Strategy Research Project

A Cyberspace Primer: What Every Strategic Military Leader Must Know

by

Lieutenant Colonel Michael J. Perez
United States Marine Corps

United States Army War College
Class of 2014

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-04-2014	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
A Cyberspace Primer: What Every Strategic Military Leader Must Know

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Michael J. Perez
United States Marine Corps

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Mr. Brian Gouker
Department of Military Strategy Planning and Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

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

13. SUPPLEMENTARY NOTES
Word Count: 8126

14. ABSTRACT

Adversary cyberspace capabilities threaten the United States military and national security interests across all levels of conflict. Despite these threats, within the United States military and senior civilian leadership there exists limited knowledge on cyberspace beyond rudimentary user-level understanding. This project serves as a primer to help fill the educational gap of strategic military leaders on the attributes and issues of cyberspace relevant to modern national security. It will accomplish this task by reviewing cyberspace's evolution, the legal issues surrounding the application of international law of armed conflict, and the ways and means of conducting offensive and defensive cyberspace operations. The discussion will conclude by developing a framework based on the variables of attribution, attacker identity, target criticality, and attack severity to provide the strategic military leader with a conceptual model for development of a whole-of-government response to adversaries who threaten the United States through cyberspace.

15. SUBJECT TERMS
Cyberspace Attributes, Offensive Cyberspace Operations, Defensive Cyberspace Operations

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	44	

USAWC STRATEGY RESEARCH PROJECT

A Cyberspace Primer: What Every Strategic Military Leader Must Know

by

Lieutenant Colonel Michael J. Perez
United States Marine Corps

Mr. Brian Gouker
Department of Military Strategy Planning and Operations
Project Adviser

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

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

Abstract

Title:	A Cyberspace Primer: What Every Strategic Military Leader Must Know
Report Date:	15 April 2014
Page Count:	44
Word Count:	8126
Key Terms:	Cyberspace Attributes, Offensive Cyberspace Operations, Defensive Cyberspace Operations
Classification:	Unclassified

Adversary cyberspace capabilities threaten the United States military and national security interests across all levels of conflict. Despite these threats, within the United States military and senior civilian leadership there exists limited knowledge on cyberspace beyond rudimentary user-level understanding. This project serves as a primer to help fill the educational gap of strategic military leaders on the attributes and issues of cyberspace relevant to modern national security. It will accomplish this task by reviewing cyberspace's evolution, the legal issues surrounding the application of international law of armed conflict, and the ways and means of conducting offensive and defensive cyberspace operations. The discussion will conclude by developing a framework based on the variables of attribution, attacker identity, target criticality, and attack severity to provide the strategic military leader with a conceptual model for development of a whole-of-government response to adversaries who threaten the United States through cyberspace.

A Cyberspace Primer: What Every Strategic Military Leader Must Know

> The importance of cyberspace to the American way of life – and to the Nation's security – makes cyberspace an attractive target for those seeking to challenge our security and economic order.
>
> –2014 *Quadrennial Defense Review*

Adversary cyberspace capabilities threaten the United States military and national security interests across all levels of conflict. At the tactical and operational levels, our potential adversaries are increasing their ability to create physical effect on the battlefield through integration of cyberspace capabilities with conventional forces to negate United State conventional military advantage. At the strategic levels, cyberspace enables adversaries to bypass American conventional and even nuclear military strength to target indirectly the industry, resources, and will of the people that are the foundation for American power and whose loss could potentially cause the collapse of American society. Even without creating these mentioned severe strategic, operational, and tactical effects, cyberspace allows our adversaries to undermine American innovation and economic advantage as they steal billions of dollars of intellectual property each year.

Despite these threats to the American way of life, within the United States military and senior civilian leadership there exists limited knowledge on cyberspace beyond rudimentary user-level understanding. The military is slowly correcting this deficiency through education and empirical experience. However, the rate of change of cyberspace and computer technology capabilities roughly doubles every two years[1] while strategic leader education on cyberspace, when it occurs, evolves at a significantly slower rate.

As an example, at the U.S. Army War College in academic year 2014, students received only 3 hours of explicit instruction on cyberspace in the core curriculum. This instruction covered very basic characteristics of cyberspace and discussed the government agencies responsible for United States cyberspace operations. The limited instruction did little more than provide a cursory glimpse of the complexity cyberspace creates in socio-economic and competitive dynamics of international relations and provided no insight for integrating cyberspace across the broader Joint Force and interagency structure.

Approximately 14% of the 2014 Army War College class participated in electives on cyberspace that totaled between 30 and 60 additional hours of instruction. While this creates a small pool of students with greater awareness of cyberspace operations, the fact that this group represented such a small portion of the class indicates the lower priority assigned to understanding the strategic importance of this critical warfighting domain and the associated risk it creates for the United States.

This project serves as a primer to help fill the educational gap of strategic military leaders on the attributes and issues of cyberspace relevant to modern national security. It will accomplish this task by reviewing cyberspace's evolution to its present day characteristics that make it both a force multiplier and a critical vulnerability. It will then review the legal issues surrounding the application of international law of armed conflict and the ways and means of conducting offensive and defensive operations in cyberspace. The discussion will conclude by developing a framework based on the variables of attribution, attacker identity, target criticality, and attack severity to provide the strategic military leader with a conceptual model for development of a whole-of-

government response to adversaries who threaten the United States through cyberspace.

Background

Despite almost 45 years elapsing since the transmission of the first segment of data on the predecessor of today's internet, the world is still struggling to develop norms for behavior between, individuals, groups, and states in this relatively new domain. Initially designed as an open information-sharing network, the Advanced Research Projects Agency Network (ARPANET) and its descendant, the internet, were "designed to be collaborative, rapidly expandable, and easily adaptable to technological innovation. Information flow took precedence over content integrity; identity authentication was less important than connectivity."[2] This open access to information is "an incubator for new forms of entrepreneurship, advances in technology, the spread of free speech, and new social networks that drive our economy and reflect our principles."[3]

The openness of cyberspace and the internet have also been a source of threat by those who seek to control other humans through control of their access to information. Additionally, the nefarious side of human nature saw opportunity in the accessibility cyberspace provides. From almost the beginning of cyberspace interaction, those with the technical means, and the will to use those means to create relative advantage, have exploited cyber-enabled access for their unitary rather than collective advantage or to deny advantage to others.

As the technological capability of these means have evolved, the effects cyber antagonists can generate in both the cyberspace and physical domains have increased exponentially which highlights that "(o)ur reliance on cyberspace stands in stark contrast

to the inadequacy of our cybersecurity."[4] The threat of these increasing effects and the United States' dependence on cyber is creating an asymmetric advantage for adversaries that if left unchecked could significantly undermine the United States' leadership and ability to influence the international environment through its more traditional instruments of power. Determining when exploitive cyber activity is legally, ethically, practically, and politically justified requires a holistic understanding of the actors involved, the action taken, and the outcome of the action. This understanding begins with knowledge of the cyberspace environment.

Key Attributes of the Cyberspace Environment

Joint military doctrine and government policy have identified cyberspace as a manmade domain. Military professionals will attempt to comprehend this relatively new warfighting domain by applying the principles of war as they have to the physical domains. While similarities of cyberspace to the physical domains exist, many key attributes of cyberspace are so distinct either they magnify parts of the principles of war to previously unimagined levels or they are so unique they require a new perspective on their effect on conflict. In particular, we will discuss here the pervasiveness, speed, volume, scalable effects, and anonymity cyberspace creates.

Pervasiveness

Although the internet originated in the United States as ARPANET, it has become a global phenomenon. By 2012, one third of the world's population was online.[5] Although the western world (Europe and North America) has a greater percentage of its population online (63-78%), the larger population of the rest of the world creates a greater total number of internet users – 67.1% of the total online population.[6] Asia alone

accounts for 44% of world internet population with over one billion people online (over three times the entire population of the United States).[7]

Even those individuals that are not directly online are still dependent upon cyberspace for many aspects of their day-to-day living. Financial transactions; power, water, and food distribution; communication and transportation services; to name just a few, are dependent on the free flow of information in cyberspace. An important point regarding the pervasiveness of cyberspace is the vast majority of the actors are not governments or militaries but individuals, corporations, and private companies. Therefore, government institutions can play an important role in defining norms and policy for cyberspace activities but they will not be the exclusive arbiters of acceptable behavior.

