain in their international relations from the threat or use of force" in ways not consistent with the purposes of the UN.
- Article 25: Requires members "to accept and carry out the decisions of the Security Council."
- Article 39: Establishes that "the Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression" and make recommendations or decide measures accordingly.
- Article 41: Establishes that the Security Council may decide what measures not involving uses of armed force can be "employed to give effect to its decisions."
- Article 42: Stipulates that if measures under Article 41 are inadequate, the Security Council can escalate to the use of air, sea, or land forces "as may be necessary to maintain or restore international peace and security."

- Article 51: Establishes "the inherent right of individual or collective self-defense if an armed attack occurs."

In March 2014 testimony to Congress as part of his nomination process for command of U.S. Cyber Command, Vice Admiral Michael Rogers summed up the DoD policy regarding the UN principles as follows:

> As a matter of law, DoD believes that what constitutes a use of force in cyberspace is the same for all nations, and that our activities in cyberspace would be governed by Article 2(4) of the U.N. Charter the same way that other nations would be. With that said, there is no international consensus on the precise definition of a use of force, in or out of cyberspace. Thus, it is likely that other nations will assert and apply different definitions and thresholds for what constitutes a use of force in cyberspace, and will continue to do so for the foreseeable future.[40]

In other words, the language contained in the UN Charter may be interpreted differently for specific circumstances due to cultural and political factors. As witnessed in the evolving situation in the Crimean Peninsula, any such incongruity is not unique to matters in cyberspace.[41] A significant dynamic in UN affairs that may impact cyberspace matters is the permanent membership of the United States, Russia, and China on the Security Council, which permits each to have veto power in that forum.

The provisos of the UN Charter include a spectrum of hostile activities among members that include (in increasing order of violence): use of force, threat to the peace, breach of the peace, act of aggression, armed attack, and armed conflict. While "act of war" is not

defined within the charter, activities of armed conflict conducted by an aggressor member against a victim member could serve as an implicit definition. But how does one evaluate whether an act of aggression in cyberspace is an attack? In 1999, renowned military legal expert Michael Schmitt proposed seven factors that countries could use as criteria to determine whether specific cyberspace operations amounted to a use of force, or more. These factors, commonly referred to as the "Schmitt criteria" are severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[42]

Collective Defense Agreements.

In general terms, the UN recognizes the menace to international peace posed by cyber attacks, and it promulgates cooperative activities among member countries to address such threats. UN Secretary-General Ban Ki-moon summarized this view in his remarks to the Seoul Conference on Cyberspace, Seoul, Korea, October 17, 2013:

> Cyberattacks have the potential to destabilize on a global scale. Cybersecurity must therefore be a matter of global concern. We need to work together to bolster confidence in our networks, which are central to international commerce and governance. We need to strengthen national legislation, push for international frameworks for collaboration and adopt the necessary means to detect and defuse cyber threats (available from *www.un.org/sg/statements/index.asp?nid=7209*).

In more specific terms, UN Article 51 provides for collective self-defense if an armed attack occurs. Of course, the North Atlantic Treaty Organization (NATO) is one of the most important collective de-

fense agreements for the United States. The NATO Strategic Concept from its 2010 Lisbon conference elucidated that collective cyber defense among its members applies not only to kinetic but also to cyber activities as part of the "full range of capabilities necessary to deter and defend against any threat to the safety and security of our populations." Further, the concept calls for NATO members to:

> Develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations.[43]

This is an important extension of traditional NATO obligations, and it was driven by such events as the April-May 2007 cyber attacks on Estonia. Historians and analysts note that NATO collective defense measures were not initiated during this crisis, mainly because NATO had not yet defined cyber attack as a clear military action.[44] However, with the increased scope of NATO activities, the United States must include the stipulations of NATO Articles 4 and 5 (see Appendix 1) in its criteria for assessing potential attacks in or through cyberspace. One proposed NATO cyber early warning framework emphasizes the examination of purpose, target, context, and scale to help differentiate tactical from strategic cyber attack.[45]

Law of Armed Conflict.

Although this monograph is not designed to develop responses to cyber attacks, it is important to consid-

er the potential follow-on consequences to classifying an incident as an act of war. If the United States seeks a military response to such an incident, then it enters into the regime of international rules that help to define acceptable measures. Central among these is the Law of Armed Conflict (LOAC), which is built upon four principles to ensure that *jus in bello* is legal and moral: military necessity, distinction (or discrimination), proportionality, and unnecessary suffering (or humanity). While there are many LOAC-related treaties in force today, most have their foundation in the "Hague Tradition" of regulating the means and methods of warfare and the "Geneva Tradition" regarding the respect and protection of victims of warfare.[46]

Several authors have studied possible interpretation of LOAC applied to cyberspace activities in concept as well as case studies.[47] The U.S. Air Force has codified this concept in part by requiring legal review for use of cyber capabilities. This review includes an examination of the concept of operation and the reasonably anticipated effects of employment as well as any specific rules of law that prohibit or restrict its use. Further, if there is no explicit prohibition, two additional questions are considered regarding the possibility of superfluous injury and the potential for the capability to be directed against a specific military objective.[48] Such efforts will remain a work in progress as operations in the cyberspace domain continue to be integrated into joint military operations.

*Pictet Criteria for Armed Attack***.**

Many legal scholars posit that criteria developed by Jean Pictet to examine if actions can be interpreted as armed conflict under the 1949 Geneva Conventions

may also be applied to cyberspace. Specifically, Pictet considered the scope, duration, and intensity of a use of force to see if the aggregate was sufficient to be considered an armed attack. While elegant in its simplicity, these criteria require additional context to be practical for cyberspace applications. David Graham, Executive Director of The Judge Advocate General's Legal Center and School, identifies three analytical frameworks to facilitate this process. The first is an "instrument-based approach," which considers whether the damage resulting from a cyber attack could previously have been achieved only by kinetic means. The second framework is an "effects-based approach," often called "consequence-based model," which focuses on the overall effect of the attack on the victim states without comparison to kinetic means. Graham posits that this is the model adopted by the United States. The third framework is the "strict liability approach," which simply regards any cyber attack against critical national infrastructure as an armed attack. For the United States, applicable targets would be systems defined in the Critical Infrastructure Protection Act of 2001. Graham notes that while there is some debate as to which should be the preferred model, "proponents of all three approaches agree on the singularly important conclusion that cyber attacks can constitute armed attacks."[49]

The Tallinn Manual.

*History and Purpose***.**

In 2009, a group was organized by the NATO Cooperative Cyber Defence Centre of Excellence (CCD-COE) to undertake "an expert-driven process de-

signed to produce a non-binding document applying existing law to cyber warfare." This assemblage of 46 participants included international legal and technical experts, as well as observers from NATO's Allied Command Transformation, the International Committee of the Red Cross, and U.S. Cyber Command. Developed over 3 years, the primary end product of their collective effort is the *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[50]

This extensive study faced many challenges, among which was the realization that views on the subject ranged from one where cyber warfare must follow strict LOAC compliance to the more liberal position that, whatever is not specifically forbidden by law, is generally permitted. The findings of this thorough examination are expressed in 95 rules within seven chapters that are divided into two major parts: "States and cyberspace" and "The law of cyber armed conflict." The group's analyses addressed applying *jus ad bellum* and *jus in bello* principles to cyber warfare, with emphasis on cyber-to-cyber operations. The group readily acknowledges that its discussions often drew upon content from the military manuals of Canada, Germany, the United Kingdom, and the United States. In contrast, the group did not intend their work to produce a manual on the holistic aspects of cyber security and thus did not address cyber activities below the level of "use of force," such as cyber crime, espionage, national law, or domestic legislation. Content was reached by consensus among the group, not through full unanimity.[51]

Schmitt-Tallinn Criteria for Use of Force.

Tallinn Manual Chapter 2, "The Use of Force," includes Rules 10 through 19, many of which align with existing international convention. Specifically, Rule 13, "Self-defense against armed attack"; Rule 16, "Collective self-defense"; and Rule 17, "Reporting measures of self-defense" include references to UN Article 51. Also, Rule 18, "United Nations Security Council" and Rule 19, "Regional organizations" discuss UN Articles 39, 41, 42, and 52. But it is Rule 11, "Definition of use of force," that refines and expands the Schmitt criteria to a list of eight factors: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legitimacy (see Appendix 2 for illustrative questions). But the team offers these criteria with strict caveats:

> The approach focuses on both the level of harm inflicted and certain qualitative elements of a particular cyber operation. In great part, it is intended to identify cyber operations that are analogous to other non-kinetic or kinetic actions that the international community would describe as uses of force…It must be emphasized that they are merely factors that influence States making use of force assessments; they are not formal legal criteria.[52]

The text also points out that neither the UN Charter nor any other authoritative source provides a definition of "use of force," let alone any criteria for its assessment. Perhaps these factors can be best utilized in combination with other criteria.

Spectrum of Force.

The paradigms and philosophies regarding the association of cyber warfare with existing international norms discussed in this section have slightly different foci. Figure 2 illustrates how all these different factors and criteria may be conceptually integrated to provide a more holistic assessment to determine how cyberspace incidents may be assessed as well as if a military response might be considered. It is not intended to be a rigid checklist or flowchart; rather, it is envisioned to serve as a starting point for staffs and decisionmakers to modify for their own utilization. It depicts increasing levels of the use of force peaking at armed conflict as assessments gravitate from *jus ad bellum* tenets, which help guide incident analyses, to *jus in bello* tenets, which help guide selection of the means of any military response.

Again, the chart is not meant to be linear or sequential. Incidents judged to be armed attack may prompt a state to pursue UN Article 51 and NATO Article 4 actions directly, as well as to move toward a rapid military response that meets LOAC principles. Of course, such assessments will be most effective when they occur in the context of informed international situational awareness. To aid decisionmakers in this process, let us now examine such considerations.

POLICY CONSIDERATIONS

Having identified viable criteria to aid with the assessment of cyberspace incidents, let us now look at the policy considerations associated with applying such principles.

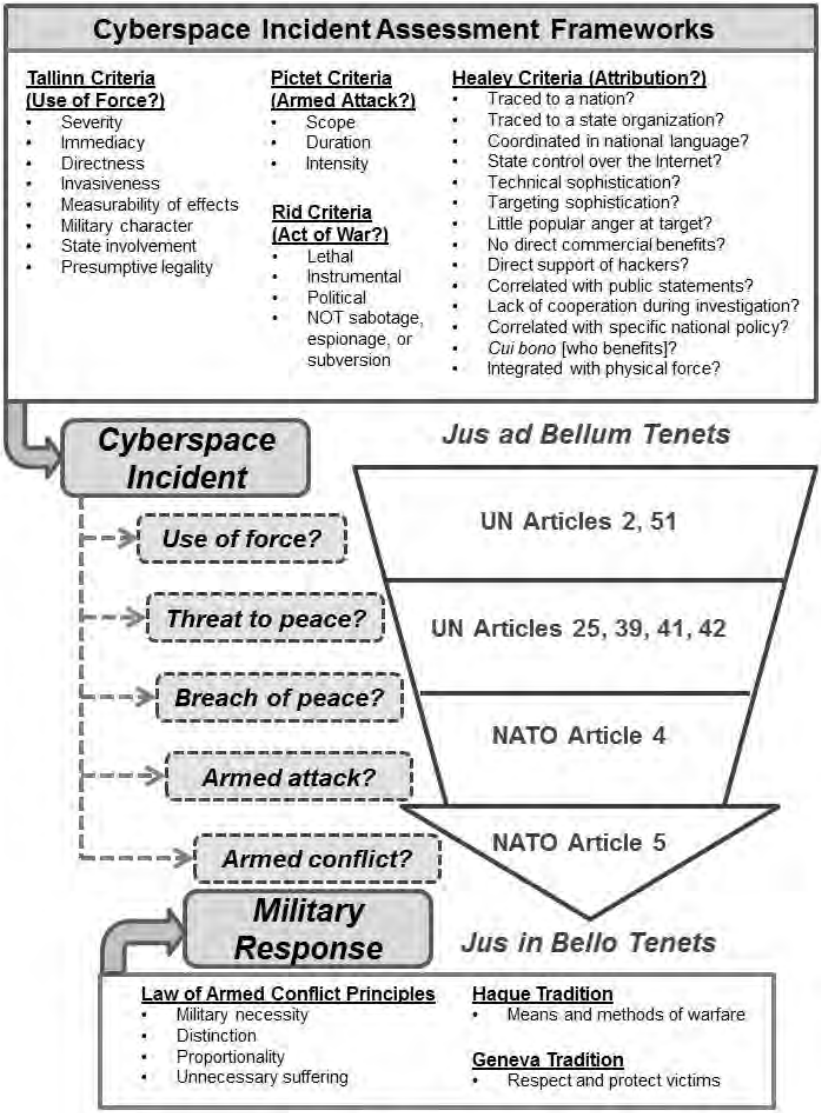

Figure 2. A Cyberspace Incident Assessment Methodology.

This section first examines the relevant U.S. strategies; next, it investigates the strategies of other key countries and international organizations and how they compare to U.S. tenets; and finally, it evaluates how nonstate actors may affect U.S. deliberations.

Cyberspace in U.S. Strategies.

