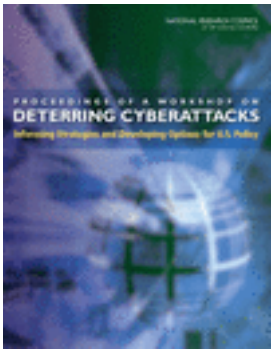

Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy

Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council

ISBN: 0-309-16086-3, 400 pages, 8 1/2 x 11, (2010)

Categorizing and Understanding Offensive Cyber Capabilities and Their Use

Gregory Rattray
Internet Corporation for Assigned Names and Numbers

Jason Healey
Delta Risk

OVERVIEW

This paper provides a framework for categorizing the offensive cyber capabilities across a range of potential scenarios to help further the dialogue on cyber deterrence and conflict management. Though not an in-depth analysis of the subject, this paper does include suggestions where further analysis might prove useful. Beginning with key features of the aspects of cyberspace that are most applicable for the offense, the paper outlines several key ways to categorize offensive operations. Attacks, for example, could be in support of existing kinetic operations and used in conjunction with other capabilities; however offensive capabilities could also be used as part of standalone engagements, operations and entire cyber campaigns.

Though many have posited notions on what a "real" cyber war would be like, we lack understanding of how such conflicts will be conducted and evolve. Accordingly, the third main section dives into an analysis of cyber war analogies, from the well-known "cyber Pearl Harbor" and "cyber 9/11" to less discussed analogies like a "cyber Vietnam." As cyber warfare is often compared to combat in the air, both in speed and range of operations and the loudly touted strategic effects, the paper also includes an extended case study on a cyber Battle of Britain fought force-on-force in cyberspace with little relation to fielded military forces.

For the purposes of this paper, offensive operations are those analogous to Computer Network Attacks (CNA), as defined by the Department of Defense,[1] and do not include acts of cyber espionage, or Computer Network Exploitation.[2] Though both types of operations may use similar technical techniques to access an adversary's networks, cyber exploitation is generally more akin to espionage than offensive operations. This paper's focus is therefore on Computer Network Attacks, whether operations between political actors operating across state boundaries or by non-state actors for political purposes.

[1]Joint Publication 1-02 (JP 1-02): Dictionary of Military and Associated Terms. Department of Defense. Washington, D.C., October 2009, available online at: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, accessed on March 1, 2010.

[2]Department of Defense Dictionary of Military and Associated Terms. Joint Publication 1-02, (JP 1-02), Department of Defense. Washington, D.C., October 2009, available online at: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, accessed on March 1, 2010.

CYBERSPACE AS A WARFIGHTING DOMAIN

From the birth of powered aviation in 1903, it was only fifteen years to the World War One battle of St. Mihiel, which involved the first mass operation of airpower during wartime. We are now rapidly approaching the 30th anniversary of the Internet and yet we have not yet had large-scale, coordinated military operations conducted to control cyberspace. As noted by the United States Air Force in the mid-1990s:

> Before the Wright brothers, air, while it obviously existed, was not a realm suitable for practical, widespread, military operations. Similarly, information existed before the Information Age, but the Information Age changed the information realm's characteristics so that widespread operations became practical.[3]

Just as aerodynamics drive military operations in the air, so do the physical and logical laws of cyberspace define military operations in that domain. Recognizing that understanding of cyberspace has changed, the *National Military Strategy for Cyber Operations* has put forth a military strategic framework that orients and focuses the actions of the Department of Defense in areas of intelligence, military and business operations in and through cyberspace. It defines cyberspace as "a domain characterized by the use of electronics and the use of the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures."[4] Though cyberspace is fairly well understood as a warfighting domain there are a few key aspects that help us to better examine the role of offensive operations. Cyberspace is

1. Logical but physical;
2. Usually used, owned, and controlled predominantly by the private sector;
3. Tactically fast but operationally slow;
4. A domain in which the offense generally dominates the defense; and
5. Fraught with uncertainty.

Logical but physical. Though a warfighting domain, cyberspace has some striking differences from the other domains. "Unlike the land, sea, air and space where the laws of physics do not change, cyberspace is a man-made creation that continually changes and evolves."[5] However, it is not infinitely mutable. Cyberspace is physical because the information that transits through it is grounded in the physical infrastructure that creates and stores it and the physical infrastructure that gave rise to the domain is generally housed within states' borders. Cyberspace is also logical, as the information that transits through it, goes through on agreed-upon routing protocols. Certain logical aspects of cyberspace such as the functioning of open source code have no clear ownership, geographic basis or locus of responsibility. As described by Lawrence Lessig, cyberspace is governed by "laws of code" which are man-made and designed to achieve a wide variety of purposes.[6] This emergent synthesis of physical and logical attributes means that offensive operations can cross borders at great speed but with affects that are more likely to be reversible than other kinds of military attacks, as they often don't have actual physical impacts, such as destroying equipment or causing casualties.

This logical-physical disconnect is one of the reasons why cyber attacks thus far have tended to have effects that are either (1) widespread but limited in duration or (2) persistent but narrowly focused. Few attacks, if any, have so far been *both* widespread and persistent. We do note that the possibility of cyber attacks which cause physical destruction of equipment and cause events in physical space that

[3]Department of the Air Force. Cornerstones of Information Warfare, Department of Defense. Washington DC, 1995, available at http://www.iwar.org.uk/iwar/resources/usaf/iw/corner.html, accessed on March 1, 2010.

[4]Chairman of the Joint Chiefs of Staff. National Military Strategy for Cyber Operations. Department of Defense, December 2006, available at http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf, accessed on March 2, 2010.

[5]"Defending IT: Words from the New Military Cyber Commander." Gov Info Security, June 24, 2009, available at http://www.govinfosecurity.com/articles.php?art_id=1575, accessed April 10, 2010.

[6]Lessig, Lawrence. 1999. Code and Other Laws of Cyberspace. New York, NY: Basic Books.

result in deaths and possibly mass casualties does exist. So far, the known occurrences of such attacks have been highly limited.

Because of the current state of the logical and physical laws which govern cyberspace, attribution of particular attacks may be difficult, though it needn't rule out determining a particular nation responsible regardless of the technical attribution. Additionally, as the laws of code, technology and obligations of operators of cyberspace evolve, progress may well occur improving the attribution of attacks occurring within or from cyberspace.

Usually used, owned, and controlled predominantly by the private sector. Future conflicts in cyberspace are very likely to be won or lost in the private sector, which runs, owns, and depends on the underlying networks and information, at least in the most advanced economies. America does not primarily depend on cyberspace to support the U.S. military—it is one of the underlying engines of our economic advantages and productivity as well as a key way to export our culture of freedoms. Offensive operations undertaken by the U.S. military must consider that we could have much more to lose than to gain.

Similarly, when military planners consider conflicts in cyberspace, they often use metaphors from their own military service which may serve them poorly in the privately owned cyberspace. Consider aerial warfare: there is a lot of sky out there and very few aircraft, especially in a warzone. Pilots can "slip the surly bonds of earth,"[7] confident they will have little interaction with civilians and, if they do, the Air Forces will be in control. Nothing could be more different in offensive cyber operations. As soon as a military mission is "wheels up" from the base, it is likely to be transiting in some measure through a system owned, controlled, and used, by the private sector including in transit across global commons between international borders in undersea cables or through satellites. The targets of our offensive operations could include private sector targets and the attacks of our adversaries are even more likely to do so, hoping for asymmetric attacks against poorly defended targets.

Tactically fast but operationally slow. Cyberspace, where the computer is the battlefield, is widely considered to be an operational environment through which an attacker can strike with minimal investment while yielding potentially large-scale effects with great speed. While it is true that individual attacks can happen quickly—"approaching the speed of light" we are often assured[8]—the planning cycle for each attack to achieve a specific military effect is likely to be far longer than that. Cyberattack planning may take more time and effort than use of conventional forces due to the complexity of the environment and the targeted systems. Moreover, even well planned military attacks can have very transient effects. In past conflicts, to have a persistent strategic impact, an adversary needed to apply continuous pressure, to re-attack as the defenders repair damage, substitute for the disrupted goods or services, and re-establish themselves. There is little reason in this regard to believe that conflict in cyberspace will be different. The implication is that cyber wars, rather than consisting of a single, sharp attack, may instead be a long serious of tactical engagements, as part of larger operations, or as part of a larger campaign.