Speed and Volume of Effects

Related to the pervasiveness of cyberspace are its characteristic speed and volume of effects. With the push of an 'Enter' key, an actor can project their intent near-instantaneously around the globe. Additionally, these generated effects can impact millions of people and systems simultaneously, highlighting cyberspace's asymmetric nature. "Small-scale technologies can have an impact disproportionate to their size; potential adversaries do not have to build expensive weapons systems to pose a significant threat to U.S. national security."[8]

Scalable Effects

Cyberspace can be a precision weapon or a 'weapon of mass disruption'.[9] An actor can direct malicious cyber activity[10] simultaneously to either a single user or nearly the entire cyberspace population. The scale of these effects can range from legal, beneficial activities like financial transactions, to mildly annoying spam email, on to

disruptive viruses, and destructive attacks that cause significant damage or even death. The multipurpose use of cyberspace for both beneficial and harmful effects and the speed and volume with which an actor can apply them magnifies the challenge of controlling and protecting activities in cyberspace.

Anonymity

Even without taking deceptive measures, an actors' physical identity is filtered through a computer and transmitted through servers into cyberspace as an Internet Protocol (IP) address. Tracing the IP address back to its source only provides the location of the computer but not necessarily the identity of the user. Skilled cyber-attackers have developed methods to prevent IP address tracing during the conduct of cyber activity. Worse yet, they provide these techniques and software for free or for purchase to others on the internet.

A simple Google search yields thousands of downloadable applications for identity spoofing or concealment to completely erase online activities or make it appear to network defenders that an external attack was conducted by someone else (proxy spoofing). Likewise, there are other applications that circumvent networks' security altogether by scanning already authenticated IP addresses and then exploiting vulnerabilities in authenticated systems to replicate the address of one of these systems providing the attacker access the network disguised as an authorized user. Likely, the most accessible and self-proclaimed legitimate identity-concealing services is the Tor Project.

Originally known as The Onion Routing Project[11] and developed with funding from the United States Naval Research Laboratory, Tor attempts to provide anonymous internet communication. Without going into a highly technical discussion, Tor accepts a

data transmission request into a network of over 5000 volunteer servers[12] and randomly assigns a communication path through these servers to the destination. At each step through the path, Tor creates a new encryption scheme for the data it is sending so each node knows only one step of the prior source and future destination but not the entire routing path.[13]

Methods of statistical analysis exist that may allow inference of the originator and destination by scanning the entrance and exits of the Tor network. However, these methods require either specific knowledge of the suspected originator and destination or significant and costly whole network monitoring and analysis capability. As the number of Tor users increases, so does the difficulty of monitoring and analysis.[14]

Tor usage is on the rise as its potential anonymity provides an incentive for 'good' behavior like human rights activists in repressive countries and for darker, exploitive behavior like the "Silk Road"[15], a drug smuggling ring operating exclusively on Tor's hidden network.[16] While these examples of behavior in cyberspace are clearly distinguishable as good or bad, significant behavior also exists whose virtue is interpretive based on the viewers' perception? It is on the basis of defining proper behavior in these grey areas that governments, businesses, and populations must tackle the legal issues related to cyberspace.

Legal Issues

Specific to competition and conflict, the international community has struggled with framing the use of cyberspace for influencing the actions of others in the business, political, and diplomatic realms. From the state-to-state and state-to-non-state actors' perspectives, the international community has attempted to apply various bodies of law like the Geneva Conventions and the United Nations Charter to cyberspace activities as

a framework for determining their legality and ethics. The issue whose legal ambiguity creates the largest instability for international relationships in cyberspace is determining what constitutes an attack in cyberspace. This issue is central to bringing clarity to international norms and legality as it relates to state and non-state interactions in cyberspace. Its resolution will also clarify a host of other issues like 'when a state can invoke self-defense' and 'whom it can respond against for an attack from cyberspace'.

The United States position as expressed by State Department Legal Adviser Harold Koh, and concurred with by a NATO 'International Group of Experts' in the Tallinn Manual[17], is "(c)yber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force".[18] The phrase 'use of force' is consistent with the United Nations Charter Article 2, which directs charter members to "refrain… from the threat or use of force".[19] Although not specifically stated in the United Nations Charter, the opinion of the Tallinn Manual 'Group of Experts' is that a use of force in cyberspace that reaches a threshold of injury, death, or significant destruction[20] would constitute an "armed attack".[21] Therefore, a self-defense response from the victim state according to Article 51 of the United Nations Charter would be justified.

While the 'injury, death, or destruction' legal correlation of a cyber-attack to an armed attack appears straightforward, there are two complicating factors. The first factor is what the author identifies as 'layers of causality'. The second factor is the collective body of laws on armed conflict is state-centric while cyberspace enables non-state actors to conduct an "armed attack" whose significant effects were previously only within the power of states' armed forces to create.

The recent DIRECTV television commercials are a humorous representation of the concept of layers of causality. In the commercials, an unpredictable series of events begins with an individual watching cable television instead of DIRECTV and ends with the person being "body slammed by a lowland gorilla" or becoming "a local fisherman they call Big Fatty Face."[22] Similarly, since at its most basic level a cyber-attack is just the transmission of a low-voltage signal it likely is incapable of creating injury, death, or destruction as first order effect. Instead, it relies on a series of cascading higher-order effects to achieve an attacker's objective that exist in the physical domain. As the layers of causality increase in number, the ability to correlate directly a higher-order effect to the initial attack becomes more ambiguous since other factors external to the cyber-attack likely also contributed to its ultimate effect.

The authors of the Geneva Conventions could not have envisioned the asymmetric empowerment cyberspace would create for non-state actors. Thus, the 1949 conventions do not specifically address non-state actors conducting armed attacks against state entities. Even the 1977 Additional Protocols adopted fourteen years after ARPANET's first transmission, do not account for this empowerment. The United States Military Commissions Act of 2006 codified a status of "unlawful combatants" for hostile non-state actors and updated the status title in the 2009 Military Commissions Act to "unprivileged enemy belligerent".[23] The United States Congress created this status specifically in response to terrorist organizations like Al Qaeda and the Tallinn Manual affirmed the concept with a near-identical status of "unprivileged belligerent".[24]

Though created for Al Qaeda, it is easy to see the utility to states of applying this status to other non-state actors who use asymmetric means, whether they are large

fuel-filled commercial aircraft or computers and networks to create devastating effects. The Geneva Conventions do not reflect this belligerent status, though, which creates legal ambiguity that may inhibit the United States use of its military to attack or counter non-state cyberspace actors in or out of the cyberspace domain. Strategic leaders understanding of these issues of ethics and legality is just as relevant to the concepts of offense and defense in cyberspace as in the physical domains.

Cyber Offense

The conduct of offensive actions in cyberspace requires resolution of the strategic question of ‘why to attack’; the operational question of ‘when to attack’; and the tactical question of ‘how to attack’. First, we will tackle the operational and strategic questions as they relate to the legality of initiating a cyber-attack. To begin this discussion, we must recognize the previously discussed cyberspace attributes of pervasiveness, speed, and volume all enable the generation of scalable effects across many of the instruments of power with relatively little resource expenditure.

As a form of cyber maneuver-warfare based on the Sun Tzu-ish notion of ‘attack weakness, avoid strength’, adversaries in cyberspace are developing cyber capabilities as an alternate means and low cost asymmetric counter to traditional military dominance and economic strength. The determinants for the legality of cyber-attacks on or by the United States are the amount of initiative the attacker possesses and the underlying and precipitating causes that triggered the attack. On the proactive end of the scale are ‘purely offensive’ operations where the attacker’s initiative is very high. On the other end is a reactive counterattack in response to aggression from an attacker.

‘Purely Offensive’ Cyberspace Operations

A purely offensive attack is an option when an actor has the initiative to choose when to execute a cyber-attack and actions by the victim prior to the attack cannot be reasonably perceived as a threat that precipitated the attack. In this case, the attacker’s perception of the political situation and strategic to operational environment created an assessment of risk versus gain that favored taking offensive action. In this null-deterrence situation, the attacker perceived the potential gain action would create outweighs any risk of potential loss.