How should a government approach the prospect of waging cyberspace related warfare? What ends, ways, and means are required, and how are they crafted together? Kuehl offers a concept of "cyber strategy" as:

> the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational realms, to achieve or support the achievement of objectives across the elements of national power in support of national security strategy.[53]

Let us examine some of the factors and unique challenges of developing and implementing such a strategy for the United States.

*National Security Strategy***.**

In his May 2010 *National Security Strategy*, President Obama divides the pursuit of U.S. enduring national interests into four areas: security, prosperity, values, and international order. The theme of the increasing U.S. reliance on cyberspace in all of these areas is woven throughout the document, but two subsections are of particular interest to our discourse—Use of Force and Secure Cyberspace. In the text, the use of

force is tied directly to military force "to defend our country and allies or to preserve broader peace and security," with the clarifications that such force will not necessarily be the first or only option and that cyber is a domain for military action:

> This means credibly underwriting U.S. defense commitments with tailored approaches to deterrence and ensuring the U.S. military continues to have the necessary capabilities across all domains—land, air, sea, space, and cyber. It also includes helping our allies and partners build capacity to fulfill their responsibilities to contribute to regional and global security.

Clearly, the tenet of seeking broad international support for U.S. military action is included with specific mentions of working with NATO and the UN Security Council. But the section closes with the reminder that "the United States must reserve the right to act unilaterally if necessary to defend our nation and our interests."[54]

In contrast, the Secure Cyberspace subsection delineates threats in other areas of security separate from those involving direct military operations. In broader terms, it states that "Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation," and that these threats "range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced nation states." Two overarching ways are put forth to mitigate these risks: Investing in People and Technology, and Strengthening Partnership. For the latter, the strategy affirms that the United States:

> will also strengthen our international partnerships on a range of issues, including the development of norms for acceptable conduct in cyberspace; laws concerning cybercrime; data preservation, protection, and privacy; and approaches for network defense and response to cyber attacks.[55]

U.S. International Strategy.

The May 2011 *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* refined much of the cyberspace related vision of the *National Security Strategy.* It is geared toward a more holistic view of cyberspace captured in seven policy priorities: economy, network protection, law enforcement, Internet governance, Internet freedom, international development, and military. The envisioned U.S. role in cyberspace's future is threefold: diplomacy, defense, and development. In the context of this strategy, the broad goal of defense involves dissuading and deterring all types of threats:

> The United States will defend its networks, whether the threat comes from terrorists, cybercriminals, or states and their proxies. Just as importantly, we will seek to encourage good actors and dissuade and deter those who threaten peace and stability through actions in cyberspace. We will do so with overlapping policies that combine national and international network resilience with vigilance and a range of credible response options. In all our defense endeavors, we will protect civil liberties and privacy in accordance with our laws and principles.[56]

However, as the text focuses on implicit threat to peace and uses of force, the strategy minces no words in its *de facto* declaratory statement:

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. 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, our allies, our partners, and our interests. 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 and strengthens our legitimacy, seeking broad international support whenever possible.[57]

This passage provides the utility of being purposefully vague to allow flexibility in response options and avoids establishing any discrete red lines that may undermine effective deterrence. But it clearly connotes that when matters intensify to where U.S. military forces are engaged against hostile acts in cyberspace, the stakes for U.S. interests are serious. So if cyberspace activities do escalate to the point of military involvement, what is the strategy for such engagement?

DoD Strategy.

In July 2011, the unclassified *Department of Defense Strategy for Operating in Cyberspace* was released after months of anticipation following the Deputy Secretary of Defense William Lynn III article, "Defending a New Domain: The Pentagon's Cyberstrategy" in the September 2010 issue of *Foreign Affairs*. Secretary Lynn's

conclusion provided a concise and accurate preview of the upcoming formal strategy:

> These risks [in cyberspace] are what is driving the Pentagon to forge a new strategy for cybersecurity. The principal elements of that strategy are to develop an organizational construct for training, equipping, and commanding cyberdefense forces; to employ layered protections with a strong core of active defenses; to use military capabilities to support other departments' efforts to secure the networks that run the United States' critical infrastructure; to build collective defenses with U.S. allies; and to invest in the rapid development of additional cyberdefense capabilities. The goal of this strategy is to make cyberspace safe so that its revolutionary innovations can enhance both the United States' national security and its economic security.[58]

Upon review, the strategy fell short of providing any new information or clarity regarding how DoD was progressing with its cyberspace activities, but it did consolidate the description of ongoing efforts into a single document.[59] It also addressed all aspects of military operations in cyberspace, not just those related to warfare:

> In developing its strategy for operating in cyberspace, DoD is focused on a number of central aspects of the cyber threat; these include external threat actors, insider threats, supply chain vulnerabilities, and threats to DoD's operational ability. DoD must address vulnerabilities and the concerted efforts of both state and non-state actors to gain unauthorized access to its networks and systems.[60]

The strategy was organized into five strategic initiative areas: domain-based operations; new defense concepts; domestic partnering; international partner-

ing; and technological innovation. In his analysis, Dr. Thomas Chen of Swansea University, United Kingdom, notes two critical observations relevant to our discussion: 1) The strategy does not distinguish between different types of adversaries—nation-states, foreign intelligence, hacktivists, criminals, hackers, terrorists—nor does the strategy address initiatives for specific types of adversaries; and 2) The unclassified version of the strategy neglects to address important issues: offense; attribution; rules for proper response to cyber attacks; and metrics for progress toward implementation.[61]

Another limitation not mentioned by Chen is that the strategy does not clarify the different roles of U.S. Cyber Command and its Title 10 responsibilities that include cyber attack versus those of the National Security Agency and its Title 50 responsibilities related to cyber exploitation. It does provide a vague description of the shared commander structure of the two units:

> A key organizational concept behind the stand-up of USCYBERCOM [U.S. Cyber Command] is its co-location with the National Security Agency (NSA). Additionally, the Director of the National Security Agency is dual-hatted as the Commander of USCYBERCOM. Co-location and dual-hatting of these separate and distinct organizations allow DoD, and the U.S. government, to maximize talent and capabilities, leverage respective authorities, and operate more effectively to achieve DoD's mission.[62]

Among the recommendations by Chen for any future version of the strategy is that it should address two fundamental issues: "When does a cyber attack justify a military response?" and "What is an appro-

priate response?"[63] In essence, these questions frame the realms of *jus ad bellum* and *jus in bello* depicted in Figure 2 and they cannot be fully answered with discrete statements. Perhaps the 2014 *Quadrennial Defense Review* (QDR) provides a general approach to the two questions posed by Chen:

> The Department of Defense will deter, and when approved by the President and directed by the Secretary of Defense, will disrupt and deny adversary cyberspace operations that threaten U.S. interests. To do so, we must be able to defend the integrity of our own networks, protect our key systems and networks, conduct effective cyber operations overseas when directed, and defend the Nation from an imminent, destructive cyberattack on vital U.S. interests.[64]

While precise answers to these questions remain unresolved, the official views of the U.S. Government regarding military operations are consistent with the legal sources already discussed. U.S. State Department Legal Advisor Harold Koh went on public record during a September 2012 conference hosted by U.S. Cyber Command with 10 rhetorical questions and answers regarding how existing international law applies in cyberspace. This presentation averred that "international law principles do apply in cyberspace," with several specific references to the UN Charter and LOAC responsibilities for States.[65] In response, Michael Schmitt authored an article that compared Koh's position with those in the draft *Tallinn Manual,* noting that:

> The relative congruency between the U.S. Government's views, as reflected in the Koh speech and those of the International Group of Experts is striking. This confluence of a state's expression of *opinio juris* with

> a work constituting "the teachings of the most highly qualified publicists of the various nations" significantly enhances the persuasiveness of common conclusions. Of course, the limited differences that exist as to particular points of law render the respective positions on those points somewhat less compelling. . . . The Koh speech and the Tallinn Manual are but initial forays into the demanding process of exploring how the extant norms of international law will apply in cyberspace. But the long overdue journey has at least finally begun.[66]

In his recent confirmation hearing before Congress, the new Commander of U.S. Cyber Command, Admiral Rogers reiterated his command's three-fold mission, consistent with both the DoD Strategy and the QDR:

> The prioritization of capability development for national and combatant command cyber mission forces flows directly from USCYBERCOM's three mission areas; (1) defend the nation; (2) secure, operate, and defend Department of Defense information networks (DoDIN); and (3) provide support to combatant commands. USCYBERCOM's highest priority is to defend the nation. This is done in parallel with activities dedicated to securing the DoDIN and supporting combatant commands.[67]

Evidently, there is considerable content in U.S. national, international, and military strategies to help guide decisionmakers and planners in their assessment and response of any use of force in cyberspace. Also, while they do not provide discrete criteria for such tasks, these documents do have consistent, but evolving, legal and organizational frameworks for any supporting analyses. How does this compare to the rest of the world regarding approaches to national security and military activities in cyberspace?

The International Community.

Prominent cyber security expert Melissa Hathaway conducted a detailed assessment of the cyber security readiness of 35 countries. The initial report, released in November 2010, found that "27 of 35 countries have a [published] Cyber Security Strategy, yet few are measuring progress and even fewer have invested in the strategy's successful outcome." Of these, only Australia, Canada, The Netherlands, the United Kingdom, and the United States had actions by their governments that met all five of the study elements.[68] In implementing its cyberspace strategy, DoD has identified "both senior-level and expert coordinating activities with Australia, Canada, New Zealand, and the United Kingdom" as well as its efforts toward "strengthening its relationships with Japan and the Republic of Korea."[69] All seven of these countries have national cyber security strategies with competent authority. Of course, such strategies are mere documents unless action is taken. For our purposes, let us accept them at face value as a reflection of interests, values, and priorities.

Due to the study's selection criteria for countries, there was little coverage of South America and Africa (only 4 of the 35 countries). However, there are organizations on these continents that are developing and incorporating cyber security policies. The 35-member strong Organization of American States (OAS) adopted a comprehensive strategy to combat threats to cyber security that addresses issues of cyber crime and terrorism, "but it has not yet developed a more active program for addressing cyber-attacks more generally."[70] The OAS General Assembly Resolution calls for cooperation and collaboration, but makes no mention of military activities or collective defense:

> The destruction of data that reside on computers linked by the Internet can stymie government functions and disrupt public telecommunications service and other critical infrastructures. Such threats to our citizens, economies, and essential services, such as electricity networks, airports, or water supplies, cannot be addressed by a single government or combated using a solitary discipline or practice.[71]

The African Union (AU), comprising 54 states, is developing a convention with concepts similar to those of the OAS. To wit, their draft capstone document makes no mention of military activities; rather, it guides its members toward the following endeavors:

> As part of the promotion of a culture of cyber security, Member States may adopt the following measures: devise a cyber security plan for the systems run by their governments; conduct research and devise security awareness-building programmes and initiatives for the systems and networks users; encourage the development of a cyber security culture in enterprises; foster the engagement of the civil society; launch a comprehensive and detailed national awareness raising programme for home users, small business, schools, and children.[72]

In contrast, the 2013 *Cybersecurity Strategy of the European Union* (EU) adopts a broad approach which addresses civilian and military aspects as well as potential seams with NATO responsibilities:

> Given that threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be enhanced. These efforts should be supported by research and development, and closer cooperation between governments, private sector and

> academia in the EU. To avoid duplications, the EU will explore possibilities on how the EU and NATO can complement their efforts to heighten the resilience of critical governmental, defence and other information infrastructures on which the members of both organisations depend.[73]

NATO.

