Strategy Research Project

The Flawed Strategic Discourse on Cyber Power

by

Colonel Brandon Newton
United States Army

United States Army War College
Class of 2015

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

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

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

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

1. REPORT DATE *(DD-MM-YYYY)* 01-04-2015	**2. REPORT TYPE** STRATEGY RESEARCH PROJECT	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE The Flawed Strategic Discourse on Cyber Power	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Colonel Brandon Newton United States Army	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Professor Thomas P. Galvin Department of Command, Leadership, and Management	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES

Word Count: 5972

14. ABSTRACT

This paper examines flaws in the strategic discourse on cyber power. The current discourse is flawed because it is dominated by hyperbole, misapplies context, and lacks sufficient precision in terms and definitions. There are two critical flaws in the current discourse. The first is descriptions of the existential nature of strategic cyber war, and the Armageddon like environment that would be created by such a war, despite evidence to the contrary. The second flaw is in the understanding of the context of any cyber action potential adversaries, state or non-state. Recommended adjustments to the discourse need to be informed by clear and valid assumptions on what can be done with cyber power, as well as the application of a model for cyber threat prioritization. The final analysis addresses the needed changes in education and training, and the role of humans in understanding the nature of cyber power.

15. SUBJECT TERMS

Cyber War, Cyber Strategy, Cyberspace

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES** 33	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	UU		**19b. TELEPHONE NUMBER** *(w/ area code)*

USAWC STRATEGY RESEARCH PROJECT

The Flawed Strategic Discourse on Cyber Power

by

Colonel Brandon Newton
United States Army

Professor Thomas P. Galvin
Department of Command, Leadership, and Management
Project Adviser

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

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

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

Abstract

Title:	The Flawed Strategic Discourse on Cyber Power
Report Date:	01 April 2015
Page Count:	33
Word Count:	5972
Key Terms:	Cyber War, Cyber Strategy, Cyberspace
Classification:	Unclassified

This paper examines flaws in the strategic discourse on cyber power. The current discourse is flawed because it is dominated by hyperbole, misapplies context, and lacks sufficient precision in terms and definitions. There are two critical flaws in the current discourse. The first is descriptions of the existential nature of strategic cyber war, and the Armageddon like environment that would be created by such a war, despite evidence to the contrary. The second flaw is in the understanding of the context of any cyber action potential adversaries, state or non-state. Recommended adjustments to the discourse need to be informed by clear and valid assumptions on what can be done with cyber power, as well as the application of a model for cyber threat prioritization. The final analysis addresses the needed changes in education and training, and the role of humans in understanding the nature of cyber power.

The Flawed Strategic Discourse on Cyber Power

If there were ever any doubt that cyber power had taken its permanent place among the other more traditional domains of warfare, the recently published National Security Strategy would erase that notion. According to the Strategy, cyberspace is the preeminent shared commons, an infrastructure responsible for our “economy, safety and health.”[1] For the United States (U.S.), cyberspace is an interest to be defended, with costs imposed on those who attack it. This year, 2015, marked a year of cyber events in the news and public debate. With the Sony Corporation hack, the Central Command Twitter hack, and threats to financial networks, there has been constant attention on cyber-threats in the media.

Unfortunately, the hyperbole of a “Cyber 9/11” or “Cyber-Armageddon” has merged fact with fiction in the strategic discourse.[2] Although existing cyber-threats are certainly capable of striking U.S. interests, the likely effects of such attacks are being overblown and can be mitigated by current information assurance policies. After all, as Martin Libicki writes in his article on the cyber strategic instability, “Cyber war has yet to claim its first life.”[3] In defense, business, and media circles, cyber threats are often presented as unqualified existential threats. The current strategic discourse on cyber power and cyber defense is flawed because it is dominated by hyperbole, misapplies context, and lacks sufficient precision in terms and definitions. The result is an incomplete development of policy and strategy for cyberspace, and an unclear picture of how to strategically interpret cyber threats. This paper will examine the strategic discourse on cyber, and attempt to reshape the debate to bring about more clarity, analysis, and constructive dialogue.

This paper presents two critical flaws in the current discourse. The first is the degree to which writers have extolled the existential nature of strategic cyber war, and the Armageddon like environment that would be created by such a war, despite evidence to the contrary. Overestimating the capabilities of cyber warriors and effects of cyber warfare confuses the realities of what can be done with cyber power. It is certainly possible that cyber power alone could result in actual physical harm, but as of 2015 cyber attacks have only produced effects indirectly. Cyber warfare's ability to force a strategic reaction that affects the will of a nation is suspect, given that even a catastrophic loss of digital networking capability can be overcome, according to Libicki. In 2015, it is difficult to imagine a scenario in which cyber power alone (promulgated through a cyber war) would pose an existential threat to the U.S.[4] A properly shaped discourse recognizes how rapidly cyber threats are adapting and evolving, and can aid policy makers in properly aligning resources against the threats, while avoiding hyperbole in favor of a rational and suitable assessment of the real capabilities of cyber power.