The standard risk formula states risk is the product of the probability of an event occurring and the severity of harm if it did occur. Applying this formula to an actor’s risk versus gain calculus could quickly tilt it in favor of taking offensive cyber action if the perceived risk of being caught is low due to an assumption of anonymity in cyberspace. In the evolving history of the modern world, the interdependence wrought by globalization and cyberspace means few, if any, international relationships do not have historical precedence. This makes a purely offensive attack from a solely realist-based calculation of interests unlikely, which leads to the discussion of attacks based on a perception of threat from an adversary.

Preventive Cyberspace Operations

Applying ‘opportunity’ to the traditional quasi-mathematical representation of threat as the product of capability and intent[25] creates a more accurate threat ‘equation’:

Threat = Capability x Intent x Opportunity

Within the context of this derivative equation, a preventive attack is an attempt to deny an adversary with a professed hostile intent from gaining a future capability and/or opportunity to harm your interests. However, historic application of the United Nations

Charter implies preventive attacks against a potential future threat are illegal. Recent legal opinions found both in Mr. Koh's statement and in the findings of the international 'Group of Experts' also condemn the preventive use of offensive cyber activities that cross the "armed attack" severity threshold.[26]

Although commonly regarded in the context of a symmetric cyber-versus-cyber preventive attack, this concept can also apply asymmetrically from cyberspace to other future capabilities of an adversary in the physical domains. For example, the Stuxnet virus damaged over 1000 centrifuges at Iran's Natanz nuclear facility until 2010 when the Iranians finally detected it. Stuxnet represents an asymmetric employment of a preventive attack from cyberspace that analyst estimate setback Iran's nuclear enrichment program by two years.[27]

Preemptive Cyberspace Operations

The distinguishing characteristic of a preventive attack and a preemptive attack is the perception of the attacker to the imminence of the threat posed by the adversary. If the would-be victim determines the adversary possesses intent and is on the brink of creating the capability while an opportunity to exploit a vulnerability exists, or already possesses the intent and capability and is awaiting a viable opportunity, the would-be victim may launch a preemptive attack to disrupt the threat.

Literal application of the United Nations Charter does not explicitly condone a preemptive attack. However, the international community in both common law jurisprudence and practice allows nations not to 'take the first hit' if hostile intent and imminence of attack are certain.[28] In cyberspace this is difficult, though, because unlike in the physical world, there are no 'forces massing on the border' to assist with

imminence determination and once an attack begins, the ‘movement-to-contact’ progresses near instantaneously at the speed of electronic signal transmission.

Cyber Response Operations

The most legitimate and internationally accepted type of attack is counterattack. International law and norms advocate a state’s right to self-defense and collective self-defense with allies.[29] The intent for allowing counter attack in self-defense is to stop the attack and its effects. Historically, counters to physical attacks, also tended to be physical or ‘kinetic’ in current parlance. Cyberspace convoluted the ways and means of counterattack since a physical attack may be countered with cyber response and vice versa.

The asymmetry available in responding to aggression from a physical domain or the cyber domain can make determining the Law of Armed Conflict *jus in bello* requirements for proportionality and discrimination more opaque, especially when determining the source of the attack is difficult. Additionally, the justness of counterattack is derived from the necessity of stopping the initial aggression. However, more enduring security comes from deterring future aggression, not just stopping the current attack. An asymmetric or disproportionate reprisal may be necessary to deter future hostile acts by changing the aggressor’s risk-benefit calculation.

Cyber-Attack Actions

Having determined the strategic and operational answers for ‘why’ and ‘when’ to conduct offensive cyberspace operations, we can progress to a brief discussion to familiarize strategic leaders with the most common tactics adversaries use to conduct cyber-attacks. As previously noted in the scalable effects discussion, attacks in cyberspace can vary in range from inconvenience to destruction. Joint Publication 3-12

Cyberspace Operations identifies the predominant function of a cyber-attack as 'Deny' with a scale of severity based on the degradation and duration the targeted system experiences.[30] Table 1 outlines the attributes of the progressive levels of severity: Degrade, Disrupt, and Destroy. As depicted, Degrade is a reduction in capacity of the targeted system for a temporary period. Disrupt, colloquially referred to as a Distributed

Table 1 – Denial Severity Levels

Deny		
	Level of Degradation	Duration
Degrade	< 100%	X = Temporary
Disrupt	~100%	X
Destroy	100%	Infinite

Denial of Service (DDOS) attack, renders the targeted system essentially non-functional for a temporary period. Destroy aptly describes permanently rendering the targeted system non-functional.

Four additional types of malicious cyberspace activities also exist. They are probes, espionage, theft, and corruption.[31] The first of these activities is not actually an attack but an enabling, non-destructive probe. Although often characterized in the media as an attack, a probe is just a scan of a network conducted by a potential adversary to collect intelligence, map systems, or determine if vulnerabilities exist. However, as seen in the legal discussion, they do not meet the threshold of a use-of-force.

Cyber espionage is gaining unauthorized access to information and exploiting this access to gain advantage. This can include compromising commercial proprietary information, military war plans, or advanced weapons design. This is the form of malicious cyber activity arguably most often attributed to China. The 2013 Commission on the Theft of American Intellectual Property estimates the United States loses over

$300 billion of intellectual property each year to Chinese cyber espionage in what then-Director of the National Security Agency, General Keith Alexander, called “the greatest transfer of wealth in history.”[32]

Similar to cyber espionage is cyber theft. It also begins with the adversary gaining unauthorized access to network systems but rather than just accessing the compromised information, they steal it thereby depriving its owner of access to it. Thus, theft is a form of denial but rather than just denying the victim access to the information, the attacker also derives benefit from exclusive possession of it. The most prevalent form of this activity is the theft of ‘virtual wealth’ in a zero sum game flowing from the victim to the cyber thief.

Possibly the most insidious of malicious cyber activities is corruption. In cyber espionage or denial attacks, the victim’s data are still intact, though potentially inaccessible for a period, and in a cyber-theft, the data are recognizably missing. In a corruption attack, data or the targeted system itself are still present but altered. If corruption is unrecognized, cyber-attackers can use it to enable follow-on exploitation. If recognized, it can lead to loss of trust for the exploited data or network. The Iranian attack on the Navy-Marine Corps Intranet (NMCI) in late 2013 is a prime example of a corruption attack. Although it does not appear any damage was done, the loss of trust for the integrity of the network and the information stored on it, caused the Navy to iteratively shut down portions of the network multiple times at a cost $10 million to confirm removal of the malicious software (malware).[33]

While it may appear convenient to segregate discussion of offensive and defensive cyber activities, the reality is the complexity of the interaction of deterrence,

preemption, and response to aggression inextricably links cyber offense and defense. Although the adage ‘the best defense is a good offense’ is useful in the physical domains, at the intersection of the physical domains with international law and cyberspace, the ambiguity requires a strong defense as well.

Cyber Security and Defense

Regardless of the domain, defensive strategy tends to be an integration of three principles: Prevention, Deterrence, and Response. Referring back to the elements of the derived threat equation, the intent of a potential adversary lies in the larger realm of international relations and diplomacy, meaning cybersecurity can only indirectly influence it. Where cybersecurity can directly influence the remaining elements of the threat equation is through ‘Prevention’ to deny the adversary the credible capability to inflict harm. An actor can create ‘Prevention’ through self-screening cybersecurity best practices to identify and eliminate vulnerabilities before adversaries can exploit them. This will make critical systems ‘hard targets’ that are ideally impervious to cyber-attack.

‘Deterrence’ works against the would-be attacker’s opportunity perception by displaying sufficient credible capability to promise unacceptable harm to an adversary in response to a cyber-attack. ‘Response’ reinforces deterrence when it has failed by decisively stopping an adversary’s current attack before it achieves its objective. This alone may be insufficient, however, to deter future attacks and has not wrested initiative from the adversary. An overmatched response – where *jus in bello* questions of proportionality and discrimination must be resolved – makes harm caused through response to the initial attack more than the adversary is willing to endure in the future, thus reestablishing ‘Deterrence’.