NATO's cyber defense program has progressed significantly since its adoption in 2002 at the Prague Summit, spurred by cyber incidents against NATO during Operation ALLIED FORCE. The initial organization included the creation of the NATO Computer Incident Response Capability designed to prevent, detect, and respond to future cyber incidents. Following the 2007 cyber attacks on Estonia, the 2008 Bucharest Summit laid the foundation for two major NATO institutions: the Cyber Defense Management Authority and the Cooperative Cyber Defense Center of Excellence.[74] Acting upon declarations from the 2010 Lisbon Summit, in June 2011, a formal NATO policy on cyber defense was released with the stated focus as:

> In order to perform the Alliance's core tasks of collective defence and crisis management, the integrity and continuous functioning of its information systems must be guaranteed. NATO's principal focus is therefore on the protection of its own communication and information systems. Furthermore, to better defend its information systems and networks, NATO will enhance its capabilities to deal with the vast array of cyber threats it currently faces.[75]

New policies and capabilities are vetted through the Cyber Defense Management Board. Overall prog-

ress toward normalizing cyber activities into NATO operations can be summarized as:

> Allies also agreed at the Lisbon Summit that cyber defence and relevant capabilities need to be included in NATO's Defence Planning Process (NDPP). In June of 2013 NATO Defence Ministers approved the initial integration of cyber defence capability targets into the NDPP. This process will help to harmonize important work on cyber policy and procedures within NATO and at the national level to ensure that the Alliance's overall cyber defence capability meets agreed targets.[76]

*"Near Peer" Rivals – Russia and China***.**

Among the many countries that the United States and its allies may face as opponents in cyberspace, Russia and China have the most formidable national capabilities to consider. In addition to cyberspace forces, they also have significant global economic, military, and political powers. Both have enduring nuclear forces; both are permanent members of the UN Security Council; and both have publicly discussed elements of their cyber security strategies. In his January 2014 Senate testimony on the Worldwide Threat Assessment, Director of National Intelligence (DNI) James R. Clapper noted:

> Russia and China continue to hold views substantially divergent from the United States on the meaning and intent of international cyber security. These divergences center mostly on the nature of state sovereignty in the global information environment states' rights to control the dissemination of content online, which have long forestalled major agreements.[77]

A March 2014 study by Keir Giles, director of the Conflict Studies Research Centre, and Andrew Monaghan, a Research Fellow at St. Antony's College, Oxford, echoes this view:

> In fact, China, Russia, and a number of like-minded nations have an entirely different concept of the applicability of international law to cyberspace as a whole, including to the nature of conflict within it. These nations could therefore potentially operate in cyberspace according to entirely different understandings of what is permissible under international humanitarian law, the law of armed conflict, and other legal baskets governing conduct during hostilities.[78]

Specifically regarding the determination of an act of war in cyberspace, they conclude "On this point, Russian thinking appears at odds with the emerging Western consensus."[79]

The uses of cyberspace activities to support military options have been postulated in operations in Estonia (2007) and Georgia (2008), as well as ongoing activities with Ukraine. Concerning the evolution of its military forces, Clapper noted:

> Its [Russia's] Ministry of Defense (MOD) is establishing its own cyber command, according to senior MOD officials, which will seek to perform many of the functions similar to those of the US Cyber Command. Russian intelligence services continue to target US and allied personnel with access to sensitive computer network information.[80]

The current Russian perspective is expressed in its 2011 cyber security document, which addresses the connection of international law to operations by its armed forces as:

> Peculiarities of the military activity in the global information space are guided by the following regulations and principles thereof: respect towards national sovereignty, non-interference in internal affairs of other states, non-use of force and threat of force, [and] rights for individual and collective self-defense.[81]

The strategy goes on to promulgate the "containment and prevention of military conflicts in the information space" utilizing such means as: force readiness; cooperative efforts through the Collective Security Treaty Organization, Commonwealth of Independent States, and the Shanghai Cooperation Organization; escalation prevention; and the resolution of conflicts by agreement or other peaceful means, such as the UN Security Council.[82] It summarizes its goals in the final paragraph:

> Implementing this Conceptual Perspective, the Armed Forces of the Russian Federation shall strive towards the maximum use of the opportunities of the information space for strengthening the defensive potential of the state, the containment and prevention of military conflicts, the development of military cooperation, as well as the formation of the system of international information security in the interests of the entire global community.[83]

Officials from China have listed similar goals in public statements, referring to their collective efforts with Russia, Tajikistan, Uzbekistan, Kazakhstan, and Kyrgyzstan to have the UN accept an "International Code of Conduct for Information Security" that they introduced to the General Assembly in 2011.[84] The proposed code would be voluntary for nations and it is organized into four categories: peace, security,

openness, and cooperation. In drafting the code, they claim that "China and other cosponsors tried their best to reflect international consensus in a comprehensive and balanced manner."[85] These statements also contained some thinly veiled criticisms of U.S. cyberspace activities:

> Some countries keep others from participating in the equitable distribution of information resources and enjoying the digital dividends by monopolizing critical information resources. Some countries are developing cyber military capabilities and threatening others with preemptive strikes, turning the information space into a new battlefield. Some negative incidents exposed recently indicate that many countries' data security and personal privacy were compromised and caused widespread concern of the international community.[86]

It is reasonable to assume the following was directed at the establishment of U.S. Cyber Command:

> To ensure a country's security by developing its cyber military capabilities and seeking military advantage is not only untenable, but is triggering arms race and increasing the possibility of conflicts in information space, which is against the common interests of the international community. China believes that countries should comply with the UN Charter and the basic principles governing international relations, not to use force or threaten to use force in information space, and settle disputes through peaceful means.[87]

Such language supports the findings of an April 2013 workshop hosted by the University of California on the political, economic, and strategic dimension of China's cyber security. The workshop noted that "the security of global information systems has become a

contentious issue in U.S.-China relations," and further specified that "failure to appreciate China's domestic economy and politics can lead to a profound misunderstanding of its international activities."[88] This view is in concert with Clapper's recent report:

> China's cyber operations reflect its leadership's priorities of economic growth, domestic political stability, and military preparedness. Chinese leaders continue to pursue dual tracks of facilitating Internet access for economic development and commerce and policing online behaviors deemed threatening to social order and regime survival.[89]

Finally, China's own words before the UN General Assembly substantiate the DNI assessment by making a "don't tread on me" statement:

> We should adhere to the principle of balance between freedom and law. Information space is no "global domain". Countries should enjoy state sovereignty in information space. The governments are entitled to managing its network-related activities and have the jurisdiction over its information infrastructures within its territory. Under such premises, we should protect the freedom for all in information space. Countries shouldn't use ICTs [information and communication technologies] to interfere in other countries' internal affairs and undermine other countries' political, economic, and social stability as well as cultural environment. Countries should not take advantage of its dominant position in information space to undermine other countries' right of independent control of ICT products and services.[90]

Any Chinese implementation of military action in cyberspace will likely focus on their concept of "informationalized" warfare[91] utilizing "tactics known

as 'cocktail warfare', a concept developed in the 1999 book *Unrestricted Warfare,"* which describes "new concepts of weapons [that] involve the ability to combine various elements to produce types of weaponry never imagined before."[92]

While it is doubtful that Russia and China will form any enduring cyber alliance, they appear to be acting in concert with mutual interest to shape the international legal environment to keep as much control as possible over internal cyber matters without inference from others. In addition to Russia and China, the other two countries mentioned prominently in U.S. public documents are Iran and North Korea. Clapper noted that "Iran and North Korea are unpredictable actors in the international arena. Their development of cyber espionage or attack capabilities might be used in an attempt to either provoke or destabilize the United States or its partners."[93] Of course, there are many other countries that may derive benefit from interfering with U.S. military activities, but they will not be discussed any further here. Instead, let us consider nonstate groups that may influence (positively or negatively) operations in cyberspace.

Nonstate Actors.

Daily, billions of individuals connect to the Internet, each with numerous associations to governmental, commercial, and social groups formed in structures that may range from rigorous to ad hoc fashion. Therefore, there are too many potential nonstate actors (individual and collectives) to list, let alone analyze. To illustrate the prospective roles that certain nonstate entities may play in international cyberspace activities, let us consider three areas that may have the most influence on the implementation of U.S. strategies.

Non-Governmental Organizations and Governing Bodies.

In July 2010, the U.S. Government Accountability Office (GAO) was tasked to examine Internet governance and other aspects of global cyberspace shared interests. They focused on 19 organizations considered by experts as the most important and influential.

> The organizations range from information-sharing forums that are nondecision-making gatherings of experts to private organizations to treaty-based, decision-making bodies founded by countries. Their efforts include those to address topics such as incident response, technical standards, and law enforcement cooperation. These entities have reported ongoing initiatives that involve governments and private industry stakeholders to address a broad set of topics, such as implementation of incident response mechanisms, the development of technical standards, the facilitation of criminal investigations, and the creation of international policies related to information technology and critical infrastructure.[94]

Active participation in these venues provides opportunities to shape international cyberspace infrastructure and functional protocols as well as security policies. Accordingly, the GAO report identifies 73 areas where the roles of U.S. federal entities (primarily Departments of Commerce, Defense, Homeland Security, Justice, and State) include involvement with these organizations. Fulfilling these roles is a complex process and the report notes that "federal agencies have not demonstrated an ability to coordinate their activities and project clear policies on a consistent basis."[95] This may be due in part to the evolving elements

of the overall U.S. strategy regarding cyberspace; the GAO cautions that:

> Unless agency and White House officials follow a comprehensive strategy that clearly articulates overarching goals, subordinate objectives, specific activities, performance metrics, and reasonable time frames to achieve results, the Congress and the American public will be ill-equipped to assess how, if at all, federal efforts to address the global aspects of cyberspace ultimately support U.S. national security, economic, and other interests.[96]

To add to these challenges, other countries as part of their own strategies may be working counter to U.S. efforts with multinational bodies. Clapper noted that "Russia presents a range of challenges to US cyber policy and network security. Russia seeks changes to the international system for Internet governance that would compromise US interests and values." Further, he concludes that, "Internationally, China also seeks to revise the multi-stakeholder model Internet governance while continuing its expansive worldwide program of network exploitation and intellectual property theft."[97]

Malicious Actors.

Unlike groups that strive for cyberspace governance that provides fair and stable access to settings such as the Internet, some actors actually thrive on the unpredictable, uncertain, and vulnerable nature of the same. Such nonstate actors may derive power by their exploitation of cyberspace and may be driven by a variety of motivations—ideology (political or religious), monetary gain, knowledge sharing, or even destruction of societal structures.

Malicious actors of all kinds—terrorists, criminals, hacktivists, thrill-seekers, and so forth—may cause negative effects on critical systems and infrastructure that could be mistakenly attributed to nations and thus entered into the assessment of an attack. Unfortunately, many of these groups may not consider the broader implications of their disruptive activities. Assemblages such as WikiLeaks, LulzSec, and Anonymous may see themselves as "combatants in a war to achieve the goal of Internet freedom" who may take "pride in being unstructured without hierarchy or central authority."[98] Despite this sentiment, these nonstate actors are able to not only coordinate sophisticated attacks, but also provide volunteers with the software necessary to participate:

> The *Operation Payback* was launched by a group of WikiLeaks supporters, after multiple financial service providers stopped their services for WikiLeaks after the latest, massive disclosure of classified US documents. The attacks were carried out by using an open source network attack application called Low Orbit Ion Cannon. The attacks were coordinated by using internet forums, Twitter and some C&C [command & control] servers.[99]

Ironically, even the most extreme of these actors still have a vested interest in maintaining a functional structure in cyberspace from which they can obtain power.[100]

Commercial Sector.

The information and communications systems that form part of cyberspace infrastructure are largely owned and operated by domestic and international

commercial interests. Considering this, the 2009 Cyberspace Policy Review observed that "addressing network security issues requires a public-private partnership as well as international cooperation and norms."[101] The volume of commerce activity that utilizes cyberspace is far from trivial. In June 2011, then Secretary of Commerce Gary Locke stated that industry estimates claim that the Internet "global network helps to facilitate $10 trillion in online transactions every single year."[102] But unfortunately, the security efforts applied across such a magnitude of economic bustle may be spotty and disproportionate:

> Despite increasing awareness of the associated risks, broad swaths of the economy and individual actors, ranging from consumers to large businesses, still do not take advantage of available technology and processes to secure their systems, nor are protective measures evolving as quickly as the threats. This general lack of investment puts firms and consumers at greater risk, leading to economic loss at the individual and aggregate level and poses a threat to national security.[103]

Indeed, recent commercial security breaches demonstrate why this is a concern. The impacts can be substantial, such as the hacks into Target store systems that affected as many as 40 million consumers during the 2013 holiday season.[104] Perhaps more worrisome is the discovery of the Heartbleed vulnerability in the OpenSSL program that may allow criminals to hack over 500,000 websites, many designed to conduct secure business transactions.[105]

Not surprisingly, the volume of commercial activity performed over networks is also not inconsequential and vast amounts of the overall bandwidth availability may be used by a few application groups.

For example, streaming video providers account for a significant portion of Internet usage during peak hours, such as Netflix (32 percent) and YouTube (19 percent).[106] This congestion may make it more difficult for military forces to operate in cyberspace during peak hours and it is reasonable to assume that the demand for cyberspace by news agencies and social media may increase appreciably during a national crisis. This also raises the question: What is the balance of responsibilities between government forces and commercial parties to protect against attacks and mitigate any impacts? A recent study on national cyber security frameworks examined this and observed:

> Three issues are central to the national security debate: how does the government assure the availability of essential services; provide for the protection of intellectual property; and maintain citizen confidence (and safety) when participating in the internet economy? Nations are struggling with finding the appropriate mix of policy interventions and market levers to boost the impacts of ICT [information and communications technology].[107]

While military planners and operators may deem it advantageous to view cyberspace as an operational domain, the policy considerations presented in this section indicate that decisionmakers may have more success using a commons paradigm. With all this in mind, how should we develop and weigh options to assess and respond to potential uses of force in cyberspace?

COURSES OF ACTION

This section examines the influences that course of action development and implementation may have on the assessment of cyberspace incidents. It first looks at the President's role as the primary decisionmaker in U.S. national matters regarding cyberspace. It then surveys key influences affecting subordinate decisionmakers and their staffs that may be advising the commander in chief: reliable situational awareness, global and domestic environment considerations, and options and their related risks and potential consequences. While this is necessary to provide a context and insight into the consequences of the assessment, it is important to remember that this monograph's primary focus is on analyzing incidents and supporting decisionmakers, not on how to choose and implement the appropriate types of responses.

U.S. Implementation: Who Makes the Call?

Assessing a cyberspace incident as a potential use of force, even when armed with frameworks like those depicted in Figure 2, is indeed a mixture of science and art. As articulated in the White House's 2009 *Cyberspace Policy Review*, evaluations of this sort are not optional:

> The Federal government cannot entirely delegate or abrogate its role in securing the Nation from a cyber incident or accident. The Federal government has the responsibility to protect and defend the country, and all levels of government have the responsibility to ensure the safety and wellbeing of citizens.[108]

For such deliberation within the U.S. Government, one thing is clear—the ultimate decision authority is the President:

> Without question, some activities conducted in cyberspace could constitute a use of force, and may as well invoke a state's inherent right to lawful self-defense. In this context, determining defensive response to even presumptively illegal acts rests with the Commander-in-Chief.[109]

Even so, while the overall responsibility belongs to the chief executive, there are many advisors and staffs with varying levels of delegated authority to gather information and synthesize their best advice to support the decisionmaking through constitutional processes.