The second flaw is in the understanding of the context of any cyber action potential adversaries, state or non-state. The loss of sensitive company data by Sony in 2014 as a result of a North Korean cyber attack was certainly damaging to the Sony Corporation and shareholders. What was missing was the contextualization of the hack in terms of how should policy and strategy respond. The losses seemed to result in real monetary damage to Sony, but what was held at risk in terms of national interests? What was lost in the attack, and whom did it affect? What were the North Koreans able to hold at risk that affected the national security interest of the U.S.? As the corporation was coerced into removing *The Interview* from theatres, The U.S. threatened to "respond proportionality" against the North Koreans.[5] The judgment of *what matters and why* for an action taken in cyberspace is relevant and important. This examination should be more acute when the attribution is to a state, especially when language that is normally reserved for actions in traditional domains is applied at the Executive level of the U.S. government.

The final part of this paper is to discuss areas where strategic leaders within the Department of Defense (DoD) must better understand cyber power so to properly decide upon policy, tools and methods. The first recommendation is to utilize a series of ideas that better illuminate flawed assumptions for cyber power and cyber strategy. Next the paper will examine a possible model for analyzing threats based on their likelihood, impact, and risk. Vulnerabilities in cyberspace are by their very design constructed and participatory. Cyberspace is a finite domain, bounded (at least for now) by the physical properties of voltage, and the mathematical properties of logical sequences and combinations.[6] In the end we *choose* to avail ourselves of the benefits of cyberspace, and "if that cyberspace is found vulnerable to attack, or unexpectedly prone to technical failure, the fault will be ours."[7]

Terminology

Terminology is important in this discussion. There is inconsistency in the terms of cyber power that leads to its confusion in the strategic discourse. This paper will adopt the useful explanations that Colin Gray provides in his monograph *Making Strategic Sense of Cyber Power: Why the Sky is not Falling.* Gray unpacks three terms: cyberspace, cyber power, and cyber strategy and provides useful definitions of each. *Cyberspace* is generally meant to describe the:

> Global domain within the information environment whose distinctive and unique character is framed by the use of electronics and electromagnetic spectrum to create, store, modify, exchange, and exploit information via independent and interconnected networks using information-communication technologies.[8]

Cyber power describes the "ability to do something strategically important in cyberspace."[9] Gray borrows from both Daniel Kuehl and air-power theorist Billy Mitchell in constructing this practical definition. The last term is *cyber strategy* (or as Gray adjusts it "strategies for cyber") and is used for describing strategy for using cyber power in cyberspace. Gray emphasizes that "strategy is strategy, whether it is for cyber power, land power, or sea power."[10] His phrasing reinforces how strategy is the prevailing concept over cyber, as opposed to the other way around. This is integral in placing the right value on cyber powers' commonality with its sister domains as opposed to highlighting its technological distinctiveness.

Two additional terms that are important for this paper are the terms *cyber warfare* and *cyber war*. Libicki in his article *Why Cyber War Will Not and Should Not Have its Grand Strategist* provides the method of differentiating these two concepts. Cyber warfare is meant to describe the use of cyber power to accentuate warfare and combat in the physical domain. Cyber war is used to describe cyber power that is used to affect the will of another nation or adversary.[11] In both cases, these terms describe warfare that takes place solely in cyberspace between adversaries that use cyber power to affect another entity's will. Later examples will describe cyber war or strategic cyber war in this context.

Current Research on Cyber Power

There is a relatively small amount of research that addresses the theoretical nature of cyber strategy and cyber power compared with more traditional domains. Gray gives us a few plausible reasons for this. According to Gray what has been written is largely focused on the technical subject matter of securing digital networks. Gray also notes that the strategic discourse on cyber was late in coming because of a number of recent events: the so-called revolution in military affairs, transformation, and the post 9/11 war on terror.[12] The majority of what has been in the news and in the public discourse is that cyber warfare and cyber attacks are an existential and present danger to our national security. The best examples of strategic cyber warfare's effects can be found in articles like Amit Sharma's *Cyber Power, a Means to an End* and John Stone's *Cyber War Will Take Place!*[13] There are also numerous articles, books, and monographs that portend a coming cyber war. Samples of these include *Awaiting Cyber 9/11* from *Joint Force Quarterly* and books and articles by Joel Brenner, such as *America the Vulnerable*.

A second and somewhat smaller community of scholars takes an opposing position to the idea of strategic cyber warfare and the existential nature of the cyber threat. Libicki has written a number of expansive articles on cyber power including *Cyber Deterrence and Cyber War* and *Why Cyber Will Not and Should Not have its Grand Strategists*. Another important monograph for this paper is Gray's *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*. Both of these writers form the basis of the evidence supporting this paper's thesis. Other articles that take a similar position are Sean Lawson's *Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats* and a series by Thomas Rid including *Cyber War Will Not Take Place*. All of these papers have a common denominator in that they minimize the existential nature of cyber power, and warn against overestimating the capabilities of cyber power and cyber warfare.

Problems with the Discourse

Having presented the current state of cyber power literature, this paper will provide more detail on the nature and extent of the two aforementioned flaws in the discourse.