The pervasiveness, anonymity, and low cost to enter the cyber environment provide advantage to the attacker. Therefore, an effective cyber defense must integrate the three principles of Prevention, Deterrence, and Response. When used collectively, they reinforce each other, but a defense based on only one or two of the principles will eventually reveal vulnerabilities an adaptive adversary will exploit.

In addition to the above issues with ‘Prevention’, there is often a technical dichotomy of security and usability where increasing security decreases accessibility and functionality of cyber systems. Inherent human complacency and laziness allows attackers to exploit human nature to create, locate, and exploit vulnerabilities in cyberspace systems. Phishing schemes, simple/common system access passwords, and failure to apply security updates are prime examples of this troubling aspect of cybersecurity.

These issues pose government agencies and departments with a difficult choice: attempt a ‘defend everything’ approach or play ‘whack-a-mole’ against threats as they become apparent. Without completely scrapping current cyberspace protocols and architecture and starting over, the former approach is currently liable to fail. It is likely prohibitively expensive and technically impossible to defend all aspects of friendly networks all the time. The rapidly evolving nature of cyberspace technology usually creates new vulnerabilities when it is upgraded.

The ‘whack-a-mole’ approach is also expensive because time-sensitive corrective software and hardware development processes are disproportionately expensive. An attacker can purchase rudimentary malware on the internet for a few thousand dollars. Though network defenses usually detect and eventually defeat these

applications, it costs the government and commercial industry millions of dollars to develop and maintain these responsive systems.

Against more sophisticated threats, network defenses may not know a vulnerability exists until an attacker exploits it. The cybersecurity community refers to these instances as ‘zero day vulnerabilities’.[34] Zero day vulnerabilities/attacks are especially damaging because cybersecurity or original software developers must rush to develop a patch for the vulnerability, often at significant cost. Meanwhile, until the patch is released, networks continue to suffer harm caused directly by the threat or from the loss of access as administrators take them offline to prevent exploitation. This is why cybersecurity specialists are trying to change the paradigm with a defense-in-depth mindset similar to what the military uses to defend against a physical attack.

“Active cyber defense is DoD’s (Department of Defense) synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities.”[35] The active defense concept[36] is based on prioritizing limited defensive capabilities to proactively defend the most vital assets while ceding non-critical activities/items (analogous to ceding terrain in a physical military defense) as maneuver space. This creates a defense-in-depth where ever-increasingly capable layers of defense attrite enemy cyber-attacks prior to them achieving their objective.

In the United States, the government has identified these vital assets as ‘critical infrastructure’. Critical infrastructure’s survival and unencumbered function “provides the essential services that underpin American society… (and) are vital to public confidence and the Nation’s safety, prosperity, and wellbeing”.[37] Critical infrastructure consists of 16

sectors and includes such assets as financial markets, nuclear programs, emergency services, and the defense industrial base.[38]

A downside of active cyber defense is it is analogous to ‘squeezing a balloon’ where increasing security measures in one area transfers threat to other parts of ‘grey’ (neutral or non-critical friendly) cyberspace. However, it does attempt to create ‘hard targets’ out of truly critical systems to ideally dissuade lower level threats from challenging these systems so cybersecurity can focus on high-end threats.

Cyber Response Model

Integrating the preceding discussions on cyberspace attributes, legal, offensive, and defensive issues, this section provides the strategic military leader with a conceptual model for cybersecurity, defense, and response. It also introduces the current DOD lexicon for cyberspace operations as they relate to the model.

The speed and anonymity of cyberspace attacks means the response model must be comprised of two different layers. The first layer assumes the source of an attack is not readily apparent. Therefore, the United States will initially rely on an active defense to recognize an attack is occurring, isolate the target to eliminate spread, stop the attack, and then mitigate the effects to restore affected systems and entities. Investigation of the attack to determine its source will ideally enable a counter-response, which is the second layer of the model based on classic deterrence theory.

If the United States can determine who attacked its government or private enterprises, it will then have the option to hold the antagonist accountable. Determining the appropriate response (meaning a counter action in this discussion) to malicious cyber activity must account for whether the source of the attack is known, the severity or level of damage from the attack, the criticality of the object or activity attacked, and the

identity of the attacker. Of these contributing response variables, the most important initially is determining the source of the attack as none of the other variables matter if the response action has no target. The problem of determining the source, identity, intent, and authority of a cyber-attacker is referred to as attribution.

Attribution

As covered in the anonymity attribute discussion, the volume of cyberspace and the relative technical ease of obscuring identity within it makes gaining attribution challenging. As cyberspace technology continues to advance, those seeking anonymity and those seeking to determine identity will remain locked in a cat-and-mouse game. This means it is unlikely that determining attribution will ever be completely impossible. Identity-obscuring techniques of today may be defeated by tomorrow's technology.

However, achieving attribution against an attacker using sophisticated identity-masking measures can be time and resource intensive. This may make the cost of determining the source of an attack not worth the expense of just mitigating and recovering from the attack's effects. This is the premise of anonymity under which many of the lower end cyber-attackers operate and persist. As long as they do not cross a threshold of severity or threaten a critical item or activity, it is cost ineffective to individually determine their identity and respond to them.

Another complication for determining attribution is technically it may only be possible to determine the geographic location and individual computer system from which an attack was launched. This does not provide the actual identity of the individual(s) who initiated the cyber-attack. For example, a cyber-operator from China could physically travel to the United States and initiate an attack from a server within the United States to remove any direct electronic linkage to China. Further complicating

attribution is the capability to route an attack through multiple proxy systems. When tracing an attack back to its source, unless the cyber response forces can determine the physical identity of the attacker, it can be difficult to know when they have arrived at the end of the trace… is there another layer to the onion?

Even when the attribution threshold is reached, for intelligence, technical, or diplomatic reasons, it may be infeasible for the United States to publicly acknowledge or respond to an attack. A response may deny the United States further intelligence from the source of the attack. Additionally, if the response is cyber-based, the technical details of it will likely become apparent. The United States must then make a hard determination of whether the current attack severity and target criticality are worth the potential loss of effectiveness of future cyber-attack/response capability. Weighing technical and intelligence gain/loss for future potential threats against the current situation can be a difficult choice. It may also be a difficult diplomatically and politically to publicly acknowledge a cyber-attack has occurred. In the strategic balance of international relations, even if an attack is attributable, if its severity is tolerable and it does not threaten critical interests or resources, the United States may not seek retribution if doing so would create a larger political, diplomatic, or economic cost.

From all of these complications, it should be apparent that attribution is not a polarity of ‘knowing’ or ‘not knowing’, but rather a gradient of how much do you know. The determination of knowing enough to create a ‘response-quality’ attribution threshold of the identity of a cyber-attacker is likely contextual. Figure 1 depicts the basic two layers of the response model with a gradient of attribution. The base non-attributable layer is target-centric and consists of defensive actions to detect, isolate, and stop an

attack. If the United States can attribute the attack's source to a 'response-quality' level,