Fraught with uncertainty. Cyberspace is an extremely complex environment, characterized by rapid change and adaption, whose direction is difficult to predict. Though present in conventional warfare, uncertainty of effects is especially prevalent, and is often the dominant state, in conflict in cyberspace. This uncertainty stems from a variety of sources, as has been discussed in detail in the National Research Council report *Technology, Policy, Law, and Ethics Regarding the U.S. Acquisition and Use of Cyberattack Capabilities*.[9] In short, not only is there great uncertainty due to the normal fog and friction of military operations, but cyberspace also has particular challenges: rapid changes in the domain,

[7]Gillespie, Magee Jr. High Flight. Great Aviation Quotes, available at http://www.skygod.com/quotes/highflight.html, accessed on July 27, 2010.

[8]As is expressed on page 3 of: Chairman of the Joint Chiefs of Staff. National Military Strategy for Cyber Operations. Department of Defense, December 2006, available at: http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf, accessed on March 2, 2010.

[9]National Research Council. 2009. Technology, Policy, Law, and Ethics Regarding the U.S. Acquisition and Use of Cyberattack Capabilities. Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds. Washington, D.C.: National Academies Press.

insufficient knowledge of targets and dynamics, and uncertainty of cascading effects. This uncertainty imposes great demands on a military commander looking to use offensive cyber operations in a strictly controlled manner, as with any other application of force. The needs for intelligence support, target preparation, understanding of second and third order effects, and political and legal wavering make that commander's choice to rely on offensive cyber operations not as straightforward as it may seem at first. The challenges have been addressed in depth in *Strategic Warfare in Cyberspace*[10] as well as numerous studies conducted by the Department of Defense.

Ultimately, the inability to thoroughly plan and predict in cyberspace makes it difficult to achieve specific objectives through offensive cyber operations and seems to be one of the main brakes on more operational use of offensive operations.[11]

CATEGORIZING OFFENSIVE MISSIONS

Many previous attempts to categorize offensive cyber capabilities have focused understandably on what is new in the cyber domain. For example, cyber capabilities have often been categorized technically, such as the previous National Academy of Sciences paper[12] which looked at techniques for remote access (such as botnets, penetrations, worms and viruses, and protocol compromises) and close access (like compromising the supply chain or patch process). The United States Air Force was perhaps the first military organization to officially translate these technical categories into military operational terms.

In 1995, the Secretary and Chief of Staff of the Air Force signed out an official White Paper called *Cornerstones of Information Warfare*[13] which started the process of integrating cyber effects into defined military operations by listing "information attack" alongside physical attack and defining it as "directly corrupting information without visibly changing the physical entity within which it resides." This went several steps further in 1998 with new Air Force doctrine[14] which codified new missions of information warfare (that is, not just cyber) in parallel with those of more typical aerial warfare:

> Offensive counterinformation (OCI) includes actions taken to control the information environment. OCI operations are designed to limit, degrade, disrupt, or destroy adversary information capabilities . . .
>
> Defensive counterinformation (DCI) includes those actions that protect information, information systems, and information operations from any potential adversary.

This new Air Force doctrine made several key points on this new construct, including noting that "while the analogy is not perfect, there are strong parallels and airmen can apply many of the hard-won precepts of OCA-DCA to OCI-DCI." This statement helped tie what might be new in the cyber domain to the institutional lessons the Air Force had learned in its first fifty years.

Just as relevant to modern cyber operations, the Air Force was presciently highlighting that "the dividing line between [the offense and defensive missions of OCI and DCI] can be exceedingly thin and the transition nearly instantaneous." This rapid transition between defense and offense underlies the current direction of cyber conflict in the United States military with its increasing focus on "response actions" or "dynamic defense" to use more muscular methods to stop attacks.

---

[10]Rattray, Gregory J. 2001 Strategic Warfare in Cyberspace. Cambridge MA: MIT Press.

[11]For example, see Markoff, John, and Thom Shanker. Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk. *New York Times* online, available at http://www.nytimes.com/2009/08/02/us/politics/02cyber.html, accessed on 26 July 2010. Also see Nakashima, Ellen. Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Cyberwar Policies. *Washington Post* online, available at http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464.html.

[12]National Research Council. 2009. Technology, Policy, Law, and Ethics Regarding the U.S. Acquisition and Use of Cyberattack Capabilities. Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds. Washington, D.C.: National Academies Press.

[13]Department of the Air Force. *Cornerstones of Information Warfare*, Department of Defense, Washington DC, 1995, available at http://www.iwar.org.uk/iwar/resources/usaf/iw/corner.html, accessed on March 1, 2010.

[14]Department of the Air Force. Air Force Doctrine Document 2-5*:* Information Operations (AFDD 2-5). Department of Defense, Washington, D.C., 1998, available at http://www.dtic.mil/doctrine/jel/service_pubs/afd2_5.pdf, accessed April 3, 2010.

These terms of OCI and DCI were not widely used (and have been since dropped[15]), soon displaced after by new terms approved in 1998[16] by the Chairman of the Joint Chiefs of Staff, and therefore applicable to all the military services. These terms remain in very common use and are still official joint doctrine[17]: Computer Network Attack (CNA), Exploitation (CNE) and Defense (CND).

Though these concepts brought needed doctrinal stability for over a decade, they did not have the same institutional parallels of offensive and defensive counterinformation. They categorized but they did not resonate, cutting off further deep thinking into how military operations in cyber conflict may differ or be similar to traditional missions and doctrines. The following is an illustrative list[18] of how such borrowed, customized doctrinal terms might help categorize military cyber missions (in each case, the definitions are from official Joint doctrine[19] with additions in italics):

- **Counter *cyber*[20]:** A mission that integrates offensive and defensive operations to attain and maintain a desired degree of *cyber* superiority.
- ***Cyber* interdiction:** An action to divert, disrupt, delay, or destroy the enemy's military cyber ~~surface~~ capability before it can be used effectively against friendly forces, or to otherwise achieve objectives.[21]
- **Close *cyber* support:** *Cyber* action against hostile targets' *information systems* that are in close proximity to friendly forces and that require detailed integration of each *cyber* mission with the fire and movement of those forces.
- ***Cyber* reconnaissance in force:** An offensive *cyber* operation *conducted by military (not intelligence) forces* designed to discover and/or test the enemy's strength or to obtain other information.
- **Suppression of enemy *cyber* defenses:** Activity that neutralizes, destroys, or temporarily degrades enemy *cyber* defenses by destructive and/or disruptive means.
- **Strategic *cyber* mission:** A mission directed against one or more of a selected series of enemy *cyber* targets with the purpose of progressive destruction and disintegration of the enemy's warmaking capacity and will to make war.

CATEGORIZING OFFENSIVE OPERATIONS

Offensive cyber operations (as distinct from their missions, above) can be categorized according to a number of factors. This list is neither mutually exclusive nor collectively exhaustive—indeed some even overlap or imply one another. Instead, these have been chosen as they seem to shed the most light in distinguishing between different kinds of offensive operations and ways that a cyber war might be fought, as analyzed in later sections of this paper. These key factors are summarized in the list below and briefly described after that:

[15]Department of the Air Force. Air Force Doctrine Document 2-5: Information Operations (AFDD 2-5). Department of Defense, Washington, D.C., 1998, available at http://www.dtic.mil/doctrine/jel/service_pubs/afd2_5.pdf, accessed April 3, 2010.

[16]Joint Publication 3-13, Joint Doctrine for Information Operations. Department of Defense, Washington, D.C., 1998, available at http://hqinet001.hqmc.usmc.mil/pp&o/PLN/Files/Op%20Planning%20Policies%20Procedures/Planning%20Process%20Dev/JP%203-13%20Joint%20Doctrine%20for%20Info%20Operations.pdf, accessed on March 7, 2010.

[17]Joint Publication 3-13, Joint Doctrine for Information Operations. Department of Defense. Washington, D.C., 2006, available at http://www.fas.org/irp/doddir/dod/jp3_13.pdf, accessed March 7, 2010.

[18]The authors are encouraged by the understanding that such an effort is currently underway within the Joint Staff, though any results will be published after this paper.

[19]Joint Publication 1-02 (JP 1-02): Dictionary of Military and Associated Terms. Department of Defense. Washington, D.C., October 2009, available online at: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, accessed on March 1, 2010.

[20]Please note, the crossed out text represents the word taken out and are not an editorial artifact.

[21]The Air Force, in *Cornerstones*, used this term back in 1995 explaining that "One approach to interdiction is wrecking bridge spans using laser-guided bombs. Alternatively, we might be able to alter the adversary's planners' information, falsely categorizing the bridges as destroyed, causing [them] to reroute forces and supplies."