Overestimating Strategic Cyber War

The current discourse of overestimation leads to evaluation of cyber war as an existential threat and a survival interest. Amit Sharma gives us an example of the overestimation of the effects of cyber warfare in a 2010 article published in the journal *Strategic Analysis*. Sharma's thesis is that cyber power's place in warfare has wrongly been as an adjunct to traditional operations. He posits that traditional operations should enhance strategic cyber warfare, not the reverse. He applies Clausewitz's trinity to cyber capabilities, envisioning the ability of cyber power to destroy all of the cyber-manifestations of the trinity, causing a cascading effect that will "induce a strategic paralytic effect on the nation, pushing it into chaos and mayhem."[14] Sharma continues by asserting that strategic cyber parallel warfare against all aspects of society leverages information warfare for strategic effect and brings about desired strategic ends by introducing paralytic effects on the enemy nation.[15]

Joel Brenner devotes a whole chapter of his book *America the Vulnerable* in describing a future (2017) cyber-enabled conflict between China and the U.S. The scenario culminates when the U.S. is coerced to acquiesce to China's demands in the South China Sea after China demonstrates the ability to control the U.S.' critical power infrastructure.[16] This is an example of a hypothetical use of cyber power that is an example overestimation and reach. Gray presents a strong case in his article that this type strategic cyber war is infeasible, and that cyber power “can only be an enabler of physical effort. . . . .[and] that “stand-alone (properly misnamed as ‘strategic’) cyber action is inherently and grossly limited in its immateriality.”[17] The idea that strategic cyber warfare, executed singularly without the complementary effects of traditional air, space, sea, and land warfare characterizes cyber power with a specialness that is inaccurate. Cyber power is fundamentally under the same constraining factors of the weapons and tools of the other domains of war.[18]

In Sharma’s construct, strategic cyber war’s impact on the state is explained in existential terms, with the ability to affect even the basic resilience of the Nation. An attack on all aspects of the Sharma’s cyber trinity (defense networks, government and law enforcement networks, and critical national infrastructure) would drive the government and its citizens into chaos.

> The disappearance of their facilities on which they are hopelessly dependent will result in catastrophic outcomes, where chaos, fear, bedlam, anarchy, and basic animal instincts will prevail, resulting in complete destruction of the nation as a system.[19]

Libicki also provides an argument that cyber warfare would not have the effects that Sharma describes. Cyber attacks digital networks and systems; in the worst case the nation returns to its pre-networked state and "to argue that cyber warfare can have a revolutionary effect on the battlefield requires establishing that digital networking is itself revolutionary. This is a step many proponents of cyber warfare neglect to take."[20] This does not discount the very real indirect effect that cyber can achieve; it only informs the magnitude of the effects on all aspects of the government and life. Another counter to Sharma’s example of the effects of strategic cyber war is that society possesses far more resiliency in the face of the type of adversity described above. Sean Lawson questions the idea that cyber war could achieve this type of devastation. His argument is that if massive conventional and atomic air attacks on populations “generally failed to deliver the panic, paralysis, technological and social collapse, and loss of will, it seems unlikely that a cyber-attack would achieve these results.”[21] There is a tendency to use historic devastating attacks on the U.S. as comparisons to what cyber warfare would do to the nation. Warning of a “cyber Pearl Harbor” or the aforementioned Cyber 9/11, some authors capitalize on our knowledge of those events to illustrate a level of devastation that is familiar.[22]

An explanation for this tendency to overestimate the threat is that it continues our historical technological pessimism and fear of new innovations, a fear reinforced by our ever-present reliance on digital networks.[23] The overestimation of cyber power is a continuance of a distrust of technology, and a belief that computers could spin out of control and act independently. Others call into question the comparisons to attacks like 9/11 or Pearl Harbor by illustrating that it is unlikely that any cyber exclusive attack would have an impact *near* as devastating as recent large natural disasters or the strategic bombing campaigns of World War II.[24] In each of these examples the population was physically affected, but was certainly resilient enough to eventually recover and move forward. An additional view on cyber doom and cyber 9/11 scenarios is that we have already experienced that level of attack, but the damage was existential in other more broadly defined ways. In execution, cyber warfare may look less like earthquake and more like climate change; “[Snowden] is our Cyber 9/11, we just imagined it differently."[25]

Strategic cyber warfare is often credited with the ability to influence the will of adversary, and with capabilities as powerful as our most lethal strategic weapons. Sharma argues that cyber warfare can have an attractive outcome: conflict termination without conventional warfare. He argues that Strategic cyber warfare against the Trinity in order to achieve strategic paralysis is,

> Eventually more important than the conventional paradigm of destruction-based warfare to annihilate the forces it depends on for its defence; generating not only a strategic victory, but also a constructive conflict termination.[26]

He continues this passage by making the linkage between constructive conflict terminations as a modern day requirement, strengthened by the domestic necessity of not repeating protracted conflicts like the Iraq War.[27] Gray's observation is that it would be difficult to extrapolate the ability of cyber power to cause enough kinetic damage in order to cause a forced change affecting will. He also notes that it is not hard to draw analogies with other non-kinetic methods and see that cyber could be included for its ability to have an indirect effect as well as a "contributing enabler of effectiveness of physical efforts in the other four geographies of conflict. Speculation about cyber war, defined strictly as hostile action by networked computers, is hugely unconvincing."[28]