> It is up to the President to determine when, based upon the circumstances of any event, including a cyberspace event, and the contemplated response that the President intends to proceed with, what consultations and reports are necessary to Congress, consistent with the War Powers Act.[110]

Due to the dynamic nature of not only cyberspace activities but also international happenings in general, Congress tasked DoD to address the following in a 2011 report:

> The necessity of preserving the President's freedom of action in crises and confrontations involving nations which may pose a manageable conventional threat to the United States but which in theory could pose a serious threat to the U.S. economy, government, or military through cyber attacks.[111]

The DoD response outlined measures in three areas: intelligence and situational awareness; defense and resilience; and options of response using all necessary means of national power.[112] While there is no discrete checklist or methodology that will facilitate this process for the President, advisors, and associated staffs, Figure 3 may serve as a general guide. It expands the conceptual framework of Figure 2 for assessing cyberspace incidents to include issues and considerations that should influence the decisionmakers. In implementing the framework, one must balance the demands represented by the various inputs to provide senior decisionmakers with the best possible advice. The influences of national purpose, interests, and policies were covered in the previous section. The influences of the other four inputs are addressed in the remainder of this section.

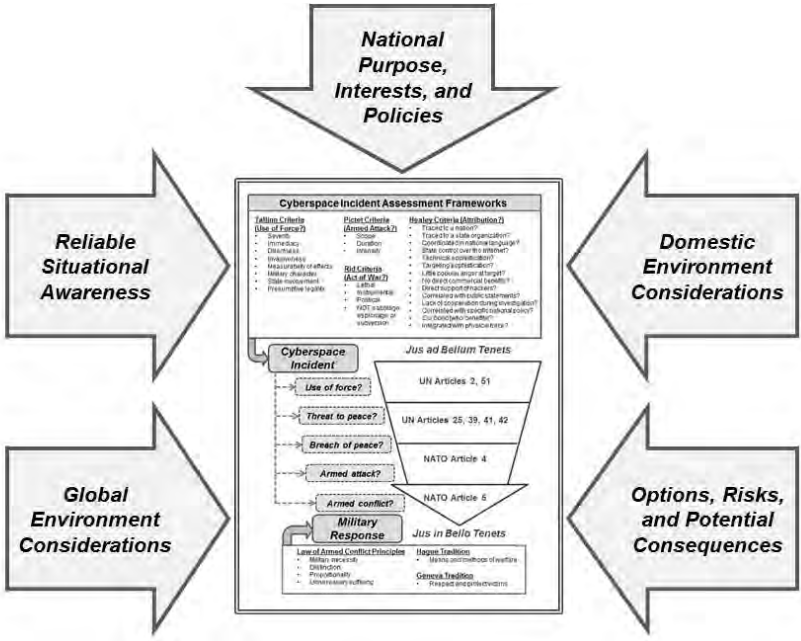

Figure 3. Course of Action Influences on Cyberspace Incident Assessment.

Reliable Situational Awareness.

Incident Reporting.

Reliable situational awareness is critical to the assessment of incidents in cyberspace. How do the President and other government officials get such information? In October 2009, then Secretary of Homeland Security Janet Napolitano established the National Cybersecurity and Communications Integration Center (NCCIC):

> This 24-hour watch and warning center serves as the nation's principal hub for organizing cyber response efforts and maintaining the national cyber and communications common operational picture. DHS [Department of Homeland Security] also works with the private sector, other government agencies and the international community to mitigate risks by leveraging the tools, tradecraft, and techniques malicious actors use and converting them into actionable information for all 18 critical infrastructure sectors to use against cyber threats. [113]

As this description indicates, the focus of the NCCIC is on the "dot gov" portion of the Internet, as well as broader protection of the nation's critical infrastructures and coordination with the private sector. DoD has a more narrow focus on protecting the "dot mil" network as well as evaluating potential threats that may require military actions as part of a response. A 2011 DoD report to Congress noted that:

> As in the physical world, a determination of what is a "threat or use of force" in cyberspace must be made in the context in which the activity occurs, and it in-

> volves an analysis by the affected states of the effect and purpose of the actions in question.[114]

So how does the military accomplish this evaluation? In his confirmation hearings before a senate committee in March 2014, the current Commander, U.S. Cyber Command, Admiral Michael Rogers provided some insight with regard to this question:

> DoD has a set of criteria that it uses to assess cyberspace events. As individual events may vary greatly from each other, each event will be assessed on a case-by-case basis. While the criteria we use to assess events are classified for operational security purposes, generally speaking, DoD analyzes whether the proximate consequences of a cyberspace event are similar to those produced by kinetic weapons.[115]

Initial Responses.

In theory, these processes all sound sufficient, but how are they being implemented? The current applications entail an evolving relationship between DoD and DHS that was initially formalized in the October 2010 Memorandum of Agreement (MOA) signed by secretaries Gates (DoD) and Napolitano (DHS) and designed:

> to set forth terms by which DHS and DoD will provide personnel, equipment, and facilities in order to increase interdepartmental collaboration in strategic planning for the Nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities.[116]

One month before the MOA was released, DHS completed its interim National Cyber Incident Response Plan (NCIRP) which:

> provides a framework for effective incident response capabilities and coordination between federal agencies, state, and local governments, the private sector, and international partners during significant cyber incidents.[117]

The NCIRP has been tested in several "Cyber Storm" exercises sponsored by DHS and supported by multiple and diverse representatives from federal, state, and local governments as well as international and industry partners.[118] Despite this, the area of incident reporting remains a work in progress with many of the limitations noted in 2010 by the GAO being actively worked:

> Although multiple federal agencies are parties to information-sharing or incident-response agreements with other countries, the federal government lacks a coherent approach toward participating in a broader international framework for responding to cyber incidents with global impact. U.S. and European government officials, members of the private sector, and subject matter experts told us that establishing an effective international framework for incident response is difficult for multiple reasons, including the national security concerns associated with sharing potentially sensitive information, the large number of independent organizations involved in incident response, and the absence of incident response capabilities within some countries.[119]

In his final testimony in February 2014 as Commander, U.S. Cyber Command, General Keith Alex-

ander described the progress made in the DoD evaluation and reporting of significant cyberspace events:

> USCYBERCOM, for instance, has been integrated in the government wide processes for National Event responses. This regularly exercised capability will help ensure that a cyber incident of national significance can elicit a fast and effective response at the right decisionmaking level, to include pre-designated authorities and self-defense actions where necessary and appropriate.[120]

Each military service has also developed similar information and reporting systems to serve both their own unique service-related cyber component requirements as well as integrate into the sub-unified structure of USCYBERCOM.[121] Specific to potential cyberspace attacks, General Alexander noted:

> Should an attack get through, or if a provocation were to escalate by accident into a major cyber incident, we at USCYBERCOM expect to be called upon to defend the nation. We plan and train for this every day. My Joint Operations Center team routinely conducts and practices its Emergency Action Procedures to defend the nation through interagency emergency cyber procedures. During these conferences, which we have exercised with the participation up to the level of the Deputy Secretary of Defense, we work with our interagency partners to determine if a Cyber Event, Threat or Attack has occurred or will occur through cyberspace against the United States. As Commander, USCYBERCOM, I make an assessment of the likelihood of an attack and recommendations to take, if applicable. We utilize this process in conjunction with the National Military Command Center (NMCC) to determine when and if the conference should transition to a National Event or Threat Conference.[122]

The purpose of this monograph is not to critique existing command and control functions of military cyberspace actions; rather, it is to understand in general terms how they may provide actionable information for decisionmakers. But these processes cannot operate in a vacuum; let us explore some of the factors identified in Figure 3 that should influence the overall cyberspace incident assessment methodology.

Global Environment Considerations.

*Crime, Espionage, and Terrorism***.**

To establish a realistic context of the global cyberspace environment, it is essential to acknowledge how crime, espionage, and terrorism are viewed as well as how they are differentiated from use of force. The U.S. *International Strategy for Cyberspace* clearly separates "protection from crime" from "right of self-defense" and outlines the expectation for international law enforcement:

> In the case of criminals and other non-state actors who would threaten our national and economic security, domestic deterrence requires all states to have processes that permit them to investigate, apprehend, and prosecute those who intrude or disrupt networks at home or abroad. Internationally, law enforcement organizations must work in concert with one another whenever possible to freeze perishable data vital to ongoing investigations, to work with legislatures and justice ministries to harmonize their approaches, and to promote due process and the rule of law—all key tenets of the Budapest Convention on Cybercrime.[123]

The Budapest (Council of Europe) Convention on Cybercrime began in 1997, was opened for signature

in November 2001, and has been ratified by at least 42 countries. Its provisions focus on criminal offenses in four categories: fraud and forgery, child pornography, copyright infringement, and security breaches.[124] A Yale Law School comparison of crime and war in cyberspace offers a similar scope for cyber crime:

> Cyber-crime is generally understood as the use of a computer-based means to commit an illegal act . . . thus often defined by its means—that is, a computer system or network. As such, cyber-crime encompasses a very broad range of illicit activity. Among the priorities of the Department of Justice and FBI [Federal Bureau of Investigation] units addressing cyber-crime are fraudulent practices on the Internet, online piracy, storage and sharing of child pornography on a computer, and computer intrusions.[125]

The broader implications of cyber crime as a global threat is offered by Clapper:

> Cyber criminal organizations are as ubiquitous as they are problematic on digital networks. Motivated by profit rather than ideology, cyber criminals play a major role in the international development, modification, and proliferation of malicious software and illicit networks designed to steal data and money. They will continue to pose substantial threats to the trust and integrity of global financial institutions and personal financial transactions.[126]

But will the results of nonstate criminal events be sufficiently dissimilar from the potential effects of actions taken by state forces? Perhaps not in all cases, according to the Yale Law study:

> While the distinction between cyber-crime and cyber-attack is important, we acknowledge that it often will

> not be readily apparent at the moment of the cyber-event whether it is one or the other (or both)—in part because the identity and purpose of the actor may not be apparent.[127]

Thus, the problem is that it may be difficult to distinguish up front that a given incident in cyberspace with negative effects is criminal or the initiation of a use of force. This same problem with distinction may extend to the areas of espionage and terrorism since, from the victim's perspective, there may not be clear cause-and-effect evidence available to evaluation the situation.

As discussed earlier, espionage conducted by state entities is generally acknowledged as a tradition ritual among nations that is distinct from armed conflict. But facilitated by cyberspace means, the practice of industrial and economic espionage is changing in scope and sophistication as concluded in a 2011 report by the Office of the National Counterintelligence Executive:

> Foreign collectors of sensitive economic information are able to operate in cyberspace with relatively little risk of detection by their private sector targets. The proliferation of malicious software, prevalence of cyber tool sharing, use of hackers as proxies, and routing of operations through third countries make it difficult to attribute responsibility for computer network intrusions. Cyber tools have enhanced the economic espionage threat, and the Intelligence Community (IC) judges the use of such tools is already a larger threat than more traditional espionage methods.[128]

Adding to the complexity and sensitivity of this issue is that the activity is not limited to countries that are considered adversarial. Surprisingly, it is also

common among friendly nations, as the same report posited:

> Some US allies and partners use their broad access to US institutions to acquire sensitive US economic and technology information, primarily through aggressive elicitation and other human intelligence (HUMINT) tactics. Some of these states have advanced cyber capabilities.[129]

Terrorist organizations are also gaining access to advanced cyber capabilities, often using criminal profits to fund their efforts. Clapper stated that "terrorist organizations have expressed interest in developing offensive cyber capabilities. They continue to use cyberspace for propaganda and influence operations, financial activities, and personnel recruitment."[130] The attribution of terrorism acts conducted by nonstate actors must consider if the culprits were condoned or even supported by a legitimate state. If the latter were true, it should be a significant element in determining the motivation and intent of other state actions in cyberspace. Given that we can winnow these certain cyberspace incidents, what pragmatic factors should be in play during further evaluation of cyber incidents to distinguish those related to use of force?

*Pragmatic Factors for Decisionmakers***.**

Providing the best analysis and advice to decisionmakers for the discrimination of hostile actions in cyberspace activities requires consideration of the "what next" implications. Recall that Rid posited that war must include instrumental and political aspects—how might these emerge if the President decides to direct a military response to an event deemed to be

an act of force in cyberspace? DoD provided part of this answer in response to questions from Congress in November 2011:

> Cyber operations might not include the introduction of armed forces personnel into the area of hostilities. Cyber operations may, however, be a component of larger operations that could trigger notification and reporting in accordance with the War Powers Resolution [Public Law 93-148]. The Department will continue to assess each of its actions in cyberspace to determine when the requirements of the War Powers Resolution may apply to those actions.[131]

However, initiation of the War Powers Resolution applies to "situations where imminent involvement in hostilities is clearly indicated by the circumstances."[132] Jason Healey and A. J. Wilson developed a model mapping cyberspace force "logic presence" against what might be considered an equivalent physical presence of forces that are more familiar to advisors. It ranges from an outside country's simple connection to the public Internet up to a long-term campaign of manipulating foreign systems. Importantly, they integrate requirements for congressional notification as hostilities progress.[133] While not an authenticated methodology, it has value that merits possible incorporation into an advisor's kit bag.