Nature of Adversaries	Openness
Nature of Targets	Context
Target Physicality	Campaign Use
Integrated with Kinetic	Initiation Responsibility and Rationale
Scope of Effect	Initial Timing
Intended Duration	Initiation Attack

Nature of adversaries. Are the offensive operations being carried out by nation states on one side, both, or neither? If one or both adversaries are non-state groups, is there national encouragement or backing for one or both?[22] The nature of states' relationships with surrogate groups conducting offensive cyber operations has become one of the most significant and challenging aspects of understanding who is conducting offensive cyber operations. As a result, establishing effective deterrent and conflict management strategies in this environment remains challenging.

Nature of targets. Is the offensive operation against a military target, civilian target, or a dual-use target somewhere in between? This classification overlaps significantly with the nature of adversaries (above) when the offensive operation is a single attack—especially if it has tactical and short-term effects. For example, if an attack is looking to shut down power to a particular part of rail switching yard, then the target is civilian and the defender is the operator of that electrical system. However, if the offensive operations are part of a larger campaign (see below), especially if they are conducted over time, then it is likely that the adversaries are the nation states themselves. Even if particular targets may be operated by the private sector, nation-state governments may bear responsibilities for defending the targeted systems and enterprises.

Target physicality. Is the attack targeting the logical (e.g., disrupt a software service), the cognitive (convince or disrupt an adversary using false information), or the physical (breaking a generator)? Attacks with real physical effects are rare but they do exist[23] and they are likely to be far less reversible than other attacks with logical or cognitive effects. We can change our minds quickly, but new generators need to be ordered, built, delivered, and installed. We know little about the duration or impact of possible data corruption attacks but such attacks are certainly technically possible and hold significant disruptive potential.

Integrated with kinetic. Is the attack intended to be integrated or simply coincident with kinetic attacks? This could include either military attack legally conducted by a nation state or attacks by a terrorist, or other non-state, group seeking to combine cyber and physical attacks to cause more damage and panic or grab more media attention.

Scope of effect. Is the offensive operation meant for a narrow tactical or technical purposes (like disabling a botnet), achieving deep strategic gains (such as coercing a nation to stay out of an impending conflict), or something operational in between? Because of the nature of cyber space, offensive cyber operations have, like airpower, the theoretical ability to directly affect adversary centers of gravity far from his national borders and fielded military forces. On the other hand, cyber attacks can also have precise effects, which can make them appropriate for targeted operations with very limited impact.

Intended duration. Is the attack meant to have transient and short term effects (e.g., distract an adversary radar operator for a few minutes) or instead be persistent and long term (e.g., disrupt electrical transmission for the duration of a months-long conflict)? Though the duration of effects is likely to strongly correlate to the desired scope of effect (see above) this does not have to be the case. For example, a cyberattack might be intended to have a very short effect but right before a U.S. election, in an attempt to sway the results—a very limited duration attack but with strategic consequences.

[22]Healey, Jason. 2010. A Vocabulary for National Responsibility for Cyber Attacks. Cyber Conflict Studies Association. Available at http://www.cyberconflict.org/about-the-ccsa-board/-a-vocabulary-for-national-responsibility-for-cyber-attacks, accessed July 29, 2010.

[23]Meserve, Jean. 2007. Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid. CNN. Online. Available at http://www.cnn.com/2007/US/09/26/power.at.risk/index.html, accessed 26 July 2010.

Openness. Where does the offensive operation fall between being overt and covert? Though as a rule adversaries conducting espionage do not want to be identified, often the participants in offensive operations do not take as much time to cover their tracks. For example, the "patriotic hackers" who attacked the U.S. from China in 2001 or Estonia from Russia in 2007 spent less effort trying to be covert than the group behind the GhostNet intrusions attempting to track the activities of the Dali Lama and his followers.[24]

Context. Is the offensive operation being conducted as part of a wider increase in tensions—even war—between adversaries, or is the attack truly an "out of the blue" pre-emptive or surprise attack? In the kinetic world, offensive operations from a nation against another rarely, if ever, take place at times of low geopolitical tensions. Even "surprise" attacks, like the 1941 strike on Pearl Harbor (US) or 1904 attack on Port Arthur (Russia), both by the Imperial Japanese military, followed a long period of perceived encroachments and tensions.

Campaign use. Is the offensive operation meant to be a standalone tactical attack or part of a larger cyber operation and campaign? In the public mind, cyberattacks are hackers conducting one-off events of maliciousness, such as defacing a web page and it may even be tempting for cyber defenders to treat every attack as a discrete technical event. As noted in some of the other categorizations in this section, there are strong reasons for stand-alone attacks. However, in other domains, offensive operations are typically characterized by a campaign, composed of operations, each of which is a string of tactical engagements. See Attachment 2 for a discussion of this perspective of cyber warfare.

Initiation responsibility and rationale. Is the United States the first actor to use cyber weapons or has another adversary initiated the cyber conflict? The U.S. military might be most likely to initiate offensive cyber operations alongside kinetic operations while other adversaries might initiate cyber attacks early to try to gain an asymmetric advantage.

Initial timing. Is the use of offensive operations a surprise, a pre-emption to an expected incoming attack, or a counter-attack to a previous cyber or kinetic attack? A surprise attack is not just a first strike, but one strategically "out of the blue" while a pre-emption would be a first strike conducted in expectation of imminently receiving such an offensive attack. Counterattacks could be a response to a traditional kinetic offensive ("You bombed us so we'll disrupt your information.") or an earlier cyber-attack ("Hack *us*? Hack *this*. . .").

Initiation attack. If part of a campaign, are the offensive operations characterized by a massive initial set of strikes with many separate attacks? Or do the offensive operations build over time? Some theorists and movie script writers imagine a wave of attacks that debilitate the targeted adversary, whether a nation, company, or group. This is not the only tempo for an offensive cyber campaign, however, as graduated attacks could engage more targets with more profound effects over a course of weeks or months, similar to the aerial bombing of Yugoslavia as part of Operation Allied Force in 1999.

HOW MIGHT CYBER WARS BE FOUGHT?

One working definition for a "cyber war" is when between nations or groups there is an extended set of offensive operations that are each equivalent in effect to armed attacks conducted by militaries. If it is not an extended set of attacks, then given the transient nature of most certain cyber effects—the engagement is likely to be over fairly quickly, perhaps more akin to a natural disaster than a conflict. Similarly, any attacks with less than "effects equivalent to armed attacks" would not be similar enough to what militaries think of as warfare—even irregular warfare. If nations are at war, they get to stab the enemy, legally, and even civilian deaths can be acceptable if within the laws of armed conflict.

[24]Chinese Hack Into Indian Embassies, Steal Dalai Lama's Documents. 2009. Economic Times. Online. Available at http://economictimes.indiatimes.com/News/PoliticsNation/Chinese-hack-into-Indian-embassies-steal-Dalai-Lamas-documents/articleshow/4329579.cms, accessed 20 June 2010.

If this is an adequate description of cyber war, then the world has apparently not yet had one. So to think about how cyber wars might be fought, we have to use alternate methods of analysis. In the section above, this paper laid out ten characteristics of offensive operations, which can be combined to define characteristics of differing ways that cyber wars might be fought. For the next section, this paper will extend these ten characteristics to some well known, and less well known, analogies for cyber war.

This paper will start by tackling the two most often used analogies to think about cyber warfare. Newspapers splash headlines with "cyber Pearl Harbor" and "cyber 9/11," often using them interchangeably. However, both are handles that represent extremely different ways to employ force, which this paper will examine. The section after that will introduce several new analogies that capture additional possible ways cyber wars may be initiated and fought.

"Cyber Pearl Harbor" (or Surprise Attack by Military versus Military)

The Japanese attack on the U.S. military at Pearl Harbor on December 7, 1941 was a surprise attack during a period of high tensions that hoped to either dissuade the United States from engaging in protracted conflict in the Pacific theater or make that engagement at timing and terms greatly in the Japanese favor.[25]

A cyber Pearl Harbor, or "PearlHarbor.com" (see Table 1) might then be an initial, massive, integrated cyber offensive against the U.S. military in the hopes of quick strategic success, for example perhaps to coerce the United States or limit its ability to fight an upcoming conventional fight. This attack might be a tactical surprise but would be part of a larger geopolitical context of increasing tension and expectations of possible future combat.