Finally, two other explanations for this flaw in the discourse are offered. The first is that this inflation is an example of securitization theory, which establishes that when threats to security are not "naturally occurring, they must be constructed through political and public discourse."[29] This unnatural elevation of cyber threats increases the funding, attention, and importance of the enterprise that is needed to defend against cyber threats. The other possibility is that cyber "catches the wave" of the public desire that gravitates towards defense solutions that offer a technological standoff as opposed to boots on the ground (or in the air).[30] The discourse on cyber power and cyber strategies is often missing a reflection on the reality of what can be done in cyberspace, and the perspective of to what end.

Context and Vulnerabilities in Cyberspace

The second flaw in the discourse involves vulnerabilities and context, and how these are poorly understood. Cyber power needs to be placed in strategic context relative to other methods of warfare. The ease in which we apply strategic theory from other domains to cyber warfare hampers clear thought on what cyber power can do, and what it cannot do. Some of this is hampered by the immaturity of what we know about cyber power's possibilities, and in many cases we do not yet know "enough now to make strategic sense of cyber."[31] These vulnerabilities can create opportunities as well, because potential adversaries also participate in their vulnerabilities.[32] This strategic discourse on cyber needs to remain apprised of this integral component of cyber power.

In November 2014, The Sony Corporation's network was penetrated by what is reported to have been North Korean cyber-units. The exploit acquired a large amount of corporate and personal data, emails, and business intelligence from Sony. What is useful about the Sony attack is analyzing it in a discussion of its context and vulnerabilities.

The stated U.S. national response, to "respond proportionately" to the North Korean use of cyber-power against Sony, underwrote a policy to act with cyber power even when the adversary's objectives were not achieved.[33] The affected movie, *The Interview*, was critically panned and anticipated to become a commercial flop, but became far more successful after the cyber attack.[34] But what really caused that turnaround--was it the resilience of a media corporation or was it the national rhetoric? The concern for policy and strategy is that without proper context the strategic effects of cyber activity could be wrongly attributed. This could lead to significant vulnerabilities later on. Libicki urges caution:

> Strategic effects of cyber war may arise from the interaction of state actors that systematically overestimate its effects (as quasi-apocalyptic statements from both U.S. and Chinese military officials suggest is quite possible). This could lead to unfortunate dynamics.[35]

As it turned out, the exploitation of the Sony's network was not a sophisticated attack, and had more to do with the poor safeguarding of sensitive (at least to them) data than it did with the capabilities of the cyber power wielded by the North Koreans.[36]

Another issue with national response without context is that cyber power may be unique, but it is constrained by the same theoretical properties as the weapons of the other domains. Cyber power can achieve indirect effects against economies, information, and certainly defense forces, but they must be viewed carefully and in context of cyber power's place as a tool to further strategy. Gray points out that cyber may be an "extreme case of non-kinetic agency, but the legal problems (in the laws of war) created by regarding combat electrons effectively as equivalents to agents of force ought to be overwhelmed by strategic sense."[37] The Sony hack is a good example of phenomena that Peter Singer writes about in his book *Cyber security and Cyberwar: what everyone needs to know*. Singer explains, "Essential concepts that define what is possible and proper are being missed, or even worse, distorted."[38] This causes "past myth and future hype" to combine, making what actually happened even more difficult to discern.[39] The conclusion is that the context of cyber power and strategy is important, as well as the nature of what makes our cyberspace vulnerable.

Vulnerabilities in cyberspace are variable, and often the result of a need for individual convenience and profit for business. In 2015, government, business, and private citizens have a reliance on digital networking that is not only a matter of convenience, but is required in some cases by law. The current trend of digitization is upwards, and it is difficult to see how this would change. However, it should not be lost in the discourse that in cyberspaces there is an absolute separation between what can occur in those constructed spaces and what is assessed as a vulnerability, as Valeriano et al., explains:

> The most important distinction of cyber is that between the physical and synaptic layer. These layers are not collapsed together. The danger coming from cyber invasions can only apply to the knowledge existing in the information world and not to all knowledge. In other words the state is only as vulnerable at is allows itself to be.[40]

Another example is in Jeffery Carr's article in the *Bulletin of Atomic Scientists*. Carr summarizes the idea of misplaced context of cyber by stating "the potential effect of a digital or cyber weapon used against a network is directly proportional to how much a given population relies on that network."[41] Exploitation of a corporate or defense network is not a random event that just occurs on its own.