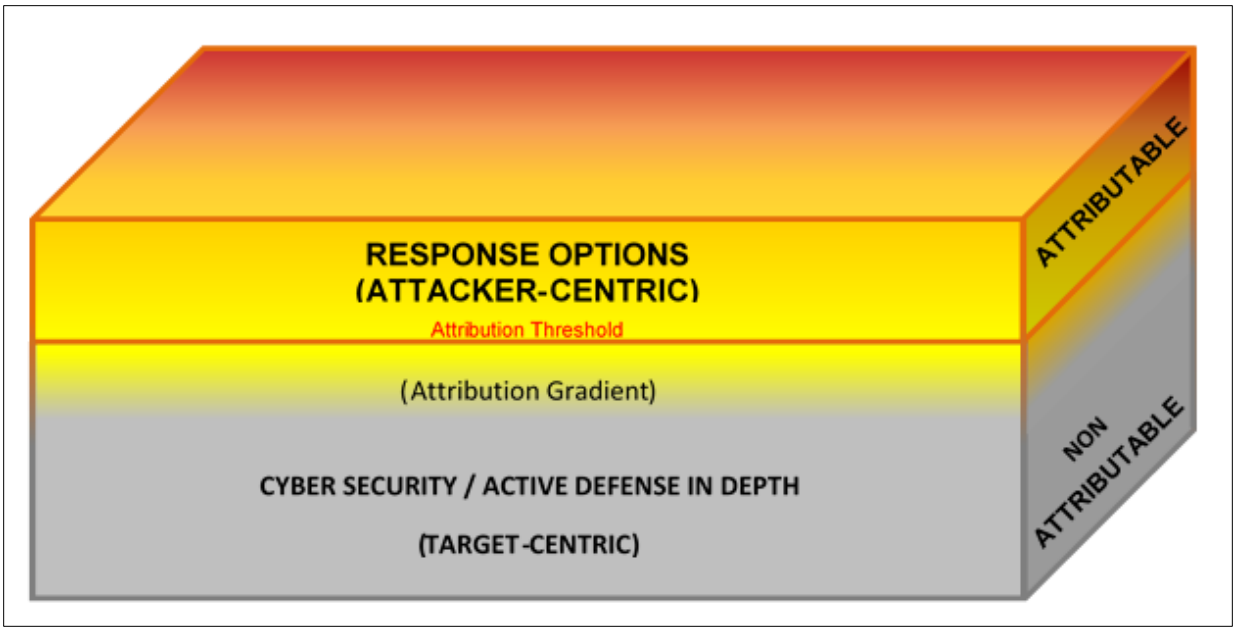

Figure 1 - Response Potential Based on Attribution

the second attacker-centric layer includes response options. How the United States should respond is contingent on and refined by the additional contributors to the model with the next relevant question being what is the identity and authority of the attacker.

Identity

At the lowest level, an individual or small group is the initiator of a cyber-attack. The real question is did the individuals operate on behalf of a state, organization, or group or were they acting on their own volition. Determining this is important because it affects the authority and ethics of a United States response to the attack. As depicted in Figure 2, cyber-attackers can range from individuals to states and the United States' appropriate response across its instruments of power would vary based on the attacker's identity.

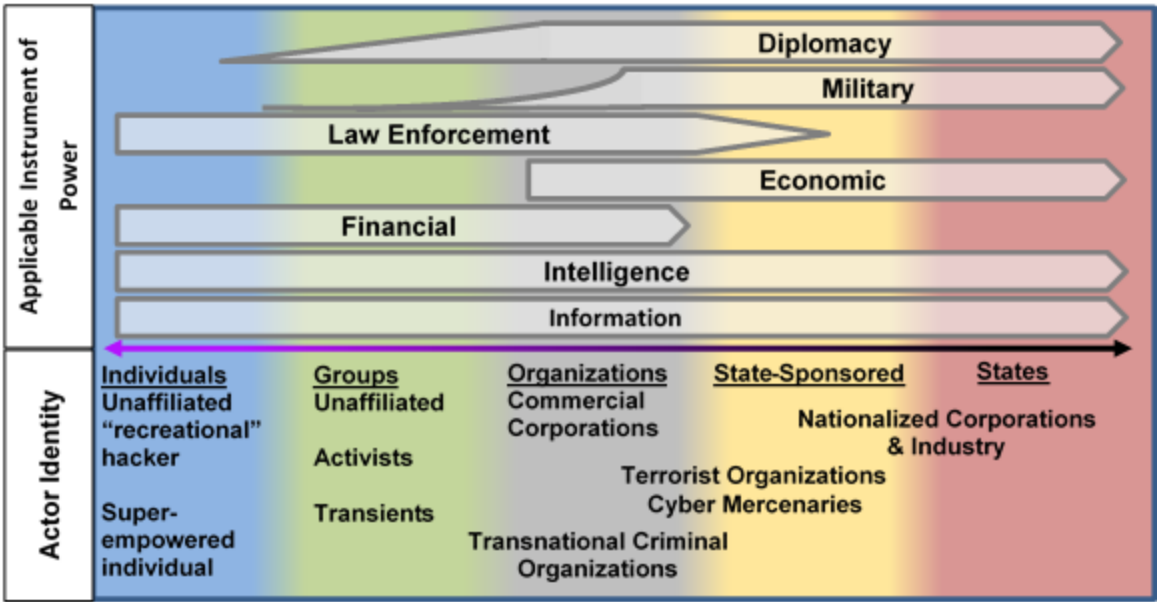

Figure 2- Attacker Identity / Applicable Response Powers

The most easily understood cyber-attacker identity is the state since the current international order is based on the primacy of states in international relations. Diplomatic, economic, and security organizations like the United Nations, Association of Southeast Asian Nations (ASEAN), and the North Atlantic Treaty Organization (NATO) base their governing conventions and rules of conduct on states as representative of their peoples' interests. Since the Treaty of Westphalia in 1648, humans have related to foreign populations primarily through their central governments. Cyberspace and globalization have enabled direct interaction of disparate populations across the globe with an overall decreasing relevance of central governments. Where the interaction is clearly state-to-state, though, a substantial body of legal and ethical norms comfortably exists to provide a modicum of clarity for acceptable interstate behavior.

In contrast to the relative clarity of action and reaction provided by state-to-state competition and conflict, the empowerment cyberspace provides to individuals and group non-state actors makes their ability to significantly influence entire states

disproportionate to the size of their populations. It also creates ambiguity for selection of the most effective response option for the United States. For example, it is unimaginable that the United States would launch a military capture or kill operation against a “recreational” hacker who probed a DOD network. However, the United States did undertake kinetic operations to kill Anwar al-Awlaki who used the internet as a means to propagate violent jihadist ideology that inspired Umar Farouk Abdulmutallab, the so-called ‘underwear bomber’.[39] The strike on Anwar al-Awlaki, even though the United States declared him an unlawful combatant for his affiliation with Al Qaeda in the Arabian Peninsula (AQAP), has met with domestic and international outrage directed at the legitimacy of the United States’ declaration.[40] This will likely remain a murky legal issue as the international community wrestles with the evolving ethical norms of states’ application of force on super-empowered non-state actors who can generate and wield influence through cyberspace at a level that previously only states possessed.

As the composition of the cyberspace non-state actor increases from transient opportunity-based groups to specifically structured organizations, the associated response by the United States to cyber-attacks from these groups must also become more sophisticated. As the previously mentioned individual ‘recreational’ hackers coalesce under a unifying ideology, increased United States awareness and integration of defensive and response measures is necessary to account for the generally greater influence larger groups can wield. Representative of this class of non-state actors is groups such as the ‘hacktivist’ collective Anonymous and criminal organizations.

The United States response to groups’ malicious cyber activity will likely remain within the realm of financial pressure and law enforcement, although a diplomatic

element may also come into play if the presence of adverse non-state groups within another country is pervasive. A large quantity of cyber-attacks on United States government and private institutions comes from China[41] and though many of these attacks are not directly attributable to the Chinese government, they still influence Chinese-United States diplomatic relations.

The distinction between a group and an organization is a function of increasing organizational structure, size, and increasing sophistication of the organization's interests. These organizations can be wholly legitimate private or state-sponsored commercial businesses or sophisticated terrorist and transnational criminal organizations that utilize cyberspace to not only conduct their primary objective of terror or illegal activities but also to run the business aspects that allow their organizations to sustain themselves. This collection of non-state actors also contains an interesting development: cyber-mercenaries.

Due to either a lack of technical capability or a fear of attribution and reprisal, state competitors and hostile non-state actors may be deterred from directly challenging the United States through cyberspace. However, they may still seek the asymmetric advantage that cyberspace can generate to counter the United States conventional economic and military dominance. This has created a new cyber mercenaries market for technically adept individuals or groups willing to risk powerful states' response to malicious cyber activity for the right price.[42]

The most important take-away from Figure 2 is the application of United States instruments of power across the range of actors in cyberspace is not homogenous. Specific authorities within United States' law determine which department or agency has

responsibility and will respond to each of the different types of actors that may threaten the United States in cyberspace. If the United States' overall strategy does not seamlessly blend the transitions of authority across the responsible departments and agencies, our intelligent adversaries will find and exploit these seams to gain and maintain decision-superiority in and through cyberspace.