One overlooked factor in discussions of a "cyber Pearl Harbor" is that it was just the opening strike of a larger campaign by the Japanese across the Pacific (including the Philippine Islands, Guam and Wake in the "eastern plan," and Hong Kong, Singapore, and other attacks as part of a "southern plan"). Moreover, these initial attacks were just the opening campaign of World War Two in the Pacific theater, a four-plus-year-long conflict that directly resulted from the sunken ships at Battleship Row. Likewise, any "cyber Pearl Harbor" could be reasonably expected to have the United States not succumb to coercion and angrily respond with all elements of national power.

So "cyber Pearl Harbors" can reasonably be expected to be followed by a major war, perhaps a traditional and kinetic war, possibly also though by a mix of major kinetic and cyber attacks (see "Cyber St. Mihiel" below) or an all-cyber fight (see "Cyber Battle of Britain" below). Of course, in that larger fight, the United States may not be again as talented and lucky as during the early 1940s, when Navy cryptographers could read the adversary's codes. However, any state adversary conducting such a massive surprise attack on the U.S. military must know that retaliation could come with devastating kinetic firepower even without 100% confidence of where the attack originated from. Non-state actors present a more challenging proposition in terms of retaliation. The 2003 U.S. *National Strategy to Secure Cyberspace* explicitly takes this approach in stating that "when a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner. The United States will be prepared for such contingencies."[26]

If there were a cyber Pearl Harbor against the United States, then obviously this kind of deterrence measure was clearly not enough to prevent the attack. The adversary may have judged its attack would be so successful the United States would be unable to withstand it, and would capitulate. However, deterrence might be able to limit the escalation, such as limiting the scope or lethality of follow-on attacks.

[25]Summary Report. U.S. Strategic Bombing Survey. Washington D.C., 1946, available at http://www.anesi.com/ussbs01.htm, accessed April 20, 2010.

[26]National Strategy to Secure Cyberspace. The White House. Washington, D.C., 2003, available at http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf, accessed March 3, 2010.

Table 1: Analogy: "Cyber Pearl Harbor"

Nature of adversaries	Military versus military
Nature of targets	Military
Target physicality	Any
Integrated with kinetic	Any
Scope of effect	Strategic
Intended duration	Long-term
Openness	Fully overt
Context	Surprise during tensions
Campaign use	Larger campaign
Initiation responsibility	U.S. defending
Initiation timing	Surprise
Initiation attack	Massive

Table 2: Analogy: "Cyber 9/11"

Nature of adversaries	Non-state versus State
Nature of targets	Civilian
Target physicality	Any
Integrated with kinetic	Any
Scope of effect	Operational
Intended duration	Medium-term
Openness	Partially covert
Context	Surprise
Campaign use	Stand alone
Initiation responsibility	U.S. defending
Initiation timing	Surprise
Initiation attack	Massive

"Cyber 9/11" (or Surprise Attack by Non-State Versus Civilian Targets)

Though a "cyber Pearl Harbor" and "cyber 9/11" (see Table 2) seem to be used interchangeably, they would not be similar. The attacks on Pearl Harbor targeted the U.S. military and were conducted by a foreign military in a time of rising international tensions whereas the attacks on September 11, 2001 were conducted by non-state actor—the terrorist group Al Qaeda—and targeted civilians and civilian infrastructure. The U.S. response to both these attacks also led to a protracted military campaign fought both conventionally and unconventionally, this time against Afghanistan, which, nine years later, is still ongoing.

A "cyber 9/11" then would be an attack by a non-state actor attempting to destroy or disrupt key civilian infrastructure to result in catastrophe, perhaps across several sectors and simultaneously in several locations. However, as occurred after the real 9/11 when international public and legal opinion swung overnight,[27] America might be able to hold a nation responsible for a non-national group acting from its national soil possibly leading to longer-term conventional and unconventional military campaigns.

The damage from the real 9/11 was tragic, but the economic impact, although significant, was less than expected, ranging from GDP losses of $35 billion to $109 billion or between 0.5 percent and 1 percent of the GDP[28]) and limited, even in the short-term, as the New York Stock Exchange was closed for only four days.[29] This is likely also to be the case after a cyber 9/11, as typically disruptions from cyberattacks are either widespread or catastrophic but not both. So large-scale cyber disruptions might have severe impacts for a week, or even two, after which the economy may return to normal as indeed happened after 9/11 and other catastrophes like the volcanic air disruptions of 2010, Asia-wide earthquake-induced undersea cable outages in 2006, and the Northeast blackout of 2003.

In a classic cyber 9/11, the adversary would be a non-state actor, such as a terrorist group, attackers who may be difficult to deter from attacking by threatening punishing cyberattacks in return. It would be very difficult to attribute a large non-state attack with enough precision to undertake a counterblow. Even if it could be done, the terrorists would have no assets they value that would be susceptible to significant disruption. Though deterrence with offensive cyber capabilities may not be credible, deterrence with physical force (as happened to Al Qaeda and the Taliban) may be more so if the actor's center of gravity such as operating bases and sanctuaries can be located. Attacking computer systems to make

[27]Public Opinion Six Months Later. 2002 The PEW Research Center for the People & the Press. Available at http://people-press.org/commentary/?analysisid=44, accessed July 27, 2010.

[28]From a January 2010 report by the University of Southern California and referenced at "Study: Economic Impact of 9/11 Was Short Lived." 2010. NBC Los Angeles. Available at http://www.nbclosangeles.com/news/business/Study-bin-Ladens-Strategy-Was-Short-Lived.html, accessed April 2010.

[29]History of the New York Stock Exchange. NYSE Euronext. Available at http://www.nyse.com/about/history/timeline_2000_Today_index.html, accessed May 2010.

money or for kicks may be popular amongst hackers, but few would either want to cause significant damage and fewer still would be willing to face violent death or being a prisoner at Guantanamo Bay.

Though these two analogies, of Pearl Harbor and 9/11 are the most popular, there are a number of other ways that offensive operations could unfold. According, this section examines these and, where appropriate, draws a historical analogy. These additional five scenarios are not, of course, the only possibilities and perhaps are not even the likeliest, of how offensive operations fit into national military strategy and tactics. However, they are particularly illustrative of the possibilities and spotlight an additional framework for positing future cyber conflicts.

Covert Cyber Operations

Because of the difficulty of attribution, cyberattacks seem to lend themselves strongly to covert operations, whether by the United States or other states or adversaries, as a third option between "doing nothing (the first option) in a situation in which vital interests may be threatened and sending in military force (the second option)."[30] (See Table 3.) Even if the attack is detected and attributed to the nation of origin, the low barrier of entry for cyber attack capability always gives some level of plausible deniability.

Accordingly, it may be that the future of cyber conflict is not equivalent to larger, theater-level warfare but only to select covert attacks which could range across a wide set of goals and targets. It is plausible that every step of the "covert action ladder"[31] could be undertaken through offensive cyber operations: propaganda (least violent and most plausibly deniable) through political activity, economic activity, coups and paramilitary operations (most violent and least deniable). As these have been well-covered already in previous work by the National Academies,[32] they will not be repeated here.

Deterring covert operations would only be credible if attribution could pierce the veil of "plausible deniability." This may be difficult in many situations, especially if the standard of proof needs to be particularly high, such as to counterstrike. For many responses, though, less than perfect attribution may be "good enough." The attacked nation might privately threaten retribution to the suspected party or release sufficient details and suspicions to publicly smear them in the international press. This should be considered plausible as it parallels the responses to the GhostNet and Google cyber espionage cases, where non-state defenders went public with their details. This may not have achieved a completely successful deterrence effect against the presumed Chinese spies, but may be found in the future to have had some partial deterring effect on means, methods, targets, or frequency of attacks.

Direct Support for Special Operations

Unlike their use in a 9/11 or Pearl Harbor attack, offensive cyber operations could (even more easily) be used for very targeted, covert or clandestine attacks in support of special operations (see Table 4). For example, offensive operations could disable alarms or even create enough false alarms that operators learn to disregard the information on their screens. Likewise, voice-over-IP networks would be open to short term disruption to keep defenders from raising alarms or coordinating their defenses.

Gaining access is a critical first step for offensive cyber operations, so an attack in support of special operations may be characterized by unique access methods, not just over the Internet but also those enabled by corrupting a supply chain, the help of an insider, or having the special operators themselves use their physical access to the target to gain access to the target systems.

---

[30]Lowenthal, Mark M. 2008. Intelligence: From Secrets to Policy. Washington, D.C.: CQ Press. P 165.