If the decision is made to use U.S. military forces, what resources will be available to the commander in chief? The centerpiece of the cyberspace element is the Cyber Mission Force:

> The Force includes Cyber Protection Forces that operate and defend the Department's networks and support military operations worldwide, Combat Mission Forces that support Combatant Commanders as they

> plan and execute military missions, and National Mission Forces that counter cyberattacks against the United States.[134]

The Force is scheduled to be staffed initially by 2016 with an impressive number of teams available by fiscal year 2019:

- 13 National Mission Teams with 8 National Support Teams
- 27 Combat Mission Teams with 17 Combat Support Teams
- 18 National Cyber Protection Teams (CPTs)
- 24 Service CPTs
- 26 Combatant Command and DoD Information Network CPTs[135]

One of the biggest challenges in implementing cyberspace operations is the development of a cadre of expert planners and their socialization into the greater military community. In a recent article, Jason Bender, one of the vanguards of this evolving group, offered insight into how this might be accomplished:

> In the case of the institution, the services must pursue broad and comprehensive common-core education for all potential commanders and planners regarding cyberspace operations. Doctrinal publication classifications must be carefully and appropriately overcome in order to get the word to the masses and educate them on the realm of the possible in terms of the operational environment relative to the cyberspace domain, the operational process, and fires and targeting.[136]

One of the greatest variables in this process depicted in Figure 3 is the personalities and propensities of not only the top decisionmaker, but also of the

intermediate leaders and their staffs. While this is not unique to cyberspace-related issues, the dynamic nature of the domain and the speed of operational execution may intensify the effects of decisions over those in the traditional domains. Some have argued from corporate experiences that intuitive leaders may function better within a complex adaptive system than leaders that favor rational approaches to decisionmaking and problem solving.[137] In truth, there are few, if any, leaders with sufficient experience in cyberspace matters to be able to claim intuition and the system dynamics of the domain change faster than any human can perceive, thus calling into question any deference to rational models. So what is to be done? Jody Prescott, Senior Fellow, West Point Center for the Rule of Law, examines the challenge of "building the ethical cyber commander" who must lead within a realistic framework that recognizes the increasing use of human computer interfaces and autonomous decision making processes (ADPs):

> Given the likely speed at which future cyber operations would occur, not only will commanders need to accelerate their decision making, but will also likely need to use ADPs as part of their arsenal in order to maintain their operational effectiveness. The ethical and legal challenges posed by reliance upon this sort of technology must be explored fully to ensure that possible solutions are consistent with the overarching social, political, and legal norms we expect our military personnel to meet as they conduct operations on our behalf.[138]

Even when equipped with the skills and guided by principles listed here, the ethical cyber leader must be able to comprehend that others in the world may not

share their same values and thus perceive events and actions differently.

Perceptions, Intentional and Unintentional.

Even when a hostile cyberspace event occurs that is internationally validated as an armed attack, there is no explicit requirement for a head of state to respond. There are risks inherent in the three possible outcomes of doing nothing, retaliating appropriately, or retaliating inappropriately. RAND fellow Martin Libicki studied the possible repercussions of these outcomes to a country's ongoing deterrence and attack effectiveness.[139] Doctoral student Timothy Junio questions the assumption that treating states as unitary rational actors is sufficient for modeling complex international interactions involving cyberspace. He outlines potential theoretical paradigms that incorporate bargaining theory modified to accommodate information technology factors. Less stringent than the unitary rational actor model, "the principal-agent approach, for instance, works with the premise that individuals and organizations often vary in their incentives and preferences, which could make war beneficial for some at the cost of other."[140]

Practicing appropriate transparency with regard to U.S. cyberspace force issues can help allay trepidation among friends and competitors. Regardless of the merits of the DoD Strategy and the U.S. Cyber Command structure, one has to critique the lack of adherence to proper strategic communication principles when it was unveiled to the world writ large. Certainly, the unexpected announcement by Secretary Gates did not seem well coordinated with the Department of State and thus gave skeptical nations reasonable cause

for further suspicion regarding the U.S. activities in cyberspace. The assessment of the GAO was:

> In addition, DoD and Department of State officials acknowledged that the announcement of the Secretary of Defense's decision to establish the Cyber Command was not coordinated with the Department of State, although DoD officials stated that the department had shared the purpose, intent, and mission with other agencies, including the Department of State. Nevertheless, the announcement was perceived by several foreign governments and other entities as a potentially threatening attempt by the U.S. government to militarize cyberspace, according to recognized experts.[141]

Other examples of how intentions may be viewed differently include some of the reactions to the release of the *Tallinn Manual* which was criticized by Russia as a product focused on "the rules for prosecuting cyber warfare" while Russia is "trying to prevent militarization of cyberspace by urging the international community to adopt a code of conduct in this sphere."[142] While this can be viewed as political maneuvering in line with Russia's stated policy views, it illustrates that even a product with vast consensus may still present some controversy. Congress specifically queried DoD regarding how the discovery of its penetrations of foreign networks for intelligence gathering might "cause the targeted nation to interpret the penetration as a serious hostile act." The DoD response pointed to the long history of espionage practiced in both directions between states and admitted that:

> The United States Government collects foreign intelligence via cyberspace, and does so in compliance with all applicable laws, policies, and procedures. The conduct of all U.S. intelligence operations is

> governed by long-standing and well-established considerations, to include the possibility those operations could be interpreted as a hostile act.[143]

However, they should also recognize that the dual-hatted commander status of U.S. Cyber Command and the National Security Agency may send mixed messages to the international community as well as provide grist for the propaganda mills of potential adversaries.

Domestic Environment Considerations.

For national decisionmaking regarding the judgment of a given cyberspace incident, the President as chief executive may be considered the point where the legal federal authorities stipulated in U.S. Code converge—that is, the White House is "where the buck stops" for U.S. actions in cyberspace. The evaluation process for actions in cyberspace should be supported by many different government organizations as part of the roles and responsibilities; the major duties related to these undertakings can be found in the following portions of the U.S. Code:

- Title 6: Domestic Security (Department of Homeland Security
- Title 10: Armed Force (Department of Defense)
- Title 18: Crimes and Criminal Procedure (Department of Justice)
- Title 22: Foreign Relations and Intercourse (Department of State)
- Title 32: National Guard
- Title 40: Public Buildings, Property, and Works
- Title 44: Public Printing and Documents (National Security Systems)

- Title 50: War and National Defense (Intelligence Community)
- Title 51: National and Commercial Space Programs[144]

Unless properly integrated and synchronized, the results from this diverse federal lineup may be disjointed. Alexander promulgated the teamwork necessary to achieve unity of effort in his February 2014 congressional testimony:

> Our new operating concept to enhance military cyber capabilities is helping to foster a whole-of-government approach to counter our nation's cyber adversaries. Indeed, USCYBERCOM planners, operators, and experts are prized for their ability to bring partners together to conceptualize and execute operations like those that had significant effects over the last year in deterring and denying our adversaries' cyber designs.[145]

But even when everyone desires to work together, there will inevitably be seams and overlaps of conflicting intents for shared resources. For example, how are the interests of public and private interests weighed in the selection of targets for intelligence collection and possible attack? Rogers addressed this exact question during his March 2014 senate testimony:

> The Tri-lateral Memorandum of Agreement contains a deconfliction mechanism involving DoD, DoJ [Department of Justice], the Intelligence community and agencies outlined in, and reinforced by PPD [Presidential Policy Directive]-20. Disagreements are handled similar to those internal to DoD; the issue is forwarded from the Seniors involved to the Deputies then on to the Principals Committee with the final stop being the President in cases where equities/gain-loss are ultimately resolved.[146]

Industry and Commercial.

Even if the complexities and challenges of coordinating separate federal functions toward a common goal are fully resolved, this may not be sufficient. In many cases, the evaluation of cyberspace incidents and any consideration of possible military responses should expand from a whole-of-government approach to a whole-of-nation approach. This principle was articulated in the White House 2009 *Cyber Policy Review*:

> The private sector, however, designs, builds, owns, and operates most of the digital infrastructures that support government and private users alike. The United States needs a comprehensive framework to ensure a coordinated response by the Federal, State, local, and tribal governments, the private sector, and international allies to significant incidents. Implementation of this framework will require developing reporting thresholds, adaptable response and recovery plans, and the necessary coordination, information sharing, and incident reporting mechanisms needed for those plans to succeed. The government, working with key stakeholders, should design an effective mechanism to achieve a true common operating picture that integrates information from the government and the private sector and serves as the basis for informed and prioritized vulnerability mitigation efforts and incident response decisions.[147]

However, this more holistic practice may introduce additional areas of overlapping responsibility. For example, one of the unresolved questions in Koh's presentation to U.S. Cyber Command centered on how the United States should treat dual-use infrastructure in cyberspace:

> Parties to an armed conflict will need to assess the potential effects of a cyber attack on computers that are not military objectives, such as private, civilian computers that hold no military significance, but may be networked to computers that are valid military objectives. Parties will also need to consider the harm to the civilian uses of such infrastructure in performing the necessary proportionality review.[148]

Under the National Cyber Incident Response Plan framework, DoD is assigned to assist protection efforts for the Defense Industrial Base as well as private sector critical infrastructure and key resources.[149] In his March 2014 congressional testimony, Rogers provided further details regarding the government's expectations of private sector effort to defend themselves in cyberspace:

> I believe that mission assurance and the protection of our critical infrastructure is an inherent obligation of all, not just DoD, DHS, DOJ/FBI and our government. In many cases, mission assurance relies on the provision, management, or facilitation of critical infrastructure lies in the private sector. Defensive measures could include not just automated capabilities to prevent or respond, but also adherence to proper standards of network security, administration, sharing of threat and vulnerability information, and compliance. These are as critical to protection of infrastructure as is military or cyber might. In almost any scenario, collaboration and information sharing across private and public, governmental and non-governmental organizations will be a key to successful outcomes.[150]

Of course, this expectation of corporate self-defense may lead to some interesting situations. For example, what is the limit to which an industry entity

may go to stop an ongoing or imminent criminal act in their networks? Will they be allowed to legally "hack back" at the criminals? The concept of privateering has reemerged as a possible, if not pragmatic, part of the national effort. In theory, entrepreneurial cyberspace experts would be issued the equivalent of a letter of marque that would serve as a government license for them to attack and capture cyber criminals considered to be enemies of the issuing nation. Cyberspace researcher Michael Tanji noted potential benefits as well as pitfalls to incorporating this:

> Privateering is arguably the most economical, technically feasible and historically relevant approach to the problem. Despite serious legal hurdles, privateering is precedence, and where is precedence valued more than in the law?

Privateering would require a strong, independent and transparent mechanism for validating activity since the potential for abuse would be strong. There is no shortage of events that could potentially qualify for privateer action, so much so that there will probably be a temptation over time to make the language in letters more ambiguous or to issue a "blanket" letter that takes responsibility for deciding when to act out of the hands of the government.[151]

Private Citizens.

Similar in concept to the "hack back" dilemma for corporations is the emerging trend of "patriot hacking" for individuals. This concept is explored in a NATO-sponsored book on international cyber incidents:

> "Patriot hacking" (or "patriotic hacking") is a term that reflects citizen involvement with hacking or cyber attacking the systems of a perceived adversary (e.g. another government or nation).
>
> Patriot hacking is often used as a response against a country's political decision that the country where the particular hacker or group of hackers originates from openly or presumably disapproves. As such, patriot hacking is performed by a group of people who take action "pro patria" [for one's country] in cases where they believe that this is the right thing for their government to do or where they perceive the government as unable to do "the right thing."[152]

There are also cases where computers located in the United States have been used as part of robot networks (botnets) in attacks. For example, recall that the landmark denial of service attacks on Estonia in 2007 involved computers from 178 countries.[153] Participation in botnets by private citizens may be willing (e.g., part of Anonymous) or unwilling (e.g., computer controlled by malware). In either case, there is still ongoing debate internationally with regard to what responsibilities sovereign countries have for controlling these types of cyberspace deeds within their boundaries. While there is no clear way ahead for these issues, it is clear that they require collaborative work between the public and private sectors, and that this combined effort must protect the privacy of all citizens. Rogers has reiterated this priority:

> The nature of malicious cyber activity against our nation's networks has become a matter of such concern that legislation to enable real-time cyber threat information sharing is vital to protecting our national and economic security. Incremental steps such as legisla-

> tion that addresses only private sector sharing would have limited effectiveness, because no single public or private entity has all the necessary authorities, resources, or capabilities to respond to or prevent a serious cyber attack. Therefore, we must find a way to share the unique insights held by both government and the private sector. At the same time, legislation must help construct a trust-based community where two-way, real-time sharing of cyber threat information is done consistent with protections of U.S. person privacy and civil liberties.[154]

Options, Risks, and Potential Consequences.

When complex analyses are performed in time-critical situations with potentially dire consequences, it may be possible to get lost in the details and lose sight of the overall objective. Thus, it is prudent to integrate sanity checks as options are developed to support both the assessment of cyberspace incidents as well as any responses they might entail. The traditional framework of considering the feasibility, acceptability, and suitability of proposed courses of actions could serve this purpose well.