This concept is a powerful and realistic counter argument that should not be minimized in the discussion of cyber power's real capabilities. Framing the impact of a cyber event as a constant and sustained vulnerability ignores the reality that we can be proactive in adjusting our posture once attacked. This goes farther than the ideas of improved defensive positions. In a constructed space, a space that is inherently virtual, there are choices and adjustments that can be made to the reliance on the medium. The irony with cyberspace is that its physical properties may be non-permissive, but it facilitates the construction of very permissive and discretionary environments, altered and adjusted by the user of the space.[42]

Analyzing Cyber Power and the Strategic Context

Flawed assumptions about cyber power have negative implications for cyber policy. Assumptions that overestimate cyber power, as has been illustrated in previous pages, are an example of the impact of not challenging assumptions. Focusing policy on the least likely scenarios of so-called cyber-warfare also diverts resources away from "preventing or mitigating the effects of more realistic but less dramatic scenarios" that are more likely to be encountered.[43] The focus in the past year has publicly been about loss of data and hacks by state actors against both government and business. These acts prompted calls for government (primarily defense) reaction. These are opportunities for a clear understanding of the role of national policy and defense in responding to the cyber power needs of non-defense entities. It should be noted that following the financial crisis of 2008, many financial companies admitted that they had participated in the mistakes that resulted in the crisis and the subsequent regulation. It is interesting that they don't appear to share that same feeling of culpability for failing to secure their networks and data, and see a role for government and defense involvement.

The discourse needs to always *strive for clear problem definition in assessing cyber power and cyberspace.* Lawson's example is to disaggregate the threats, and "focus on broader range of cyberspace-based events, e.g., human error, market failure, technical failure, in addition to malicious attacks by actors with intent to disrupt."[44] In other words, the focus of some strategic thought on massive cyber war and the effort that goes into preparing to defend against that unlikely event can mask the nature of other less-obvious cyber threats with real strategic impacts. An example of more broadly defining the threat is Edward Snowden's global (and illegal) publication of sensitive national security and diplomatic information. His actions did real strategic damage to our diplomatic, informational and defense (in terms of ways) power in a way that exemplifies the existential cyber war that the U.S. has been preparing for.

The discourse also needs to center around *empirical research and less on hypothetical scenarios* when evaluating what is in the realm of the possible in cyberspace.[45] Defense techniques of operational design can be helpful in framing the environment as well as to problem definition. Those charged with policy and strategy decisions about cyber power should demand a level of accuracy in information and problem framing that does not rely on inductive anecdote. Unfamiliarity with technology cannot be an impediment to good decision making and understanding the nature of cyber power. Strategic leaders must be quick to question and critically analyze whether what they are hearing is "based on empirical evidence or merely the reflection of long held anxieties about technology and recycled assumptions about infrastructure and social fragility."[46]

Finally, the discourse needs to shift its outcomes away from a crisis response orientation and toward *developing ways and means that promote resilience in technological and social systems* that ultimately bound cyber power and cyberspace. The cyber domain is constructed, and as discussed in many examples above, is largely what its users make of it. Lawson calls for the following:

1. modernization and repair of infrastructure,
2. promoting strong local communities and good governance, and

3. increasing decentralization and self-organization in social systems.[47]

Defense strategy about cyber power can improve most by adhering to the latter. It is unique that this imperative includes decentralization as a way to form cyber policy. This idea should be most familiar to military leaders because of the parallels to the principles found in Mission Command doctrine.

A Model for Assessing Cyber Threats

The Carnegie Mellon Software Engineering Institute proposes a useful holistic model for understanding cyber threats. The Cyber Prioritization Model (CTP) was a result of a larger study on cyber intelligence across business, government, and industry. During the study the research team noted diverse and problematic methods that were used to prioritize and understand various cyber threats.[48] This model would assist to better frame the strategic context of threats in cyberspace. When applied to problems of defense and strategy, there are important implications for adjusting our thinking about cyber power.

The model disaggregates threats into three areas for analysis: The *likelihood* of threat actors executing attacks, the *impact* that the threat could have on the organization, and finally the *risk* a threat poses based on an organization's known vulnerabilities.[49] The cyber threat prioritization model is useful when used to think strategically about cyber power and cyber strategies. It can help sort through the threats and value them in terms that are familiar to defense leaders. The model is based on a summation of likelihood, impact and risk. Likelihood is a function of understanding the capability and intent of cyber threat or actor. Attack methods, resources, motive and targeted data are all a part of analyzing and qualifying likelihood.[50] Impact is about assessing effects. In the CTP model, Impacts are broken down into two areas, operational impact and strategic interests. For our purposes, strategic impact deserves careful analysis.

The CTP model does not wholly omit the nature of national security impacts and interests, but considering the strategic impact of systems related to homeland security and defense is necessary. The third portion of the CTP model deals with risk. This component is also useful for thinking about DoD vulnerabilities. The CTP model breaks risk into two categories, people and the cyber-footprint.[51] What is interesting about the CTP model for risk is that it assumes that vulnerabilities are *dependent on the organization's choices and the people in that organization*. This is in line with the earlier discussions on discretionary vulnerability. The results of the three-part analysis can then be plotted on a graph similar to the one in Figure 1.