[31]Lowenthal, Mark M. 2008. Intelligence: From Secrets to Policy. Washington, D.C.: CQ Press. P 170.

[32] See section 4.2 of the NAS study: Owens, William A., Kenneth W. Dam, and Herbert S. Lin. 2009. Technology, Policy and Law Regarding the U.S. Acquisition and Use of Cyber Capabilities. Washington, D.C.: National Academies Press.

Table 3: Covert Cyber Operations

Nature of adversaries	Intel versus any
Nature of targets	Any
Target physicality	Any
Integrated with kinetic	Any
Scope of effect	Any
Intended duration	Any
Openness	Covert
Context	Tension
Campaign use	Any
Initiation responsibility	U.S. initiating or defending
Initiation timing	Surprise or pre-emptions
Initiation attack	Limited

Table 4: Special Operations Support

Nature of adversaries	Military versus any
Nature of targets	Any
Target physicality	Any
Integrated with kinetic	Fully integrated
Scope of effect	Tactical
Intended duration	Short-term
Openness	Covert
Context	Surprise
Campaign use	Stand alone
Initiation responsibility	U.S. initiating or defending
Initiation timing	Any
Initiation attack	Massive

Furthermore, as more control systems and voice systems move to IP networks—making them more accessible in a wider range of conditions—the possibility for such surgical cyber support for teams working quietly in foreign countries seems strong. Obviously, because of the nature of these operations, the general public may never hear about these operations if conducted by the U.S. military. If an adversary conducted such a covert or clandestine attack, even the U.S. military or the targets of the attack itself may not know an attack has happened.

These cyberattacks would be difficult or impossible to deter by punishment, as the main effort of the attacker is the kinetic action of the commandos, which the cyber effect only enables.

"Cyber St. Mihiel" (or Operational Support for Traditional, Kinetic Military Operations)

St. Mihiel was the first mass operation of airpower during wartime, when in 1918 then-Colonel Billy Mitchell organized nearly 1500 aircraft in a synchronized campaign[33] to support one of the first solo U.S. offensives of World War One.

Though there have been Information Operations cells as part of military commands since the mid-1990s,[34] cyberattacks in support of military operations known cases of such operations are limited in number and not part of large-scale operations. However, in the future it could be that cyber conflict has an equivalent of St. Mihiel where cyber forces engage heavily, on both offense and defense, in support of more traditional military operations (see Table 5).

In such a scenario, computer network defenses fight off attacks to maintain U.S. communications, abetted by counterforce computer network attacks to suppress adversary offenses. Other computer network attacks could be used to disrupt critical infrastructure, such as the adversary's telecommunications centers, which would enable the offense to disrupt and delay the transit of information of the opposing military, and potentially disrupt or even destroy the command and control networks. Computer network exploitation missions might ensure access to key information like troop movements, learning the adversary commander's decisions and intent, combat assessment for kinetic and cyber strikes, and helping to direct new kinetic and cyber attacks to the enemy's weakest points.

In some cases, the adversary may have cyber capabilities to shoot back, but at other times, it may be that one side has superiority of the cyber domain. Either way, cyber deterrence not only has failed, but also is likely to remain of second importance to controlling the kinetic fight. It may still have a role though, especially if patriot hackers and copycat attacks confuse each side's national leaders, potentially derailing conflict resolution.

[33]Lt Col George M. Lauderbaugh. The Air Battle of St. Mihiel: Air Campaign Planning Process Background Paper. Airpower Research Institute. Online. Available at http://www.au.af.mil/au/awc/awcgate/ww1/stmihiel/stmihiel.htm, accessed May 2010.

[34]Maj Gen Gary Pounder, USAF. 2000. "Opportunity Lost." Aerospace Power Journal. Available at http://www.airpower.maxwell.af.mil/airchronicles/apj/apj00/sum00/pounder.htm, accessed July 26, 2010.

Table 5: Analogy: "Cyber St. Mihiel"

Nature of adversaries	Military versus military
Nature of targets	Any
Target physicality	Any
Integrated with kinetic	Fully integrated
Scope of effect	Operational
Intended duration	Medium-term
Openness	Overt
Context	Existing state of war
Campaign use	Campaign
Initiation responsibility	U.S. attacking and defending
Initiation timing	Attack or counter-attack
Initiation attack	Any

Table 6: Analogy: "Cyber Battle of Britain"

Nature of adversaries	State versus state
Nature of targets	Any
Target physicality	Any
Integrated with kinetic	None
Scope of effect	Strategic
Intended duration	Long-term
Openness	Overt
Context	Hostilities
Campaign use	Campaign
Initiation responsibility	U.S. attacking and defending
Initiation timing	All
Initiation attack	Any

"Cyber Battle of Britain" (or Overt Force-on-Force Cyber Conflict with Near-Peer Nation)

The Battle of Britain was the series of aerial campaigns fought between the Axis (predominantly Germany) and the British in 1940. The first large-scale contest between air forces, the German goal was originally to enable an invasion of the British Isles through attacks on ports and convoys. This targeting shifted over time to focus on the Royal Air Force before moving to direct attacks against key cities through terror bombing. In the end, these attacks meant to inflict strategic damage, either through a collapse of national morale and unity or through direct economic damage from destroyed infrastructure. The British goals were primarily defensive, to stop the German attacks, through a mix of defensive engagements combined with their own offensive strikes. This air war was fought largely independently from the fight in other domains and theaters.

The analogous conflict in cyberspace would be a standalone, overt cyber battle or war between nations, fought entirely within the domain of cyberspace and fully engaging each side's cyber attackers and defenders (probably both in government and the private sector) (see Table 6). Though tactical engagements might take place "at the speed of light" these would be mere dogfights in the context of the larger fight, with complete operations as part of offensive and defensive campaigns. A cyber Battle of Britain may develop slowly, through various phases (as did the original, 70 years ago) moving up from smaller, less-organized attacks before blossoming into a full force-on-force unleashing of violence. Each side may be deterred from making larger cyber attacks (as the Germans originally forfeited attacking cities) but continue to one-up the other nation in a progression of violence.

Though deterrence will have failed to prevent the initiation of cyber hostilities and escalation, a cyber Battle of Britain could still provide successful escalation control. Each adversary in this conflict might choose to limit themselves to only non-kinetic operations for a number of reasons, but perhaps the most compelling would be that neither adversary would be willing to escalate from cyber force to kinetic. Even if the effects of the offensive cyber campaigns were equivalent to those from a kinetic armed attack (death or significant property destruction), escalation to kinetic operations could entail possibly unacceptable risks to both sides—from international opprobrium for going kinetic first or uncertainty of how the other side might further escalate.

For a more extended case study on the strategic air war over Europe and implications for offensive cyber operations, see Attachment 1.

Large, Covert Cyber Conflict with Near-Peer Nation

A cyber conflict need not be overt to be destructive. It is possible that two national adversaries may choose to engage in a long series of offensive operations that neither is willing to admit to publicly (though they may be more frank with each other) (see Table 7).

Table 7: Large, Covert Cyber Conflict

Nature of adversaries	Intel versus Intel
Nature of targets	Any
Target physicality	Any
Integrated with kinetic	No
Scope of effect	Any
Intended duration	Medium-term
Openness	Covert
Context	Tension
Campaign use	Campaign
Initiation responsibility	U.S. attacking and defending
Initiation timing	Attack or counter-attack
Initiation attack	Any

Table 8: Below-Legal Threshold Campaign

Nature of adversaries	State versus state
Nature of targets	Any
Target physicality	Logical
Integrated with kinetic	No
Scope of effect	Strategic
Intended duration	Long-term
Openness	Overt
Context	Tension
Campaign use	Campaign
Initiation responsibility	Any
Initiation timing	Any
Initiation attack	Gradual

For example, here is one plausible (though certainly not probable) chain of events. The nation of Zendia has been conducting long-term and massive computer espionage against Ruritania, which is unable to stem the loss of information. The Ruritanian leadership, though unwilling to openly conduct counterattacks, authorizes covert offensive operations to dissuade the Zendians. After the first disruptions of manufacturing and electrical power, the Ruritanian leadership informs the Zendians that they were behind the attacks and provide credible proof, while continuing to deny it publicly. Instead of backing down, however, the Zendians conduct covert attacks of their own, disrupting logistics networks and financial transactions. Each side feels they were unfairly escalated against and continue retaliatory strikes, which are increasingly harsh while trying to retain plausible deniability.