Criticality

The variable of criticality examines the value to the victim of what a cyber-attack

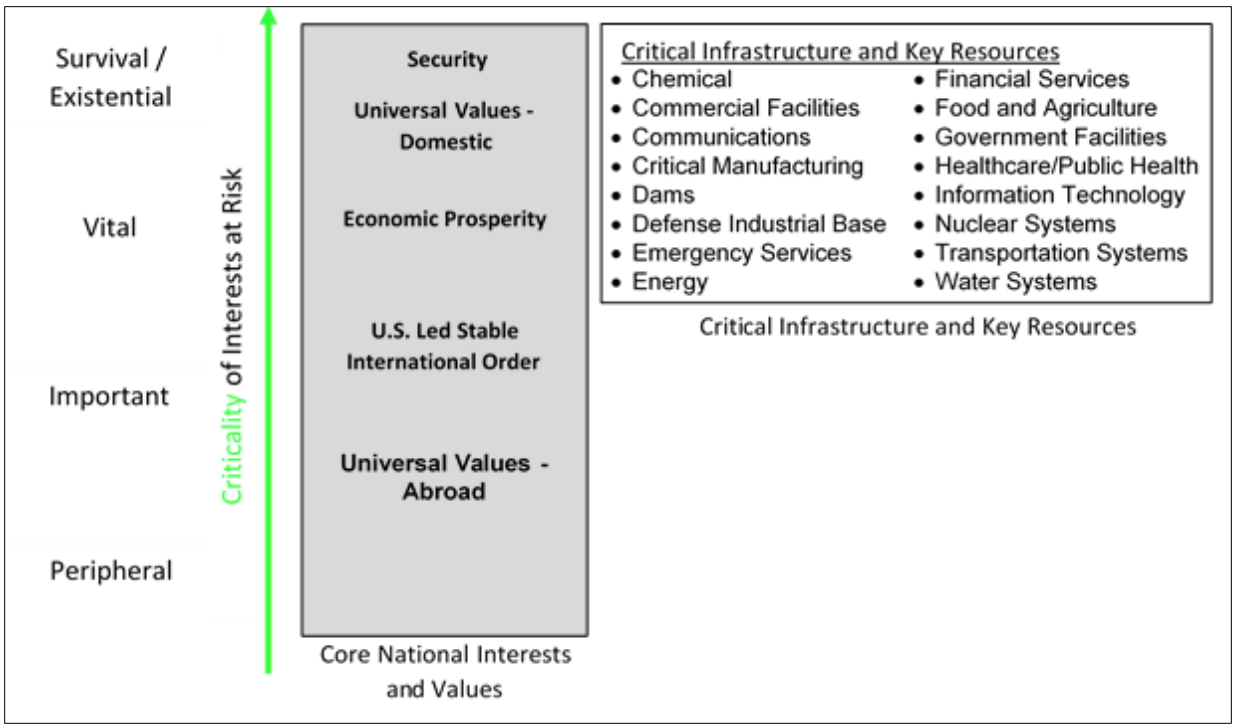

Figure 3 - Criticality: Value of the Target

is targeting. Using the ranking of interests as peripheral, important, vital, and survival[43] in ascending order of value, Figure 3 plots the United States core interests[44] to provide the policy-maker or strategic planner a measure of criticality for a cyber-attack's target. Additionally, United States' critical infrastructure and key resources as identified in Presidential Policy Directive-21 (PPD-21) are also depicted as a vital or survival

interests. Determining whether protection of a particular element of critical infrastructure or resource is a survival or vital interest is situational-dependent. Undoubtedly, though, preservation of energy (electrical) and communications are most critical, as these elements are enablers for the proper functioning of all the other critical infrastructure and resource elements.

Severity

This axis of the model relies on the previously defined 'armed attack' definition to define the high end of the spectrum. Severity below the 'armed attack' threshold is

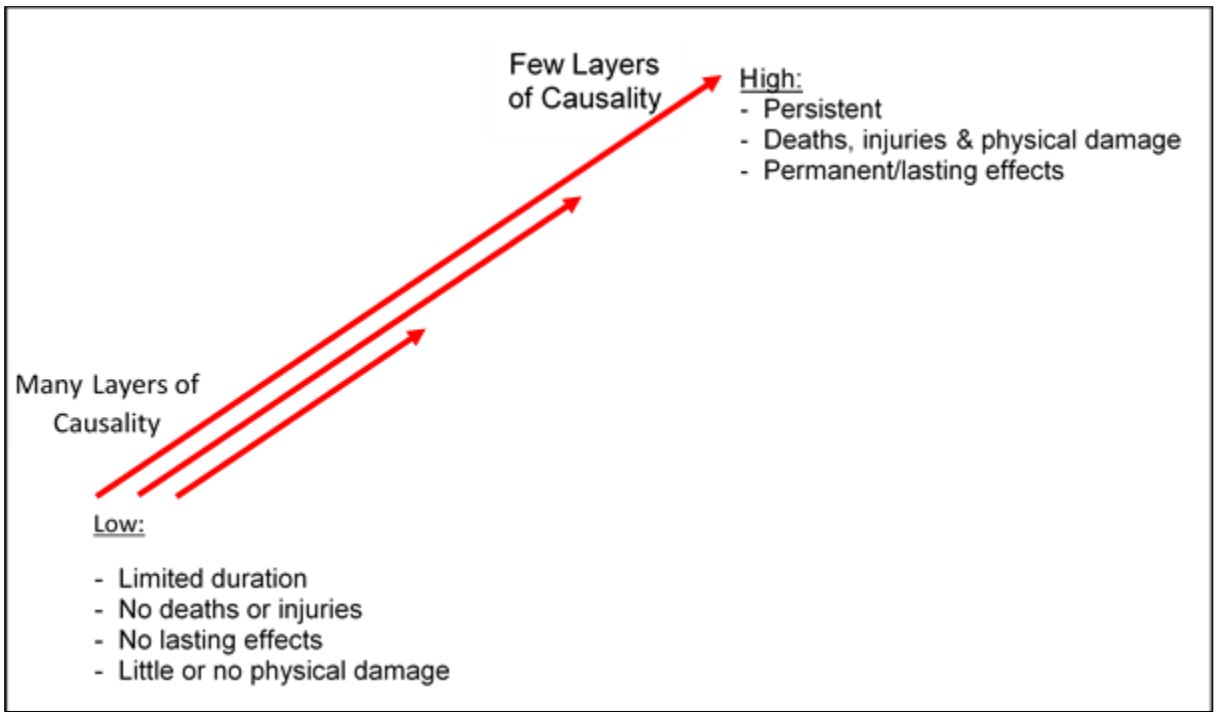

Figure 4 - Severity and Causality

based on the range of cyber-attack actions discussed in the Cyber Offense section. The low end begins with non-destructive probes and increases in severity through the Deny levels depicted in Table 1. It also acknowledges the affect layers of causality have on severity determination.

Although causality could arguably be considered part of attribution, this portion of the model assumes above the attribution threshold sufficient attacker identification has occurred. However, the layers of causality must still be accounted for when determining severity. Although the ultimate severity of an attack could be high, if too many intervening layers of causality separate the ultimate effect with the immediate effect, the cumulative result is a perception of lower severity. Low severity attacks cause little degradation for short periods and no injuries while high severity attacks cause complete degradation for long or indefinite periods of time or cause significant injuries and/or deaths.

Integrated Model

From the preceding discussion, it should be apparent that not all malicious cyber activity is a cyber-attack and that the United States government cannot conceivably respond to all malicious cyberspace activity. The difficulty of attaining an actionable attribution threshold compounded by the complexity of exercising responsibility for the differing types of actors and targets, and accounting for the severity of the damage to the target makes conceptualizing the appropriate response to a cyber-attack difficult. This section will provide the strategic leader a conceptual model that depicts the realistic capabilities and authorities for a United States response to a cyber-attack. Figure 5 graphically portrays a refinement of the Figure 1 model that depicted a base of cybersecurity/defense with a generic post-attribution response layer.