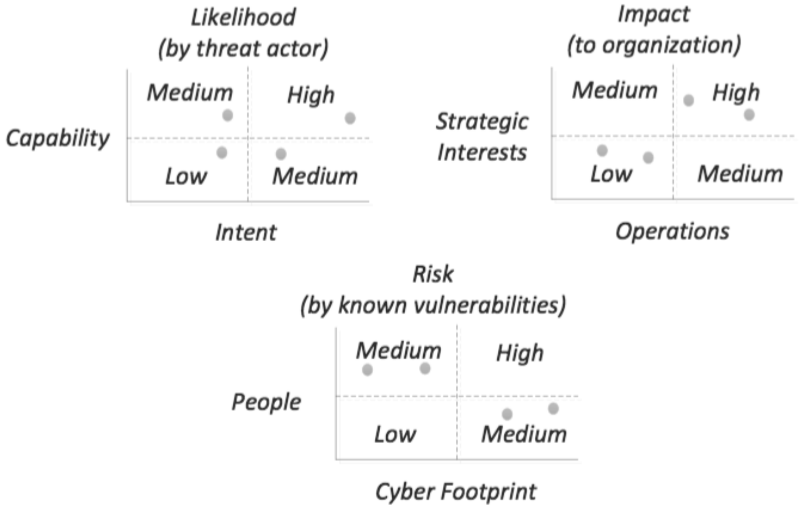

Figure 1. Cyber Threat Prioritization Model[52]

Analyzing potential cyber threats using this these areas is helpful because it allows understanding of threats based on discreet characteristics. This facilitates aligning the policy and prioritization of limited resources for the organization's cyber efforts.[53]

How does this holistically apply to understating cyber threats with national security implications? By seeing threats parsed among these three areas and evaluating them separately, we can make informed decisions on strategy and policy. For example, in Figure 1, the *impact* of the disruption of networks and systems that control the nation's nuclear arsenal would of course occupy the "high" quadrant. This should lead to a corresponding understanding that our cyber strategies in the *risk* quadrant must reduce the cyber footprint e.g., network and digital reliance, and reduce opportunities for human error and interaction with digital networks. Our two primary strategists give us a concise example of this:

> There is no inherent reason that improving information technologies should lead to a rise in the amount of critical information in existence (for example, the names of every secret agent). Really critical information should never see a computer; if its sees a computer, it should not be one that is networked; and if the computer is networked, it should be air gapped.[54]

The supplementary example is one of low impact but high likelihood. This alone can inform prioritization of effort, and may be reduced even further by reducing risk (e.g., people and cyber reliance). The distinction in both examples is that the vulnerability is discretionary. People, the cyber footprint, and the resiliency of the systems (both digitally and socially) are all adjustable and malleable. They also exist astride the digital domain and the human domain.

Our reliance on digital networking will not be reduced as time and technology increase capacity and capability. Of interest are the nature and characteristics of cyberspace as they relate to strategy. Participation in cyberspace is discretionary, and human beings who can construct cyberspaces, and reconstruct them rapidly define vulnerabilities and opportunities. When approached strategically, "Cyberspace can be what we and our enemies make of it."[55] Users participate in their own exposure in cyberspace in a unique way compared to the other traditional domains.

Recommendations

The final analysis of the cyber power conversation begins with what our role is in learning about cyber, understanding vulnerabilities, and perceiving risk. The policy and strategy documents that lay out the direction for operating in cyberspace are misaligned with the actions that the U.S. is taking with regard to understanding the primacy of humans in this domain. Humans ultimately are responsible for making judgments on context, vulnerabilities, and the strategic significance of cyber power. In spite of policy statements establishing the need for a cyber savvy workforce and defense strategies that call for better "cyber-hygiene" most of the effort has been on the technical aspects of securing our digital networks and developing new command structures for cyber forces.[56] People are ultimately the arbiters of our collective success in cyberspace.

One example of the primacy of people and cyber is the 2011 DoD Strategy for Operating in Cyberspace that places emphasis on people as the first line of defense in cyberspace. It directs the "fostering of a culture of information assurance" and advocates high costs for those who engage in malicious activities from inside the network.[57] A cultural shift would be enabled by "new policies, new methods of personnel training, and innovative workforce communications."[58] This innovation in training and culture has not seemed to manifest in practice since the publication of the document. The DoD must increase the education of users and leaders across the board, not just in those specialties related to digital networking.

This education is a baseline for an understanding of cyber power's real capabilities and the context of the power. The general choice to remain uninformed and uneducated about the true nature of cyber power has diluted the discussion and our understanding or risk. We are allowed to remain relatively uneducated about what is possible, and thus become disassociated and divested from the outcomes. Even if strategic cyber warfare is unlikely, cyber power as a complementary action to operational warfare is a reality, and the cyberspaces in which we all operate are ubiquitous. What is not ubiquitous is a common familiarity with those tools, their capabilities, and an understanding of what is actually in the realm of the possible in cyberspace. As exhibited above, there is a common thread among the strategic literature that places *people as the front-line of defense in cyberspace*. What remains in practice is a focus on minimizing the responsibility of users and leaders, hardening our systems, and specializing the expert knowledge. For the U.S. Army, the majority of users' responsibility in cyber is manifested in answering a question (right or wrong) on a logon screen and taking an annual class on information assurance. This is a minimal approach to education on cyber power and cyberspace and one that relies on centralization and control.