A similar analogy may be the hot intelligence competition during the Cold War. The actions of spies and associated covert actions illustrate how two nations can fight in the shadows, maintain plausible deniability to the world (though the other side may know full well who was responsible), but still maintain tacit norms and boundaries. In the Cold War, an American agent might kill a Bulgarian or East German in the line of duty without significant retribution. But if a Russian were killed instead, the Americans would have been seen to have crossed a red line and would expect their own casualties in response.[35] In the cyber domain as much as the physical, tit-for-tat attacks had to be carefully measured, lest either side miscalculate and have a response be seen as an unwarranted escalation.

Understanding the correct retaliation is an exceptionally fine line, especially in cyber conflict, where the second- and third-order effects cannot be fully understood beforehand. A counterattack, even if precisely measured for a specific intent by an attacker, may be misunderstood by a defender and may have effects far worse than the attacker's intent.

Below-Legal Threshold Campaign

In the physical domains, there are many actions nations may take against each other that, while aggressive, fall beneath what the international community normally considers an "armed attack," the threshold set out by Article 51 of the United Nations Charter. These actions can take a range of forms including boycotts, broadcasts, stationing warships in international waters off the coast, increasing border patrols and improving defenses, missile tests, and large-scale exercises practicing an invasion.

It is possible that a nation would overtly use offensive cyber operations, kept similarly below the nebulous threshold of "armed attack," to coerce another nation (see Table 8). This may seem alluring to a nation's leadership, frustrated at the behavior of a rival; however any offensive operations kept deliberately below the threshold of armed attack may be more likely to be just a nuisance rather than a real challenge to coerce the adversary's leadership. This could mean a Below-Legal Threshold Campaign would be paired with a covert campaign. Of course, the nation on the receiving end of the sub-

[35]Discussion between author and Mark Lowenthal, 11 August 2010.

threshold overt attacks and over-threshold covert attacks would certainly suspect with a high degree of confidence which nation was behind both—and also attribute almost every other cyberattack from whatever source to their tormentor.

If the campaign were conducted over a long period of time or caused a certain amount of cumulative disruption it is possible the international community could decide it had become a de facto armed attack. This determination may not be a formal decision, such as the decision by the International Courts of Justice, but could be the consensus of international leaders and elite. Separately, democratic nations may have particular difficulties attempting to conduct a campaign of this type, as attacks would have to be crafted to not disrupt freedom of speech and diminish the moral authority of the attacking country.

"Cyber Vietnam" (or Long-term Irregular Warfare)

The Vietnam War was an extended irregular conflict, the first part of which was dominated by a guerilla war. The lightly armed Viet Cong insurgents fought asymmetrically—backed by the North Vietnamese regime—against the South Vietnamese and their American sponsors. Though the U.S. response was with traditional military forces, some units, such as the Special Forces, would attempt to engage the Viet Cong using guerilla-style tactics, albeit aided by more firepower and technology.[36]

An analogous irregular cyber conflict might involve few large-scale incidents with large-scale effects, but a continuing string of attrition attacks seeking to erode an adversary's power, influence, and will (see Table 9).[37] For example, an adversary (such as a group of Islamic radicals or extremist environmental or animal rights groups) could undertake only a handful of attacks in a year and whose effects may be very transient, disrupting operations of Wall Street for a day, or causing local blackouts of a few hours. However, these attacks could be significant enough to gain concessions from the U.S. government or get media attention for their political aims.

The targets of such offensive operations from a non-state adversary, like those of traditional guerillas, might target fielded military forces; headquarters or logistics; military and civilian institutions relied on by those forces (like payment systems); or prohibited targets like hospitals or schools; or civilians individually or en masse. Similarly, a nation state looking to fight an online guerilla war will be constrained from attacking these same targets sets.

A typical tactic of guerillas is to cause an overreaction from the other, more powerful, adversary as this can help push more people to supporting the guerillas' cause. Another is to ensure civilians are impacted directly or indirectly to force them to pressure their government to cease hostilities or influence the way the war is fought. In cyber conflict, these tactics could take the place of goading "hack-backs" of computers in neutral countries or against prohibited targets or attacks to coerce U.S. industries or individuals.

In a true "cyber Vietnam" the attacking group would also have the backing of a national sponsor, aiding and encouraging its campaigns, though possibly unwilling to commit their own cyber or traditional military forces. In this situation, nation states may attempt to re-establish some state-to-state responsibility especially for covert attacks.

A cyber guerilla campaign should not be mistaken for the acts of patriot hackers, conducting denial of service or defacements attacks for national reasons. These attacks hint at what a determined adversary might accomplish but fall far short of actual warfare.

Cyber Threat Removal

An offensive cyber operation might also be a small- or large- scale operation conducted to counter computers engaged in mass attacks (see Table 10). Such activities could be roughly analogous to naval

[36]Department of the Army. Appendix F: After Action Report: Operation Blackjack 33. U.S. Army Center of Military History. Available at http://www.history.army.mil/books/vietnam/90-23/90-23af.htm, accessed July 27, 2010.

[37]Department of Defense. 2007. Irregular Warfare Joint Operating Concept. Available at http://www.fas.org/irp/doddir/dod/iw-joc.pdf, accessed April 5, 2010.

Table 9: Analogy: "Cyber Vietnam"

Nature of adversaries	Non-state versus military
Nature of targets	Any
Target physicality	Any
Integrated with kinetic	Possible
Scope of effect	Any
Intended duration	Long-term
Openness	Overt
Context	Hostilities
Campaign use	Campaign
Initiation responsibility	U.S. attacking and defending
Initiation timing	Attack or counter-attack
Initiation attack	Any

Table 10: Cyber Threat Removal

Nature of adversaries	State versus any
Nature of targets	Any
Target physicality	Logical
Integrated with kinetic	No
Scope of effect	Technical
Intended duration	Short-term
Openness	Overt or covert
Context	Hostilities
Campaign use	Any
Initiation responsibility	Either
Initiation timing	Attack or counter-attack
Initiation attack	Any

operations against pirates that were common up until the 18th century and are becoming increasingly so in the 21st. In this scenario, a nation state would identify botnet zombies or controllers and use offensive operations to keep these offline. These attacks could be limited to "technical" counterattacks intended to counter specific adversaries, whether states, groups, or individuals. Instead they are focused on the means of the attack, the computers themselves.

Such an operation could be considered a counterattack if the nation were attacking botnets that were themselves targeting (or had targeted that nation); a pre-emptive move if there were intelligence that the nation would soon be a target; an initiating attack if none of those were true; or even a surprise attack if the nation did not announce the intention to carry out these kinds of attacks.

These attacks may be overt or covert and may or may not be part of an overall campaign. Some nations could in future decide to choose such operations as part of a persistent, constant presence to remove threats from cyberspace. It is highly unlikely that operations for cyber threat removal, whether a standalone engagement or part of a larger campaign, would be integrated with kinetic military operations. There may theoretically be a network so dangerous that offensive cyber operations would be teamed with Special Forces or kinetic covert action, but it is more likely, of course, that these cleanups would be integrated with law enforcement.

Deterrence would likely be very effective to dissuade threat-removal operations. If a nation clearly stated that it would see clean-ups of systems residing in its national borders as illegal or even acts of war, there likely would be far fewer such operations conducted than if such operations were conducted within the boundaries of more supportive nations (who might be convinced to see the cleaning up of the cyber commons as a public good).

CNE Campaign

A CNE Campaign would be a large-scale intelligence gathering campaign, probably by one nation (or the proxies of that nation) against the government or companies of another (see Table 11). Though this is a very likely kind of cyber conflict (and indeed may describe the current state of cyberspace), it is neither cyber warfare nor a use of offensive cyber operations, and so will not be given significant analysis in this paper and is included here only for completeness in describing possible future cyber conflicts. However, an effective CNE campaign is likely a critical enabler of many of the types of offensive operations described in this paper. Many of the key challenges regarding targeting, access and likely effects on targeted systems will be most directly addressed through the conduct of CNE.