To provide simplicity and clarity to the distinction of cyberspace events, it may be tempting to identify and communicate specific actions to other countries that would serve as clear "triggers" or "red lines" to authenticate an attack as well as the U.S. response that it merits. As argued here, the complex and dynamic nature of cyberspace is beyond that of traditional domains, and therefore any preconceived evaluation runs the risk of being obsolete before it is implemented. Certainly, this presents challenges to the traditional planner mindset of having an off-the-shelf solution available, but such a tenet serves perhaps the greater

need of maintaining flexibility of action. Also, defining clear "no go" lines for potential adversaries provides a *de facto* approved operational envelope that may not be advantageous for long-term security.

Some of these triggers may already be in place unknowingly in the form of delegated authorities and automated cyber defense (ACD) mechanisms at the tactical level (e.g., antivirus software). The *Department of Defense Strategy for Operating in Cyberspace* indicates that ACD is an integral part of military cyber operations:

> Active cyber defense is DoD's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DoD networks and systems, supplementing best practices with new operating concepts. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems.[155]

Alexander stated in February 2014 that similar procedures are integrated in national event responses:

> This regularly exercised capability will help ensure that a cyber incident of national significance can elicit a fast and effective response at the right decisionmaking level, to include pre-designated authorities and self-defense actions where necessary and appropriate.[156]

Surely such measures can contribute to a neater and more expedient process—but will the results match the designers' expectations and the users' needs? How will unintended nth-order effects—the emergent cases from the interactions of a complex adaptive system—be presented to and considered by

decisionmakers? Fortunately, the significance of this concern is addressed in another of the unresolved questions posed by Koh:

> How can a use of force regime take into account all of the novel kinds of effects that states can produce through the click of a button? . . . As you all know, however, there are other types of cyber actions that do not have a clear kinetic parallel, which raise profound questions about exactly what we mean by "force."[157]

Ironically, it is a necessary paradox that one must give up tactical control of operations in cyberspace that are beyond human comprehension in order to gain control—or at least perceived control—over broader capabilities facilitated by vast collectives like the Internet. Yet, the implementation of autonomous functions should be evaluated with critical skepticism to avoid the extreme possibility of initiating a series of events that synchronize with similar systems of an adversary. In the worst case, mutual escalation could culminate in a "decisionless war" fought with multiple salvos in cyberspace occurring in the milliseconds it takes for military operators to comprehend the changed icon on their computer screen.

The serious nature of these implications may be exacerbated if cyberspace operations are more formally integrated into our nation's strategic deterrence framework. A January 2013 Defense Science Board study examined potential mutually supporting roles of global conventional strike forces, nuclear forces, and offensive cyberspace forces. The board posited that the rise of nations which may pose a strategic cyber threat to the United States warrants incorporation of "cyber survivable strike capability" into U.S. strategic forces:

> To provide a non-nuclear but cyber survivable escalation ladder between conventional conflict and the nuclear threshold—that is to increase stability and build a new sub-nuclear red line in this emerging era of a cyber peer competitor delivering a catastrophic attack.[158]

Perhaps such extrapolation may be viewed as alarmist in nature and one would certainly hope that events like these never manifest. Still, as a trite truism observes, "hope is not a strategy," and the best way to avoid future calamity is to actively and prudently investigate and mitigate the circumstances that may catalyze them.

RECOMMENDATIONS

This monograph addresses many topics relevant to the challenge of distinguishing acts of war in cyberspace. For improving the existing processes involved in this continuing endeavor, it recommends the following actions be incorporated:

- In assessing cyberspace incidents, embrace the full context and consequences as well as legal and technical criteria. Consider using the methodology depicted in Figure 3 as a starting point to build upon.
- Adopt a commons paradigm of cyberspace for any operations above the tactical level to fully embrace the full scope of operations on any global network (such as the Internet).
- Expand the military cyber operational spectrum to delineate the ultra-tactical realm—that is, actions that occur below the threshold of human comprehension. Incorporate the dynamics of complex adaptive systems with emergence into any modeling of this realm.

- Adopt future-facing paradigms to evaluate cyberspace assessment challenges in a proactive matter—that is, go beyond precedent-based legal and technical analysis and consider innovations that may be adopted by potential allies or aggressors.
- Assess where biases may be in the design and implementation of assessment mechanisms and methodologies. This should include examination of biases in information gathering and incident reporting.
- Study potential extreme implications for automated cyber defense, especially as it may relate to conflict escalation as well as the replacement of any decisionmaker cognitive processes.
- Examine how preemptive defense measures allowable under international law may apply in cyberspace as well as their potential benefits and risks.

CONCLUDING REMARKS

Determining an act of war is not a *fait accompli* in the traditional domains. In fact, it often involves sophisticated interactions of many factors that may be outside the control of the parties involved; the dynamic and complex nature of cyberspace makes such a task even more difficult. The result of the combined aspects of speed, perception limitation, and system complexity may have far-reaching implications for the reliability of information presented to support decisionmaking in the cyberspace domain. While military planners and operators may deem it advantageous to view cyberspace as an operational domain, diverse policy considerations indicate that decisionmakers may have more success using a commons paradigm.

Providing the best analysis and advice to decisionmakers for the discrimination of hostile actions in cyberspace activities requires consideration of the "what next" implications, thus it is important to consider possible responses and their implications up front in the process. Accordingly, it may be prudent to exercise caution in developing and implementing decision criteria (e.g., red lines) that are too explicit (or automated). We must also expect and accept that other nations may reasonably apply the criteria we develop to our own actions in cyberspace. Such determination should not be the exclusive purview of the legal, information technology, or intelligence communities.

But in addition to the technical, legal, and bureaucratic difficulties facing decisionmakers as they try to visualize the infinitely intricate composition of cyberspace is that these efforts may be hampered by the lack of a thoughtful and forward-thinking U.S. grand strategy. Perhaps we can learn lessons from the relatively new domain of space. In the heydays of the 1960s, there were vast amounts of resources poured into human space flight programs, all without a clear concept of how such space operations fit into national security, let alone into long-term national strategies. One can argue that the end result was the slow devolution from the U.S. victory in the moon race to the ironic position 5 decades later where U.S. astronauts must use Russian rockets to reach the International Space Station. In the end, one might observe that strategy-wise, the United States plays checkers, Russia plays chess, and China plays go. Perhaps it is time to up our game.

ENDNOTES

1. "Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934," Washington, DC: Department of Defense, November 2011, p. 9.

2. Ellen Nagashima, "When Is a Cyberattack an Act of War?" *The Washington Post*, October 26, 2012.

3. Thomas Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies*, Vol. 35, No. 1, February 2012, pp. 5-32.

4. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," Chap. 2 of *Cyberpower and National Security,* Washington DC: National Defense University Press and Potomac Books, 2009, pp. 24-42.

5. Department of the Army, *Training and Doctrine Command Pamphlet 525-7-8, Cyberspace Operations Concept Capability Plan 2016-2028,* Washington, DC: U.S. Government Printing Office, February 22, 2010.

6. Jeffrey L. Caton, "What do Senior Leaders Need to Know about Cyberspace," Derrick Neal *et al*., eds., *Crosscutting Issues in International Transformation: Interactions and Innovations among People, Organizations, Processes, and Technology*, Washington DC: National Defense University, 2009, pp. 207-228.

7. Joint Chiefs of Staff, *Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms*, Washington, DC: U.S. Government Printing Office, November 8, 2012 (as amended through February 15, 2014), p. 64.

8. The author advocates the inclusion of the phrase "and their operators" to this definition to capture all characteristics of cyberspace.

9. For a differing view on this debate, see John Knowles, "Why Two Domains are Better than One," *The Journal of Electronic Defense*, Vol. 36, No. 3, May 2013, pp. 48-50. See also *Army Field Manual 3-38, Cyber Electromagnetic Activities*, February 2014, available from *armypubs.army.mil/doctrine/Active_FM.html*.

10. John McCain (Ranking Member) and Carl Levin (Chairman), U.S. Senate Committee on Armed Services letter to Secretary of Defense Leon Panetta (no subject), Washington, DC: U.S. Senate, July 20, 2011. The letter also noted that this is not a new task for DoD and that it, in fact, was over 18 months old: "Senior DoD leaders including the Vice Chairman of the Joint Chiefs of Staff and the Principal Deputy Undersecretary of Defense for Policy, informed the Committee that your predecessor would present this report to the Committee by the end of 2010; however, that commitment remains unfulfilled."

11. *Ibid*.

12. Arthur K. Cebrowski, "Transformation and the Changing Character of War?" *Transformation Trends*, June 17, 2004, available from *www.au.af.mil/au/awc/awcgate/cia/nic2020/ceb_transformation-25may04.pdf*. Also see Jeffrey L. Caton, "Cyberspace and Cyberspace Operations" in *Information Operations Primer, AY 2011*, Carlisle Barracks, PA: Center for Strategic Studies, November 2011, pp. 19-20. The unique aspects of cyberspace as a global common are offered by Caton as:

> When considered as a strategic commons (or global commons), cyberspace has at least five unique characteristics. First, the cost of entry and access to cyberspace is low—basically the cost of a laptop and Internet café fee. Second, cyberspace offers a degree of anonymity that challenges efforts to detect, track, and target a specific user who desires to hide in the common. Third, cyberspace provides the ability to initiate a variety of physical effects across vast distances at almost instantaneous speeds. Fourth, cyberspace is an ever-growing common mostly owned and operated by private individuals and corporations; it expands with every new computer server or Internet-capable mobile device. Finally, cyberspace does not have traditional dimensions of height, depth, and length, but it does have unique metrics that can be used to map its boundaries and operations.

13. Kuehl, p. 38.

14. Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Washington, DC: Cyber Conflict Studies Association, 2013, p. 85.

15. Haly Laasme, "Estonia: Cyber Window into the Future of NATO," *Joint Force Quarterly,* No. 63, 4th Quarter, 2011, pp. 58-63.

16. Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters*, Vol. 38, No. 4, Winter 2008-09, pp. 60-76.

17. William F. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, Vol. 89, No. 5, September/October 2010, pp. 97-108.

18. Paul Rexton Kan, "Examining Warfare in Wi-Fi: Cyberwar to Wikiwar: Battles for Cyberspace," *Parameters*, Vol. 43, No. 3, Autumn 2013, pp. 111-118. This is an article that provides an excellent and concise review of five recent books: Richard Clarke's *Cyber War: The Next Threat to National Security and What to Do About It* (2010); Thomas Rid's *Cyber War Will Not Take Place* (2013); Julian Assange's *Cyberpunks: Freedom and the Future of Internet* (2012); Parmy Olson's *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency* (2012); and Rodolphe Durand and Jean-Philippe Vergne's *The Pirate Organization: Lessons from the Fringe of Capitalism* (2013).

19. Rid, p. 6.

20. Joint Chiefs of Staff, *JP 1-02,* p. 64.

21. Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, report prepared for The U.S.-China Economic and Security Review Commission," McLean, VA: Northrop Grumman Corporation, October 9, 2009. Specialization among Chinese operators has been observed in the employment of the cyber forces as small groups with specialized skills and tasks, such as reconnaissance, breach, and collection teams.

22. Jeffrey L. Caton, "On the Theory of Cyberspace," Chap. 23, J. Boone Bartholomees, Jr., ed., *U.S. Army War College Guide to National Security Issues, Volume I: Theory of War and Strategy,* 5th Edition, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, June 2012, pp. 325-343.

23. U.S.-China Economic and Security Review Commission, "2010 Report to Congress of the U.S.-China Economic and Security Review Commission," Washington DC: U.S. Government Printing Office, November 2010. The report included an account of an incident in April 2010 where a large number of routing paths to various Internet Protocol addresses were redirected through networks in China for 17 minutes, giving the network server operators the ability to read, delete, or edit e-mail and other information sent along those paths by U.S. Government, military, and business sites. Such incidents raise questions about whether potential adversaries could develop and leverage these abilities intentionally to assert some level of control over the Internet, even if only for a brief period.

24. Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32. Stuxnet Dossier Version 1.4," Cupertino, CA: Symantec Corporation, February 2011.

25. Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, CA: RAND Corporation, 2009.

26. Matthew Waxman, "When is a Cyberattack an Act of War?" *Lawfare: Hard National Security Choices*, October 28, 2012, available from *www.lawfareblog.com/2012/10/when-is-a-cyberattack-an-act-of-war/*.

27. Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," Cyber Statecraft Initiative Issue Brief, Washington, DC: The Atlantic Council, 2011. The full spectrum of state responsibility for cyber attack developed by the author is: 1. State-prohibited; 2. State-prohibited-but-inadequate; 3. State-ignored; 4. State-encouraged; 5. State-shaped; 6. State-coordinated; 7. State-ordered; 8. State-rogue-conducted; 9. State-executed; and 10. State-integrated.

28. "Statement Of General Keith B. Alexander, Commander, United States Cyber Command, Before the Senate Committee on Armed Services," Washington, DC: U.S. Senate, March 12, 2013, p. 7. See also "Advance Questions for Vice Admiral Michael S. Rogers, U.S. Navy (USN) Nominee for Commander, United States Cyber Command," Washington, DC: U.S. Senate, March 11, 2013,

p. 10. Alexander's successor reiterated the speed and complexity of cyberspace operations:

> Regardless of the target—assuming that the adversary has somehow developed the access—the physics of the cyberspace domain and the technology supporting it make it easier for an adversary to hide or obfuscate his capability, attack vector, and location, and deliver an effect on his target either singularly or repeatedly within milliseconds.