Operations in cyberspace and reliance on digital networking are a given. Cyber power-enabled intelligence can be a powerful weapon to complement operational warfare, and can be a threat when wielded by a well-resourced adversary. In practice, the DoD should demand as much understanding of this weapon and one's individual responsibilities as with other individual weapons. One could not imagine dissociation with a pistol or rifle that was as diluted as current individual knowledge about cyberspace and digital networks. Daily interaction with digital networking is exponentially more frequent than with one’s M4 carbine or M9 pistol, yet there is a considerable amount of dissociation with the former that is not accepted with the latter.

Policy that focuses on the technical aspects of threats and risk reduction at the expense of education and training may be less useful as technology further evolves. Kraft, et al., called this the “Adam and Eve Paradox,” whereby in spite of the Moore’s Law and the exponential improvement in technology every 18-24 months, the slant of cyber attacks and threats is trending towards less sophisticated attacks that target “low hanging fruit,” defined as targets that typically involve human mistake and weakness.[59] The paradox is that as technology gets more capable, so do the technical mechanisms to reduce risk. In the cyber threat priority model above, this would translate into having the ability to affect the cyber footprint positively at the pace in which technology and the threats advance. The result is that risk is now more skewed towards the low hanging fruit, *the people* in our organizations. This example reinforces that the military cannot choose to minimize education, and must expand the knowledge and responsibilities about cyber power across all of its units and activities. The cyber specialization of units and occupational specialties is necessary, but should be accompanied by robust programs to educate the majority of cyberspace participants in order to build the resiliency in the larger network.

In his example, Lawson warns against users of cyberspace being passive consumers, lacking the skills and understanding about the digital world to overcome adversity should a disruption of digital capacity occur.[60] Policy makers in the DoD should take this into account when developing units and systems that minimize the involvement of the user. In another example, Patrick Jogoda describes solutions to cyber challenges with a similar idea of decentralization. The best solutions for defending cyberspace and responding to attacks will not come from promoting centralized and monolithic structures but will be “more Wikipedia than Manhattan project. It takes networks to understand, manage, and build networks. In the early 21st century, total control--however well-intentioned--is a fantasy."[61] The trade off in controlling systems and users while decentralizing network power must be carefully balanced in a defense setting.

Conclusion

The strategic discourse on cyber power has developed into a conversation that overestimates the threat, minimizes the context, and reduces the breadth of education and understanding. The premise that gives existential capacity for cyber to damage our will, and then applies the theories of other traditional domains, fails to acknowledge the participatory nature of cyberspace. As Gray notes the “discretionary nature and therefore the variable possible characters feasible for friendly cyberspace(s), mean that the more dangerous potential vulnerabilities that in theory could be available are at best bearable and survivable at worst.”[62] There is not a way to predict the potential of threats and vulnerabilities in future cyberspace. What is predictable is that by design, humans will have the preeminent role in assessing cyber power’s capability, our vulnerabilities, and what we choose to learn and understand about cyber power.

Endnotes

[1] Barack H. Obama, *The 2015 National Security Strategy* (Washington, DC: The White House, 2015), 12.

[2] Clifford S. Magee, “Awaiting Cyber 9/11,” *Joint Force Quarterly* 70 (3rd Quarter, 2013).

[3] Martin Libicki, “The Nature of Strategic Instability in Cyberspace,” *Brown Journal of World Affairs* 18, no. 1 (Fall/Winter 2011): 72.

[4] Martin C. Libicki and Project Air Force, *Cyberdeterrence and Cyberwar* Online (Santa Monica, CA: RAND, 2009), 137, http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=304894 (accessed January 8, 2015).

[5] Barack H. Obama, “Remarks by the President in Year-End Press Conference Online,” *The White House*, http://www.whitehouse.gov/node/314731 (accessed February 23, 2015).

[6] Technical Singularity is the prediction or hypothesis by Victor Vinge that the continued advances in technology will lead to a change that is comparable to the rise of human life on earth. Vinge presented in this idea in 1993 at a NASA symposium and in a paper titled *The Coming Technological Singularity: How to Survive in a Post-Human Era*. At the time he predicted that within 30 years the technological means to create superhuman intelligence would emerge, thus ending the human era. There is a wealth of current research on singularity that blends artificial intelligence, biology, and religion; B. R. Bannister, *Fundamentals of Modern Digital Systems*, 2nd ed. (New York: Springer-Verlag, 1987), 1.

[7] Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* Online (Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2013), 39, http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1147 (accessed February 23, 2015).

[8] Daniel F. Kuehl, *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, First edition. (Washington, D C: Center for Technology and National Security Policy ; National Defense University Press : Potomac Books, 2009), 28, quoted in Gray, *Making Strategic Sense* 9.

[9] Gray, *Making Strategic Sense,* 9.

[10] Ibid., 10.

[11] Martin C. Libicki, “Why Cyber War Will Not and Should Not Have Its Grand Strategist,” *Strategic Studies Quarterly* 8, no. 1 (Spring 2014): 29.