The integrated model is cognizant of the difficulties of attribution and the resource limits that make trying to defend and respond to everything, all the time an unrealistic goal. Instead, it depicts the United States government's appropriate response to a cyber-attack being driven by the questions: "What was attacked?"; "How bad was it

hurt?" and then "Who did it?" This conceptual model will also familiarize the strategic

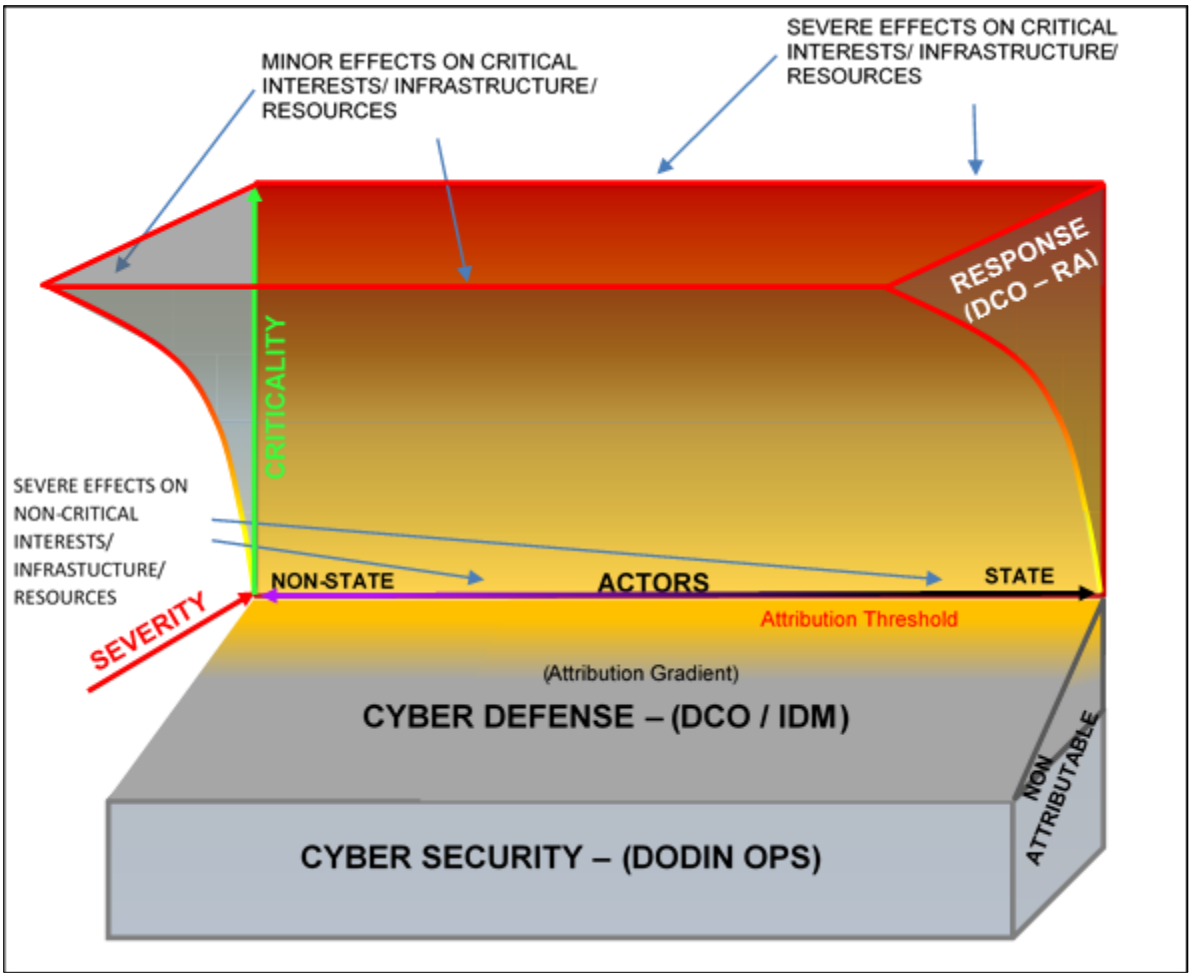

Figure 5 - Integrated Cyber Security / Defense / Response Model

military leader with the Department of Defense's doctrinal elements of defensive cyberspace operations: Information Network Operation (cyber-security), Internal Defensive Measures (cyber-defense), and Response Actions.

Knowing the cost and difficulty of attribution, a non-severe attack on a non-critical interest or resource may not be worth any United States government action other than just reviewing and reinforcing cybersecurity measures. This basic responsibility applies to all United States government departments and agencies. Likewise, the civilian sector should also seek this basic level of security, especially those elements designated as

critical infrastructure or resources. In the Defense Department, this foundation of basic cybersecurity is called DOD Information Network Operations (DODIN-OPS) and has responsibility to “design, build, configure, secure, operate, maintain, and sustain DOD networks”.[45]

As the criticality of the target increases, the United States’ defensive measure will increase as well. Threats to critical interests or infrastructure must be countered regardless of whether the United States has achieved response-quality attribution because they demonstrate an adversary’s capability and intent, and the existence of an exploitable vulnerability. This next layer of cyberspace defense consists of aggressive ‘patrolling’ of critical friendly networks to determine the presence of vulnerabilities or exploitation previously undetected by cybersecurity measures. The DOD calls this active defense posture Defensive Cyberspace Operations – Internal Defensive Measures (DCO-IDM).[46]

Upon achieving an actionable threshold of attribution, response options become available to cyber-defenders. With proper authorization, they are no longer restricted to only reactive, defensive actions and can go outside of ‘blue’ (friendly) cyberspace to conduct cyber counter-attacks to stop the effects of an attack and deter future attacks. Even with attribution achieved, higher-order effects such as intelligence or technical gain/loss, legality, and the sheer number of cyber-attacks makes active response to each of them difficult. Figure 5 portrays the United States government’s active response to cyber-attacks will likely only occur when critical interests or infrastructure are threatened or if the cumulative effects of widespread severe damage on non-critical interests or infrastructure would create overall debilitating effects. The DOD calls these

active responsive measures, undertaken by National Mission Teams at U.S. Cyber Command or regional Cyber Mission Teams at the geographic combatant commands, Defensive Cyberspace Operations-Response Actions (DCO-RA).[47]

There are two critical inhibitors to response options for the United States, though. The first is current policy restricts United States government departments or agencies from conducting cyber-attacks as either a DCO-RA or as part of an Offensive Cyberspace Operation (OCO) without first gaining presidential authorization (or in extremis, Secretary of Defense approval). The limitation is not significantly inhibiting for integrating offensive cyberspace operations with other military or interagency capabilities in deliberate operational or contingency plan development. However, this extremely centralized authorization requirement might limit effectiveness in time sensitive response windows associated with DCO-RA or crisis response unless a preplanned response requirement was foreseen and previously authorized.

The second limitation, at least from the U.S. Department of Defense perspective, is if attribution identifies the attacker as a non-state actor, authority to respond to the attack will likely reside in one of the other U.S. government departments. Since most cyber-attacks are classified as criminal activities instead of hostile acts, unless the severity of the attack and the criticality of the targets prompts an “unlawful combatant”/”unprivileged enemy belligerent” determination, the responsible department for direct response is likely the Department of Justice. Otherwise, response to the attack will shift to the Department of State for diplomatic negotiations with the country in which the non-state actor is residing to halt and prevent future attacks.

Conclusion

As the first widely recognized employment of a cyber-to-physical sabotage weapon, Stuxnet demonstrated, “Digital weapons work. And different from their analog counterparts, they don't put military forces in harm's way, they produce less collateral damage, (and) they can be deployed stealthily”.[48] The stability of a bipolar Cold War world order has shattered into a multipolar array of state and non-state actors empowered by the evolution of cyberspace. The nature of cyberspace operations with the inherent fog and friction created by the ease of access, speed and scale of attacks, and difficulty in attributing the source across the array of state and non-state actors, means there is no one-size fits all deterrence theory.

The commonly touted comparison of malicious cyber activities to a weapon of mass destruction with an associated deterrence theory like nuclear deterrence is flawed. Unlike nuclear weapons, widespread use of cyberspace espionage and weapons is already occurring; the genie is already out of the bottle and is never going back in. Strategic leaders must instead gain greater awareness of cyberspace and how it affects our national security. This understanding is necessary in order to develop credible strategies for assuring friendly access to the contested cyberspace domain while deterring (and when necessary defeating) adversaries who seek to exploit it to do us harm.