29. The following notional values were used to develop Figure 1 (speeds shown here in miles per hour [MPH]). The ovals drawn around these plotted values provide allowance for variances of other movements in domains.

Land: (lower) Soldier: 4 MPH; (upper) Bradley Fighting Vehicle: 41 MPH

Sea: (lower) Submerged Submarine: 20 MPH; (upper) Aircraft Carrier: 36 MPH

Air: (lower) UH-60 Helicopter: 180 MPH; (upper): SR-71 Jet: 2,200 MPH

Space: (lower) geosynchronous orbit: 6, 935 MPH; (upper) low earth orbit: 17,400 MPH

Munition: (lower) M-4 muzzle: 2,900 MPH; (upper) Minuteman ICBM: 15,000 MPH

Cyber: (lower) global transit: 450 million MPH; (upper) light: 670+ million MPH

The cyber global transit was selected as travelling 25,000 miles (approximately around the equator) in 200 milliseconds. The time was selected as a conservative value based on typical Internet traffic speeds. See "Internet Traffic Report" available from *www.internettrafficreport.com/.*

30. Jeffrey L. Caton, "Complexity and Emergence in Ultra-Tactical Cyberspace Operations," in K. Podins, J. Stinissen, and M. Maybaum, eds., *5th International Conference on Cyber Conflict Proceedings*, Tallinn, Estonia: NATO Cooperative Cyber Defence Center of Excellence and IEEE, 2013, pp. 299-312.

31. Thomas J. Czerwinski, *Coping with the Bounds: Speculation on Nonlinearity in Military Affairs*, Washington, DC: National Defense University, 1998.

32. Didier Sornetter, "Dragon-Kings, Black Swans and the Prediction of Crises," *International Journal of Terraspace Science and Engineering*, Vol. 2, No. 1, December 2009, pp. 1-18.

33. Daniel Geer *et al.*, "Cyber*Insecurity*: The Cost of Monopoly. How the Dominance of Microsoft's Products Poses a Risk to Security," Washington, D.C: Computer and Communications Industry Association, September 24, 2003.

34. "Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command," pp. 34-36. Testimony included details of the Joint Information Environment (JIE) structure:

> The JIE systems architecture supports the full range of operations 'of' and 'on' the DoDIN (DoD Information Network]. The JIE will shift focus from protection of military service-specific networks, systems, and applications to securing data and its uses; a paradigm shift from the traditional net-centric to a data-centric environment. Key security features that will be employed under the JIE framework include: an enterprise-wide Single Security Architecture (SSA), a secure Out-of-Band (OOB) Management network; standardized identity and access management (IdAM); and the integration of thin-client and cloud-based (virtualization) technologies.

35. Peter Foster, "'Bogus' AP tweet about explosion at the White House wipes billions off US markets," *The Telegraph*, April 23, 2014, available from *www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html*.

36. Sam Kim, "North Korea Missile Launch: 3 Short-Range Guided Weapons Fired Into Sea, South Korean Officials Say," *The World Post*, May 18, 2013, available from *www.huffingtonpost.com/2013/05/18/north-korea-missile-launch_n_3298192.html*.

37. Andrey Kuzmin, "Meteorite Explodes over Russia, More than 1,000 Injured," Reuters, February 15, 2013, avail-

able from *www.reuters.com/article/2013/02/15/us-russia-meteorite-idUSBRE91E05Z20130215.*

38. See Walter Gary Sharp, Sr., *Cyberspace and the Use of Force,* Falls Church, VA: Aegis Research, 1999; and Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace,* Falls Church, VA: Aegis Research, 2000.

39. "Charter of the United Nations," available from *https://www.un.org/en/documents/charter/.*

40. "Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command," pp. 11-12.

41. "General Assembly Adopts Resolution Calling Upon States Not To Recognize Changes In Status Of Crimea Region," United Nations Resolution GA/11493, New York: United Nations, March 27, 2014.

42. Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," in *Proceedings of a Workshop on Deterring Cyberattacks*, Washington, DC: The National Academies Press, 2010, pp. 151-178.

43. "Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation," adopted by Heads of State and Government in Lisbon, Portugal: NATO, November 19, 2010.

44. Eneken Tikk, Kadri Kasda, and Liis Vihul, *International Cyber Incidents: Legal Considerations*, Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2010.

45. Jason Healey and Leendert van Bochoven, "Strategic Cyber Early Warning: A Phased Adaptive Approach for NATO," Washington, DC: The Atlantic Council, 2012.

46. William J. Johnson and Andrew D. Gillman, eds., *Law of Armed Conflict Deskbook*, Charlottesville, VA: The Judge Advocate General's Legal Center and School, U.S. Army, 2012.

47. Two publications that examine LOAC implications for cyberspace activity are Kelli Kinley, "What Constitutes an Act of War in Cyberspace?" Thesis AFIT/GIR/ENV/08-M12, Wright-Patterson Air Force Base, OH: Air Force Institute of Technology, March 2008; and Robert Fanelli and Gregory Conti, "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict," C. Czosseck, R. Ottis, and K. Ziolkowski, eds., *4th International Conference on Cyber Conflict Proceedings*, Tallinn, Estonia: NATO Cooperative Cyber Defence Center of Excellence and IEEE, 2012, pp. 319-331.

48. Department of the Air Force, *Air Force Instruction 51-402, Legal Reviews of Weapons and Cyber Capabilities*, Washington, DC: Office of the Secretary of the Air Force, July 27, 2011.

49. David E. Graham, "Cyber Threats and the Law of War," *Journal of National Security Law and Policy*, Vol. 4, No. 1, 2010, pp. 87-102.

50. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, NY: Cambridge University Press, 2013.

51. *Ibid.* The seven chapters of the *Tallinn Manual* are: 1) States and Cyberspace; 2) The Use of Force; 3) The Law of Armed Conflict Generally; 4) Conduct of Hostilities; 5) Certain Persons, Objects, and Activities; 6) Occupation; and 7) Neutrality.

52. *Ibid.,* p. 48.

53. Kuehl, p. 40.

54. Barack Obama, "National Security Strategy," Washington, DC: The White House, May 2010, p. 17. Also note that "In addition to facing enemies on traditional battlefields, the United States must now be prepared for asymmetric threats, such as those that target our reliance on space and cyberspace."

55. *Ibid.,* p. 28.

56. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," Washington, DC: The White House, May 2011, p. 12.

57. *Ibid*, p. 14.

58. Lynn, p. 108.

59. Jeffrey L. Caton, "DoD Strategy for Operating in Cyberspace: Nothing New Here," DIME Blog, U.S. Army War College, July 15, 2011.

60. "Department of Defense Strategy for Operating in Cyberspace," Washington, DC: Department of Defense, July 2011, p. 3. The five strategic initiatives are:

1. DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential.
2. DoD will employ new defense operating concepts to protect DoD networks and systems.
3. DoD will partner with other U.S. Government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.
4. DoD will build robust relationships with U.S. allies and international partners to strengthen collective cyber security.
5. DoD will leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

61. Thomas M. Chen, "An Assessment of the Department of Defense Strategy for Operating in Cyberspace," Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, September 2013.

62. "Department of Defense Strategy for Operating in Cyberspace," p. 5-6.

63. Chen, p. 33.

64. *Quadrennial Defense Review 2014*, Washington DC: Department of Defense, March 4, 2014, pp. 14-15.

65. Harold Hongju Koh, "International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD," *Harvard International Law Journal,* online Vol. 54, December 2012, pp. 1-12. Mr. Koh's 10 questions were:

1. *Do established principles of international law apply in cyberspace?*
Answer 1: Yes, international law principles do apply in cyberspace.

2. *Is cyberspace a law-free zone, where anything goes?*
Answer 2: Emphatically no. Cyberspace is not a "law-free" zone where anyone can conduct hostile activities without rules or restraint.

3. *Do cyber activities ever constitute a use of force?*
Answer 3: Yes. Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law.

4. *May a state ever respond to a computer network attack by exercising a right of national self-defense?*
Answer 4: Yes. A state's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof.

5. *Do* jus in bello *rules apply to computer network attacks?*
Answer 5: Yes. In the context of an armed conflict, the law of armed conflict applies to regulate the use of cyber tools in hostilities, just as it does other tools. The principles of necessity and proportionality limit uses of force in self-defense, and would regulate what may constitute a lawful response under the circumstances.

6. *Must attacks distinguish between military and nonmilitary objectives?*
Answer 6: Yes. The *jus in bello* principle of **distinction** applies to computer network attack undertaken in the context of an armed conflict.

7. *Must attacks adhere to the principle of proportionality?*
Answer 7: Yes. The *jus in bello* principle of **proportionality** applies to computer network attack undertaken in the context of an armed conflict.

8. *How should states assess their cyber weapons?*
Answer 8: States should undertake a **legal review** of weapons, including those that employ a cyber capability.

9. *In this analysis, what role does state sovereignty play?*
Answer 9: States conducting activities in cyberspace must take into account the sovereignty of other states, including outside the context of armed conflict.

10. *Are states responsible when cyber acts are undertaken through proxies?*
Answer 10: Yes. States are legally responsible for activities undertaken through "proxy actors," who act on the state's instructions or under its direction or control.

66. Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard International Law Journal,* online Vol. 54, December 2012, pp. 15, 37.

67. "Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command," p. 32.

68. Melissa E. Hathaway, "Cyber Readiness Index 1.0," Great Falls, VA: Hathaway Global Strategies LLC, 2013. The study methodology assessed five essential elements: 1) Articulation and publication of a National Cyber Security Strategy; 2) Does the country have an operational Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT)? 3) Has the country demonstrated commitment to protect against cyber crime? 4) Does the country have an information sharing mechanism? and 5) Is the country investing in cyber security basic and applied research and funding cyber security initiatives broadly?

69. "Cyberspace Policy Report," p. 7.

70. Oona A. Hathaway and Rebecca Crootof, "The Law of Cyber-Attack," *Faculty Scholarship Series* Paper 3852, New Haven, CT: Yale Law School, 2012.

71. "Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity," General Assembly Resolution 2004 (XXXIV-O/04), Quito, Ecuador: Organization of American States, June 8, 2004, available from *www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm.*

72. "Draft African Union Convention on the Confidence and Security in Cyberspace," African Union Commission, January 9, 2012, pp. 37-38, available from *au.int/en/cyberlegislation.*

73. "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, Belgium: European Union, February 7, 2013, p. 11, available from *eeas.europa.eu/policies/eu-cyber-security/.*

74. Jason Healey and Leendert van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow," Washington, DC: The Atlantic Council, 2011.

75. "Defending the Networks: The NATO Policy on Cyber Defence," Brussels: NATO, 2011, available from *www.nato.int/cps/en/natolive/topics_78170.htm.*

76. "NATO Cyber Defence; Media Backgrounder," Brussels, Belgium: NATO, October 2013.

77. James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, Washington, DC, January 29, 2014, p. 1.

78. Keir Giles with Andrew Monaghan, "Legality in Cyberspace: An Adversary View," Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, March 2014, p. ix.

79. *Ibid.,* p. 34.

80. Clapper, p. 2.

81. "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space," Russian Ministry of Defense, unofficial translation, Tallinn, Estonia: NATO Cooperative Cyber Defence Center of Excellence, 2011, available from *www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf*.

82. *Ibid*. Note that Collective Security Treaty Organization members are Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Tajikistan.

83. *Ibid*., p. 13.

84. "Statement by the Chinese Delegation on Information and Cyber Security at the Thematic Debate at the First Committee of the 68th Session UNGA," New York: United Nations, October 2013.

85. "An International Code of Conduct for Information Security—China's Perspective on Building a Peaceful, Secure, Open and Cooperative Cyberspace," Geneva, Switzerland: United Nations Institute for Disarmament Research, February 10, 2014, available from *www.unidir.ch/files/conferences/pdfs/a-cyber-code-of-conduct-the-best-vehicle-for-progress-en-1-963.pdf*.

86. "Statement by the Chinese Delegation on Information and Cyber Security at the Thematic Debate at the First Committee of the 68th Session UNGA" p. 1.

87. *Ibid*.

88. "China and Cybersecurity: Political, Economic, and Strategic Dimensions: Report from Workshops," San Diego, CA: University of California Institute on Global Conflict and Cooperation, April 2012, p. 1.

89. Clapper, p. 2.

90. "Statement by the Chinese Delegation on Information and Cyber Security at the Thematic Debate at the First Committee of

the 68th Session UNGA," New York: United Nations, October 2013, pp. 1-2.

91. Jayson M. Spade, "China's Cyber Power and America's National Security," Carlisle Barracks, PA: U.S. Army War College, May 2013, pp. 13-15. Spade envisions a possible venue where U.S.-China competition may turn hot (p. 24):

> Would China risk a cyber attack on America, given U.S. military capabilities and Sino-American economic interdependence? While the two states have many conflicting interests, Taiwan is one place where the United States and China face the real possibility of military conflict...China could conduct operational-level cyber attacks against U.S. forces in the Pacific, to delay or degrade their ability to mobilize and move forces to assist Taiwan. China could also conduct strategic attacks on American government and civilian networks, disrupting civilian command and control or critical infrastructure, to coerce U.S. capitulation. Without causing much lasting physical destruction, the PLA could undermine America's military means and will to support Taiwan. For PRC cyber units, the United States is both a soft target and a target rich environment.