[12] Gray, *Making Strategic Sense*, 7.

[13] John Stone, “Cyber War *Will* Take Place!” *Journal of Strategic Studies* 36, no. 1 (February 2013): 101–108.

[14] Amit Sharma, “Cyber Wars: A Paradigm Shift from Means to Ends,” *Strategic Analysis* 34, no. 1 (January 2010): 64.

[15] Ibid., 72.

[16] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011), 137.

[17] Gray, *Making Strategic Sense*, 44.

[18] Ibid., 14.

[19] Sharma, “Cyber Wars,” 65.

[20] Libicki, “Why Cyber War,” 29.

[21] Sean Lawson, “Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats,” *Journal of Information Technology & Politics* 10, no. 1 (January 2013): 45.

[22] Susan W. Brenner, *Cyberthreats and the Decline of the Nation-State* (Florence, KY: Routledge Research in Information Technology and E-Commerce Law, 2014), 71.

[23] Lawson, “Beyond Cyber-Doom,” 90.

[24] Ibid., 95; Libicki, “Why Cyber War,” 32.

[25] Thomas Rid, “Rid Replies,” *Foreign Affairs* 93, no. 2 (April 3, 2014): 167–168.

[26] Sharma, “Cyber Wars,” 67.

[27] Ibid.

[28] Gray, *Making Strategic Sense,* 45.

[29] Lawson, “Beyond Cyber-Doom,” 88.

[30] Gray, *Making Strategic Sense,* 6.

[31] Ibid., 4.

[32] Libicki, “Why Cyber War,” 31.

[33] Obama, “Remarks by the President”

[34] Ann Hornaday, “Review: ‘The Interview’ Has Some Laughs and Makes Some Points but Isn’t as Edgy as Its Reputation Suggests Online,” *The Washington Post*, December 24, 2014, http://www.washingtonpost.com/lifestyle/style/review-the-interview-has-some-laughs-and-makes-some-points-but-isnt-as-edgy-as-its-reputation-suggests/2014/12/24/97b85a8a-8ba9-11e4-a085-34e9b9f09a58_story.html (accessed March 22, 2015).

[35] Libicki, “Why Cyber War, Strategist.” 33.

[36] ScienceFriday, “Which Cyber Hacks Should We Worry About?” January 16, 2015, *Science Friday.com*, streaming video, 12:23, http://sciencefriday.com/segment/01/16/2015/which-cyber-hacks-should-we-worry-about.html (accessed January 23, 2015).

[37] Gray, *Making Strategic Sense,* 14.

[38] P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford ; New York: Oxford University Press, 2014), 6.

[39] Ibid.

[40] Brandon Valeriano and Ryan Maness, “Persistent Enemies and Cyberwar” in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 141.

[41] J. Carr, “The Misunderstood Acronym: Why Cyber Weapons Aren’t WMD,” *Bulletin of the Atomic Scientists* 69, no. 5 (September 1, 2013): 32.

[42] Ibid., 39.

[43] Lawson, “Beyond Cyber-Doom,” 96.

[44] Ibid., 97.

[45] Ibid.

[46] Ibid.

[47] Ibid.

[48] Jay McAllister and Troy Townsend, “Implementation Framework- Cyber Threat Prioritization Online,” *Carnegie Mellon University Software Engineering Institute* (September, 2013): 4.3, http://sei.cmu.edu/about/organization/etc/upload/framework-cyber.pdf (accessed March 6, 2015).

[49] Ibid.

[50] Ibid., 4.6.

[51] Ibid., 4.8.

[52] Ibid., 4.4.

[53] Ibid., 4.3.

[54] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge ; New York: Cambridge University Press, 2007), 105-106; Martin C. Libicki and Project Air Force (U.S.), *Cyberdeterrence and Cyberwar Online* (Santa Monica, CA: RAND, 2009), 19, http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=304894 (accessed January 8, 2015); quoted in Gray, Making Strategic Sense, 47.

[55] Ibid., 31.

[56] *Department of Defense Strategy for Operating in Cyberpace*, 6.

[57] Ibid., 7.

[58] Ibid.

[59] Moore’s Law is the observation by Gordon E. Moore that over the history and glide path of computing hardware, the number of transistors that can be placed within an integrated circuit doubles every two years. This concept is explained in detail in Moore’s paper “Cramming More Components onto Integrated Circuits,” *Readings in computer architecture* (2000): 56, and the online source “Moore’s Law, Part 1: Brief History of Moore’s Law and Current State,” *Research Blog*, n.d., http://googleresearch.blogspot.com/2013/11/moores-law-part-1-brief-history-of.html (accessed March 25, 2015); Michael Kraft, et al., “The Adam and Eve Paradox,” Proceedings of the International Conference on Information Warfare & Security, January 2013, 275.

[60] Lawson, “Beyond Cyber-Doom,” 98.

[61] Patrick Jogoda, “Speculative Security,” in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron, (Washington, DC: Georgetown University Press, 2012), 33.

[62] Gray, *Making Strategic Sense,* 67.