Although executing offensive and response cyberspace operations is the responsibility of Cyber Command, the National Security Agency, and other government agencies with specialists trained and authorized to conduct cyber-attacks, we must all actively contribute to our national infrastructure and military cyberspace defenses. As strategic leaders, we will be responsible for shaping the cultures, attitudes, and

awareness of the organizations we lead. Additionally, those involved in planning effects-generation across all domains at the national level and within the geographic and functional combatant commands must have an understanding of cyberspace to integrate correctly its full-spectrum capabilities and limitations in operational and contingency plans development.

No longer, can we afford to treat cyberspace integration as an afterthought; our enemies and potential adversaries do not. Unlike preparing to fight in the physical domains where the location of our enemies is discernible and 'over there', cyberspace is all around us. In pre-deployment training, units go to the National Training Center (NTC) or Integrated Training Exercises (ITX) to sharpen their skills prior to facing the enemy in the physical domains. In cyberspace the location of the enemy is here, in our homes, at our home stations and bases, and confronting our forces overseas. There is no pre-deployment NTC or ITX equivalent to train for cyber-enabled conflict before we confront the enemy. We are in the fight every day. The first critical step to winning this fight is the education of our leaders to the reality of the threat so they may plan, train, and instill an organizational culture of cyber-awareness.

Endnotes

[1] *Moore's Law Homepage*, http://www.mooreslaw.org/ (accessed March 29, 2014).

[2] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: U.S. Department of Defense, July 2011), 2.

[3] Ibid., 1.

[4] Ibid.

[5] Internet World Stats "Usage and Population Statistics," http://www.internetworldstats.com/stats.htm (accessed March 24, 2014).

[6] Ibid.

[7] Ibid.

[8] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, 3.

[9] Adrienne Burke, "Why Microsoft's Craig Mundie Worries about Weapons of Mass Disruption," *Forbes*, November 15, 2013, http://www.forbes.com/sites/techonomy/2013/11/15/why-microsofts-craig-mundie-worries-about-weapons-of-mass-disruption/ (accessed March 18, 2014).

[10] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, 3.

[11] Dune Lawrence, "The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built," *Bloomberg Businessweek*, January 23, 2014, http://www.businessweek.com/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency (accessed March 2, 2014).

[12] Ibid.

[13] Tor, "Tor: Overview" https://www.torproject.org/about/overview.html.en (accessed March 2, 2014).

[14] Dune Lawrence, "The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built," *Bloomberg Businessweek*, January 23, 2014, http://www.businessweek.com/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency (accessed March 2, 2014).

[15] James Eng, "Silk Road Pledges to Pay Back Users After $2.6 Million Bitcoin Hack," *NBC News*, February 17, 2014, http://www.nbcnews.com/tech/security/silk-road-pledges-pay-back-users-after-2-6-million-n32341 (accessed March 2, 2014).

[16] John Koetsier, "TorSearch Launches to be the Google of the Hidden Internet," *VentureBeat News*, October 10, 2013, http://venturebeat.com/2013/10/10/torsearch-launches-to-be-the-google-of-the-hidden-internet/ (accessed March 2, 2014).

[17] Michael Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare (Draft)* (New York: Cambridge University Press, 2013), 49.

[18] Harold Koh, "International Law in Cyberspace," September 18, 2012, linked from *U.S. Department of State Home Page* at "Remarks," http://www.state.gov/s/l/releases/remarks/197924.htm (accessed March 1, 2014).

[19] United Nations Charter, art. 2, sec. 4.

[20] Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare (Draft)*, 55.

[21] United Nations Charter, art. 51.

[22] Directv, "Get Rid of Cable Commercials - Direct Tv," linked from Youtube, http://www.youtube.com/watch?v=xHs8OlXBFVs (accessed March 2, 2014).

[23] Richard DiMeglio et al., *Law of Armed Conflict Deskbook* (Charlottesville, VA: The Judge Advocate General's Legal Center and School, U.S. Army, 2012), 97.

[24] Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare (Draft)*, 87-88.

[25] J. David Singer, "Threat-Perception and the Armament-Tension Dilemma," *The Journal of Conflict* 2, no. 1 (March 1958): 94.

[26] Michael Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard International Law Journal* 54 (published online: December 2012) 24.

[27] Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy*, November 19, 2013, http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack (accessed April 5, 2014);

William Broad, John Markoff, and David Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay" *The New York Times Online*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0 (accessed April 05, 2014).

[28] Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed", 23.

[29] United Nations Charter, art. 51.

[30] U.S. Department of Defense, *Cyberspace Operations*, Joint Publication 3-12 (Washington, DC: U.S. Department of Defense, February 5, 2013), II-6.

[31] Peter Singer and Allan Friedman, *Cybersecurity and Cyberwar* (New York: Oxford University Press, 2014) 38-39.

[32] Dennis Blair et al., *The Report of the Commission on the Theft of American Intellectual Property* (Seattle, WA: The National Bureau of Asian Research, May 2013), 2.

[33] Ryan Neal, "US Navy Needed Four Months and $10 Million To Clear Iranian Hackers From Marine Corps Network," *International Business Times*, February 8, 2014, http://www.ibtimes.com/us-navy-needed-four-months-10-million-clear-iranian-hackers-marine-corps-network-1556377 (accessed March 19, 2014).

[34] Symantec Webpage, "Vulnerability Trends" http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=zero_day_vulnerabilities (accessed April 7, 2014).

[35] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, 7.

[36] William J. Lynn III, "Defending a New Domain, The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010): 103.

[37] Barack Obama, *Presidential Policy Directive-21 Critical Infrastructure Security and Resilience* (Washington, DC: The White House, February 12, 2013), 1.

[38] Ibid., 10-11.

[39] Pete Yost, "Judge Dismisses Lawsuit Over Drone Strikes in Yemen that Killed American Anwar al-Awlaki," *The Washington Post Online*, April 4, 2014, http://www.washingtonpost.com/world/national-security/judge-dismisses-lawsuit-over-drone-strikes-in-yemen-that-killed-american-anwar-al-awlaki/2014/04/04/3dca8ee4-bc4c-11e3-9a05-c739f29ccb08_story.html (accessed April 5, 2014); Office of Public Affairs, "Umar Farouk Abdulmutallab Sentenced to Life in Prison for Attempted Bombing of Flight 253 on Christmas Day 2009," February 16, 2012, linked from U.S. *Department of Justice Home Page* at "Justice News," http://www.justice.gov/opa/pr/2012/February/12-ag-227.html (accessed April 5, 2015).

[40] Mark Mazzetti, Charlie Savage, and Scott Shane, "How a U.S. Citizen Came to Be in America's Cross Hairs," *The New York Times Online*, March 9, 2013, http://www.nytimes.com/2013/03/10/world/middleeast/anwar-al-awlaki-a-us-citizen-in-americas-cross-hairs.html?pagewanted=all&_r=0 (accessed March 30, 2014).

[41] Arthur Herman, "Edward Snowden Enables Chinese Hack Attacks," *New York Post Online,* February 24, 2014, http://nypost.com/2014/02/24/chinas-military-hackers-can-thank-edward-snowden/ (accessed March 30, 2014).

[42] Zachary Fryer-Biggs, "New Cyber 'Mercenaries' Prefer Quick Strikes, Researchers Say," *Defense News*, September 27, 2013, http://www.defensenews.com/article/20130927/DEFREG02/309270009/New-Cyber-Mercenaries-Prefer-Quick-Strikes-Researchers-Say (accessed April 8, 2014).

[43] Alan G. Stolberg, "Crafting National Interest in the 21st Century, (Chapter 2)," in *U.S. Army War College Guide to National Security Issues, Volume II: National Security Policy and Strategy* (Carlisle Barracks, PA: U.S. Army War College, 2012), 19.

[44] Barack Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 7.

[45] U.S. Department of Defense, *Cyberspace Operations*, Appendix A.

[46] Ibid.

[47] Ibid.

[48] Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy*, November 19, 2013, http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack (accessed April 5, 2014).