FOR FURTHER RESEARCH AND CONCLUSION

This paper set out with the intention to outline important categories of offensive cyber operations and outline some ways cyber warfare might employ these capabilities. The framework here can be

Table 11: CNE Campaign

Nature of adversaries	State versus any
Nature of targets	Any
Target physicality	Logical
Integrated with kinetic	No
Scope of effect	Strategic
Intended duration	Not applicable
Openness	Covert
Context	Peacetime
Campaign use	Campaign
Initiation responsibility	U.S. spying or defending
Initiation timing	Not applicable
Initiation attack	Any

expanded with additional categories and trimming out of categories that lack power to analyze offensive operations as we have more empirical evidence about how these operations are conducted. Moreover, these analogies to how cyber wars might be fought are just a summary of a small subset of the possibilities. Further research can deepen the analysis of each of these analogies as well as add new analogies. Another potentially lucrative research path is utilizing the existing literature on coercive use of force to analyze how the frameworks, concepts and findings apply to cyber conflict, particularly as related to factors identified as underpinning the success or failure of cyber warfare.

Conflict in cyberspace—and offensive operations there—are new and novel, but as this paper has hopefully shown, traditional national security thinking can help illuminate the emerging issues. The ways to categorize offensive operations include adjectives typical also of modern kinetic military operations, such as whether the attack was a surprise, part of a larger campaign, or was covert or overt. Similarly, though "cyber 9/11" and "cyber Pearl Harbor" can have a deeper meaning than their popular associations, these handles can point how to apply military history and novel thinking to this new field.

ATTACHMENT 1: CYBER BATTLE OF BRITAIN

A complete, fully referenced exploration comparing the Battle of Britain to a future cyber conflict would require a separate full-length paper, so this attachment will cover only the most relevant points.

The Battle of Britain was the series of aerial campaigns fought between the Axis (predominantly Germany) and the British in 1940. This air war was the first large-scale contest between air forces and was fought largely independently from the war in other domains and theaters. The German goal was originally to enable an invasion of the British Isles through attacks on ports and convoys.[38] This targeting shifted over time to focus on the Royal Air Force before moving to direct attacks against key cities through terror bombing. In the end, these attacks meant to inflict strategic damage, either through a collapse of national morale and unity or through direct economic damage from destroyed infrastructure. The British goals were primarily defensive, to stop the German Air Force (Luftwaffe) attacks, through a mix of defensive engagements combined with their own offensive strikes both to stop the invasion (by destroying barges) but also deep strikes against Berlin, intended to target war-making capability. However, in response to the British attack against Berlin, the Germans countered with reprisal attacks against British cities.[39]

[38]Royal Air Force. The Battle of Britain. Available at http://www.raf.mod.uk/bob1940/phase1.html, accessed July 11, 2010.

[39]World War Two: Timeline 1939-1945, Fact File: the Baedeker Raids. BBC. Available at http://www.bbc.co.uk/ww2peopleswar/timeline/factfiles/nonflash/a1132921.shtml?sectionId=4&articleId=1132921, accessed July 27, 2010.

Phases of Conflict

The original Battle of Britain was conducted nearly a year into formal hostilities by the combatants and the battles up to that point had been relatively conventional, in that there were not large-scale independent operations in the aerial domain. A cyber Battle of Britain need not follow either of those patterns, possibly being the opening battle without any earlier kinetic attacks. However, to follow the analogy more directly, the goals of the offense in such a battle would begin with a purely military operational focus, such as to enable or stop an invasion or coerce an adversary. The targets would be tied to the direct military objective. During the original Battle of Britain, the German objective was to invade so their original targets were ports and convoys.

However, if facing more difficult defenses than expected, the offensive cyber forces might shift targets, as the Luftwaffe did in mid-August (after a month of fruitless battles in the English Channel) to take the Royal Air Force on directly.[40] This phase of a cyber Battle of Britain would be a battle of attrition between offensive and defensive forces. In such a fight, either side might miscalculate its attacks and accidently prompt an escalation that neither side particularly wanted. After an attack on Berlin caused civilian casualties (mistakenly thought to be intentional), the Germans shifted to reprisal and terror attacks against civilian targets to defeat civilian morale. Unexpectedly, during this "Blitz" the populace of Britain became more cohesive, not less, and the shift gave relief to the RAF from the contest focused on the attrition of forces, which had been sorely pressed by attacks on their home airfields.[41]

Forces and Institutional Capability

As in an extended aerial campaign, in a cyber Battle of Britain success would favor the side with the most flexible employment of tactical and operational forces, especially if that side had a doctrine that most closely matched the conditions of the future battle.

Both the RAF and Luftwaffe entered the Battle of Britain with equipment and ideas based on pre-war doctrines that did not meet the needs of this new kind of warfare.[42] The British did not anticipate having to fight enemy fighters over their country, only bombers. Their resulting tactics were inflexible, locked into tight v-formations with only the leader free to scout for enemies. RAF commanders recognized this weakness but did not feel able to switch to more successful tactics in the middle of a key battle, meaning they were not as successful as they could have been had they correctly anticipated the nature of the coming air war. Similarly, German commanders, though with more appropriate fighter tactics, had not planned on long-term strategic bombing in favor of tactical bombing and close-air support to ground troops. Having underestimated the problems of strategic bombing campaigns, they assessed the entire aerial campaign would be over in weeks.[43] For both sides, weapons that made doctrinal sense did not perform as expected in actual warfare, such as for limited attack capability in force-on-force engagements (the RAF's Boulton Paul Defiance with no forward-facing guns) or unexpected vulnerability during unanticipated mission types (the Luftwaffe's Stukas).[44]

There will almost certainly be similar cascading doctrinal errors made by offensive and defensive cyber forces. For example, defenders may have expected deterrence to forestall any attacks or not planned properly to operate through disruptive attacks. Attackers might have a "cult of the offense," thinking that initial attacks would paralyze the defenders, making them incapable of successful defense,

[40]Royal Air Force. The Battle of Britain. Available at http://www.raf.mod.uk/bob1940/phase1.html, accessed July 11, 2010.

[41]The Blitz and World War Two. The History Learning Site. Available at http://www.historylearningsite.co.uk/blitz_and_world_war_two.htm, accessed July 28, 2010.

[42]Dye, Peter J. Logistics and the Battle of Britain. 2000. Air Force Journal of Logistics. Accessible at http://findarticles.com/p/articles/mi_m0IBO/is_4_24/ai_74582443/, accessed July 15, 2010.

[43]The Royal Air Force. The Battle of Britain: Background. Available at http://www.raf.mod.uk/bob1940/background.html, accessed 28 July 2010.

[44]Junkers-Ju 87. Academic Dictionaries and Encyclopedias. Available at http://en.academic.ru/dic.nsf/enwiki/10000, accessed July 27, 2010.

much less being able to counter with attacks of their own. Defenders may have underestimated the vulnerability of critical infrastructure targets protected by the private sector—or even overlooked their importance entirely. For a more detailed analysis of this dynamic between the lessons of aerial and cyber warfare, see *Strategic Warfare in Cyberspace* by Greg Rattray.

While attrition in aerial warfare is relatively easy to conceptualize (and measure) the concept also holds for cyber conflict. Each side would only have a certain number of trained "pilots" to handle offense and defense—these could easily be saturated. The attackers and defenders would also have a limited number of "airfields," "aircraft," and "bullets." These could be equivalent respectively to network capability, non-attributable attack hosts or botnets, and new exploits. Each of these resources can be replenished, in varying timeframes. Even more so than in aerial warfare, cyber operations favor the attacker. Defenders can be swamped with only one attack against a critical target, and so have a steeper exhaustion curve. A sophisticated adversary should be able to exhaust the defenders over time with comparatively less effort of their own.

Though the exhaustion curve of the offense may be less steep, the resources of attackers are not limitless and can be exhausted over time. Offensive forces may deplete their supply of new exploits to continue to inflict pain on the other side. Once an exploit is used, a skilled adversary would cover that defensive hole to make future, similar attacks difficult or impossible. In addition, there are fewer offensive operators, planners, and intelligence professionals than there are skilled defenders. The attacker's forces must balance these rare subject matter experts across their operational tempo, between combat assessment for yesterday's missions, conducting today's missions, and planning tomorrow's. Few nations would have the ability to surge a reserve to bring additional attacking forces to bear.

Key Enablers

The offense and defense in the Battle of Britain were enabled by a number of key factors, several of which might also have a cyber equivalent. Some of these factors are summarized in the list below:

- Ability to train weapon system operators and produce weapon systems. One factor to cessation of hostilities in 1940 was when the attacking Luftwaffe realized they could not destroy enough aircraft and factories to prevail.[45]
- Intelligence mismatch between offense and defense. The Germans had little targeting intelligence[46] to guide their next attacks and limited resources for battle damage assessment. Accordingly the offense could not adequately assess its past attacks or plan future missions whereas the defense had excellent situational awareness to detect and track incoming attacks.
- Strong defensive coordination that made the most of early warning and enabled operational flexibility to effectively counter attacks. A centralized command and control system with decentralized execution used advanced knowledge to counter attacks long before they reached their targets.
- Support crews to keep weapon systems operational with short turnaround times after each mission.