Spade's vignette supports the QDR 2014 (pp. 6-7):

> In the coming years, countries such as China will continue seeking to counter U.S. strengths using anti-access and area-denial (A2/AD) approaches and by employing other new cyber and space control technologies. Additionally, these and other states continue to develop sophisticated integrated air defenses that can restrict access and freedom of maneuver in waters and airspace beyond territorial limits.

92. "China and Cybersecurity," p. 21.

93. Clapper, p. 2.

94. "United States Faces Challenges in Addressing Global Cybersecurity and Governance," GAO Report 10-606, Washington, DC: U.S. Government Accountability Office, July 2010, p. 14. The 19 organizations studied were: Asia-Pacific Economic Cooperation, Association of Southeast Asian Nations, Council of

Europe, European Union, Forum of Incident Response and Security Teams, Group of Eight, Institute of Electrical and Electronic Engineers, International Electrotechnical Commission, International Organization for Standardization, International Telecommunication Union, Internet Corporation for Assigned Names and Numbers, Internet Engineering Task Force, Internet Governance Forum, INTERPOL, Meridian, North Atlantic Treaty Organization, Organization of American States, Organisation for Economic Cooperation and Development, and United Nations.

95. *Ibid*., pp. 32-33.

96. *Ibid*., p. 33.

97. Clapper, p. 2.

98. Kan, p. 114.

99. Christian Czosseck and Karlis Podins, "A Usage-Centric Botnet Taxonomy," *Proceedings of the 10th European Conference on Information Warfare and Security*, Tallinn, Estonia: The Institute of Cybernetics at the Tallinn University of Technology p. 70.

100. Caton, "What do Senior Leaders Need to Know about Cyberspace," p. 218.

101. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," Washington, DC: The White House, May 2009.

102. "Cybersecurity, Innovation and the Internet Economy," Washington, DC: Department of Commerce, June 2011.

103. *Ibid*.

104. Paula Rosenblum, "Target Hit by One of Most Sophisticated Data Thefts Ever, But It Won't Hurt the Retailer," *Forbes*, December 19, 2013, available from *www.forbes.com/sites/paularosenblum/2013/12/19/data-breach-paints-targets-holiday-weekend-black/*.

105. Richard Nieva, "Heartbleed Bug: What you need to know (FAQ)," CNET, April 11, 2014, available from *www.cnet.com/news/heartbleed-bug-what-you-need-to-know-faq/*.

106. "Netflix, YouTube Could Feel Effects of 'Open Internet' Ruling" *The Wall Street Journal*, January 14, 2014, available from *online.wsj.com/news/articles/SB10001424052702304049704579320983864581364*.

107. Alexander Klimburg, ed., *National Cyber Security Framework Manual*, Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012, p. 35.

108. "Cyberspace Policy Review," p. iv.

109. *Ibid*, p. 9.

110. "Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command," p. 12.

111. "Cyberspace Policy Report," p. 3.

112. *Ibid*.

113. "Cybersecurity Results-Distributing Threat Warnings," available from *www.dhs.gov/cybersecurity-results*. Also see "Resources and Capabilities Guide: The National Cybersecurity and Communications Integration Center (NCCIC)," Washington, DC: Department of Homeland Security, October 21, 2013, p. 4. The publication describes the NCCIC function as:

> [The NCCIC] serves as a centralized location where operational elements are coordinated and integrated. NCCIC partners include all federal departments and agencies; state, local, tribal, and territorial (SLTT) governments; the private sector; and international entities. The NCCIC's activities include providing greater understanding of cybersecurity and communications situation awareness vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

The publication also lists the NCCIC mission:

> To operate at the intersection of the private sector, civilian, law enforcement, intelligence, and defense communities, applying unique analytic perspectives, ensuring shared situational awareness, and orchestrating synchronized response efforts while protecting the Constitutional and privacy rights of Americans in both the cybersecurity and communications domains.

114 . "Cyberspace Policy Report," p. 9.

115. "Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command," p. 11.

116. "Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity," Washington, DC: Department of Defense and Department of Homeland Security, October 13, 2010, p. 1.

117. "Cybersecurity Results—Distributing Threat Warnings."

118. "Cyber Storm III Final Report," Washington, DC: Department of Homeland Security, July 2011. Details on the exercise stakeholders from p. 5:

> CS [Cyber Storm] III included participation from 8 Cabinet-level departments, 13 states, 12 international partners, and approximately 60 private-sector companies and coordination bodies. Participation focused on the information technology (IT), communications, energy (electric), chemical, and transportation critical infrastructure sectors and incorporated various levels of play from other critical infrastructure sectors. In addition, CS III included the participation of states, localities, and coordination bodies, such as Information Sharing and Analysis Centers (ISACs). International participation included public- and private-sector components from four countries (Australia, Canada, New Zealand, and the United Kingdom) and Government representatives from the International Watch and Warning Network (IWWN). During the exercise, the participant set included 1,725 CS III–specific system users, including some used by watch and operations centers that allowed for access of multiple users and shifts.

119 . "United States Faces Challenges in Addressing Global Cybersecurity and Governance," p. 35.

120. "Statement of General Keith B. Alexander, Commander, United States Cyber Command, before the Senate Committee on Armed Services," Washington, DC: U.S. Senate, February 27, 2014, p. 6.

121. For example, per General Order No. 2014-02, March 6, 2014, HQ Department of the Army, paragraph 2.e., p. 2, Army-Cyber Command "serves as the single point of contact for reporting and assessing Army cyberspace incidents, events, and operations."

122. "Statement of General Keith B. Alexander," February 27, 2014, p. 9. Alexander also summarized on p. 6 that:

> The last year saw increased collaboration between defenders and operators across the US government and with private and international partners. USCYBERCOM played important roles in several areas…. In addition, USCYBERCOM participated in whole-of-government actions with partners like the Departments of State, Justice, and Homeland Security in working against nation-state sponsored cyber exploitation and distributed denial-of-service attacks against American companies. Finally, we already benefit from sharing information on cyber threats with the services and agencies of key partners and allies, and are hopeful that cybersecurity legislation will one day make it easier for the U.S. Government and the private sector to share threat data in line with what the Administration has previously requested.

123. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," pp. 10, 13.

124. Kristin Archick, "Cybercrime: The Council of Europe Convention," Report for Congress RS21208, Washington, DC: Congressional Research Service, September 28, 2006. Also see "Convention on Cybercrime Status of Signatures and Ratifications" Council of Europe, available from *conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG*. Note that in addition to the 42 countries that have ratified the convention, 11 additional countries are nonratified signatories.

125. Hathaway and Crootof, p. 834.

126. Clapper, p. 2.

127. Hathaway and Crootof, p. 834.

128. "Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," Washington, DC: Office of the National Counterintelligence Executive, October 2011, p. i.

129. *Ibid*., p. 4.

130. Clapper, p. 2.

131. "Cyberspace Policy Report," p. 9.

132. *Ibid*.

133. Jason Healey and A. J. Wilson, "Cyber Conflict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain," Washington, DC: The Atlantic Council, 2013, available from *www.atlanticcouncil.org/publications/issue-briefs/cyber-conflict-and-the-wpr-congressional-oversight-of-hostilities-in-the-fifth-domain*.

134. *Quadrennial Defense Review 2014*, p. 32.

135. *Ibid*, p. 41.

136. Jason M. Bender, "The Cyberspace Operations Planner: Challenges to Education and Understanding of Offensive Cyberspace Operations," *Small Wars Journal*, November 5, 2013, p. 15. Bender's reference to classified doctrine is probably directed at the decision to make the initial version of the JP 3-12, *Cyberspace Operations,* a secret document without regard to its use by joint forces writ large, let alone partner countries.

137. Johnny L. Morris and G. K. Cunningham, "An Exploration of Intuition among Senior Leaders," *The Exchange*, Vol. 2, No. 2, December 2013, pp. 51-63.

138. Jody M. Prescott, "Building the Ethical Cyber Command and the Law of Armed Conflict," *Rutgers Computer & Technology Law Journal*, Vol. 40, 2014, p. 76.

139. Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, CA: RAND Corporation, 2009. In this book's Appendix B, "The Calculus of Explicit Versus Implicit Deterrence," the author develops a "Decision Matrix for Retaliation, Value Parameters" that attempts to quantify the "Subsequent Outcome-Value" for each of the decisionmaker's major options.

140. Timothy J. Junio, "How Probable Is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate," *The Journal of Strategic Studies*, Vol. 36, No. 1, 2013, pp. 125-133.

141. "United States Faces Challenges in Addressing Global Cybersecurity and Governance," p. 33.

142. Elena Chernenko, "Russia Warns against NATO Document Legitimizing Cyberwars," *Kommersant-Vlast*, May 29, 2013 (originally published in Russian), available from *rbth.com/international/2013/05/29/russia_warns_against_nato_document_legitimizing_cyberwars_26483.html*. The article noted that:

> The Russian authorities especially the military—have taken a very guarded view of the Tallinn Manual. Moscow thinks its publication marks a step toward legitimizing the concept of cyberwars. Russian Defense Ministry spokesperson Konstantin Peschanenko came out with a statement to this effect in April. He was backed by Russia's Roving Ambassador, Andrei Krutskikh, who said that, while Russia is trying to prevent militarization of cyberspace by urging the international community to adopt a code of conduct in this sphere, the United States and its allies are already agreeing.

143. "Cyberspace Policy Report, Section 934," p. 6.

144. David M. Keely, "Cyber Attack! Crime or Act of War?" Strategy Research Project, Carlisle, PA: U.S. Army War College, April 2011, pp. 9-11.

145. "Statement of General Keith B. Alexander," February 27, 2014, p. 9.

146. "Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command," p. 16.

147. "Cyberspace Policy Review," p. 17.

148. Koh, p. 8.

149. "National Cyber Incident Response Plan, Interim Version," Washington, DC: Department of Homeland Security, September 2010, p. C-1.

150. "Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command," pp. 9-10.

151. Michael Tanji, "Buccaneer.com: Infosec Privateering as a Solution to Cyberspace Threats," *Journal of Cyber Conflict Studies*, Vol.1, No.1, December 2007, pp. 4-11.

152. Tikk *et al*., p. 31.

153. *Ibid*., p. 33.

154. "Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command," p. 44.

155. "Department of Defense Strategy for Operating in Cyberspace," p. 7.

156. "Statement of General Keith B. Alexander," February 27, 2014, p. 6.

157 . Koh, p. 7.

158. James R. Gosler and Lewis Von Thaer, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," Washington, DC: Department of Defense, Defense Science Board, January 2013, p. 41.

APPENDIX 1
APPLICABLE UNITED NATION CHARTER AND NORTH ATLANTIC TREATY ARTICLES

U.N. CHARTER ARTICLE 2.

The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.

1. The Organization is based on the principle of the sovereign equality of all its Members.

2. All Members, in order to ensure to all of them the rights and benefits resulting from membership, shall fulfill in good faith the obligations assumed by them in accordance with the present Charter.

3. All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.

4. All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

5. All Members shall give the United Nations every assistance in any action it takes in accordance with the present Charter, and shall refrain from giving assistance to any state against which the United Nations is taking preventive or enforcement action.

6. The Organization shall ensure that states which are not Members of the United Nations act in accordance with these Principles so far as may be necessary for the maintenance of international peace and security.

7. Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter Vll.

U.N. CHARTER ARTICLE 25.

The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter.

U.N. CHARTER ARTICLE 39.

The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.

U.N. CHARTER ARTICLE 41.

The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.

U.N. CHARTER ARTICLE 42.

Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.

U.N. CHARTER ARTICLE 51.

Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

NATO ARTICLE 4

The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.

NATO ARTICLE 5

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 and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

APPENDIX 2
TALLINN MANUAL CRITERIA

Rule 11 – Definition of Use of Force

A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.

Proposed factors that influence State assessment of potential use of force (not formal legal criteria)

(a) Severity: How many people were killed? How large an area was attacked? How much damage was done within this area?
(b) Immediacy: How soon were the effects of the cyber operation felt? How quickly did its effects abate?
(c) Directness: Was the action the proximate cause of the effects? Were there contributing causes giving rise to those effects?
(d) Invasiveness: Did the action involve penetrating a cyber network intended to be secure? Was the locus of the action within the target country?
(e) Measurability of effects: How can the effects of the action be quantified? Are the effects of the action distinct from the results of parallel or competing actions? How certain is the calculation of the effects?
(f) Military character: Did the military conduct the cyber operation? Were the armed forces the target of the cyber operation?
(g) State involvement: Is the State directly or indirectly involved in the act in question? But for the acting State's sake, would the action have occurred?

(h) Presumptive legality: Has this category of action been generally characterized as a use of force, or characterized as one that is not? Are the means qualitatively similar to others presumed legitimate under international law?

FOR THIS AND OTHER PUBLICATIONS, VISIT US AT
http://www.carlisle.army.mil/

ISBN 1-58487-643-3

This Publication

SSI Website

USAWC Website

U.S. ARMY WAR COLLEGE

Major General William E. Rapp
Commandant

*****

STRATEGIC STUDIES INSTITUTE
and
U.S. ARMY WAR COLLEGE PRESS

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven K. Metz

Author
Mr. Jeffrey L. Caton

Editor for Production
Dr. James G. Pierce

Publications Assistant
Ms. Rita A. Rummel

*****

Composition
Mrs. Jennifer E. Nevil