Defensive Coordination

The British held a decisive advantage with their "Dowding System"[47] to detect incoming attack formations and respond quickly and effectively. To detect attacks the British developed and employed both high-tech (radar) and low-tech (searchlights and observer corps) systems. Some elements, like the

[45]The Royal Air Force. The Battle of Britain: Background. Available at http://www.raf.mod.uk/bob1940/phase4.html, accessed July 27, 2010.

[46]"Battle of Britain." U.S. Centennial of Flight Commission. Available at http://www.centennialofflight.gov/essay/Air_Power/Battle_of_Britain/AP22.htm, accessed July 25, 2010.

[47]The Battle of Britain: The Dowding System. *Spiritus Temporis*. Available at http://www.spiritus-temporis.com/battle-of-britain/the-dowding-system.html, accessed July 21, 2010.

Chain Home radar stations, had to be set up well before the battle actually began while others developed over the course of the fight. For example, nearly a month into the battle a liaison unit was set up at Fighter Command to pass signals intelligence to fighter commanders.

The heart of this system was a central information center to gain comprehensive situational awareness based on all the incoming feeds, make quick assessments about the incoming attacks, and make defensive decisions, to be passed to operational commanders who would conduct their own interceptions.[48]

A defender in a cyber Battle of Britain, would have directly analogous needs, from equivalents radar (technology like deep-packet inspection at Tier 1 telecommunication providers to sense incoming attack) to observer corps (concerned users or companies reporting incidents to the government or information sharing centers). This information would have to pass to a command center empowered to see all the data and with sufficient authority to issue orders.

A cyber command center, for a cyber Battle of Britain, would present several tremendous disadvantages compared to the RAF's Fighter Command Headquarters. In a cyber conflict, attacks may target the private sector which may be outside of the military commander's authority. Accordingly there would have to be some way to pass situational awareness and coordinate defenses with key companies, including Tier 1 telecommunications providers, financial institutions, power companies and other likely targets. If the commanders don't hear about attacks because of a lack of sensors or the incident isn't reported (or even noticed), then there cannot be any Dowding-like coordination system or central defense. And while the RAF's operational commanders were able to issue orders to subordinate commands (under centralized control, decentralized execution), most Western nations lack any ability to issue orders to companies in the critical infrastructure sectors that would be the likely targets of attack. Few nations are likely to even have clear lines of authority to control their cyber defenses.

Moreover, the Germans did not know of the existence or the importance of most elements of the Dowding System so they were not countered, with the exception of some furtive strikes on radar stations, quickly abandoned as they were deemed not productive.[49] The command and control system may have been more fragile to dedicated attacks than airfields, if the Luftwaffe had had sufficiently good intelligence on its elements and locations. Cyber defenders in a cyber Battle of Britain may not be able to expect the same level of forbearance from their attackers. In many countries the major networks are well mapped and the major players known and basic emergency response plans published. All of these defensive elements are likely to be targeted early and often by a determined adversary.

Cessation of Hostilities

A cyber Battle of Britain may end the same way as the first one: the attacker realized it would not prevail and shifted its military attention to another adversary and theater, with no announcement, capitulation, or negotiation. If there were no other hostilities between the attacker and defender, this drift in a cyber conflict might mean each was willing to return to status quo ante especially if the attacks on either side were not catastrophic. The conflict could become a fight in the shadows, fought by intelligence forces stealing each other's secrets with periodic covert actions. Also, the two sides might just as easily decide on a more traditional agreement of armistice, though this may be hard to verify if there were copycat attacks or strikes by patriotic hacker.

Of course, the cyber force-on-force fight could expand into conventional, kinetic attacks. In this case, the offensive operations may take on a role more similar to a "cyber St. Mihiel," as airpower did after the Battle of Britain, taking on roles of intelligence, reconnaissance, or tactical and strategic strikes until there was a clear victor in the contest.

[48]The Battle of Britain: The Dowding System. *Spiritus Temporis*. Available at http://www.spiritus-temporis.com/battle-of-britain/the-dowding-system.html, accessed July 21, 2010.

[49]The Battle of Britain: The Dowding System. *Spiritus Temporis*. Available at http://www.spiritus-temporis.com/battle-of-britain/the-dowding-system.html, accessed July 21, 2010.

ATTACHMENT 2: TWO PERSPECTIVES OF CYBER WARFARE

There are two overlapping (but in some sense competing) perspectives of how cyber warfare will look. Both are valid and enlightening and both are needed to understand the likely course of future warfare in cyberspace. To help illustrate these perspectives, this section first charts the *military technical view of cyber warfare.*

(1) Attacks against the United States (in red [in the PDF of this volume]) are directed through unwitting hosts by a shadowy but sophisticated adversary (Figure 1).
(2) Subsequently, the United States—with the military Cyber Command in the lead—undertakes defensive counterstrikes to stop the pain while still defending against new strikes, as in Figure 2.
(3) Through skill and hard work (and luck), the United States is able to track back to the elusive adversary. Having established its identity sufficiently to convince the national leadership, Cyber Command begins the counterstrike to punish the foe and compel them to peace, as in Figure 3.

This military technical perspective is certainly valid, but also misses an important lesson of history. Typically traditional, kinetic wars—violent, large-scale conflicts between nations or armed non-state groups—take place as a series of unfolding tactical engagements over time.

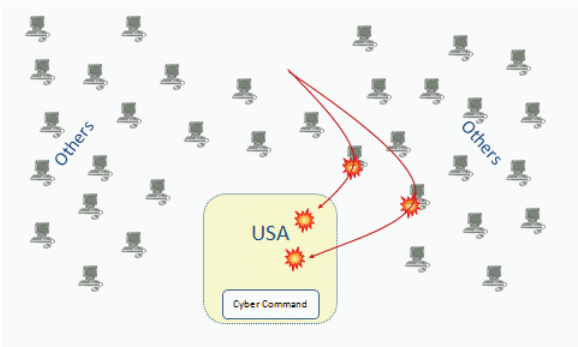

FIGURE 1 The Attack Begins: Military Technical View of Cyber Warfare

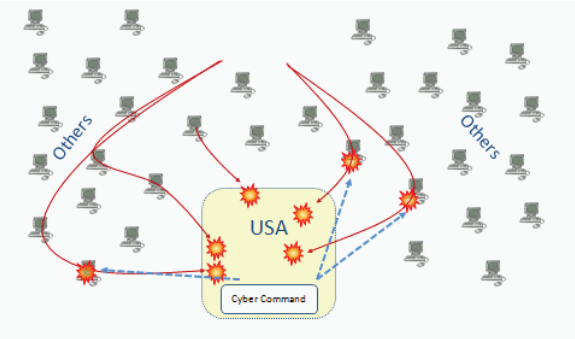

FIGURE 2 The Battle Is Joined: Military Technical View of Cyber Warfare

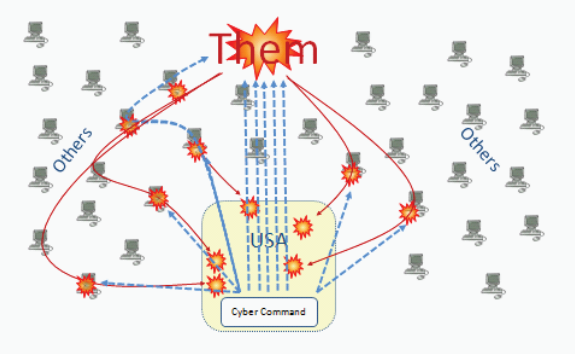

FIGURE 3 The Battle Reaches Crescendo: Military Technical View of Cyber Warfare

In the *traditional view of warfare*, it is entirely possible, even probable, that large-scale warfare in cyber space would follow the same model—a series of connected high-speed "dogfights" strung together into operations which are in turn, part of larger campaigns (see Figure 4). All happen in serial or parallel depending on the opposing forces and terrain, as part of a theater of war.

Of course, there may be combat operations in several theaters of war, either simultaneously or over the duration of a multi-year conflict, as in Figure 5.

An even more overlooked aspect of cyber warfare is that the interplay of the offensive and defensive cyber forces is likely to only be one field where the combatants compete with each other. They are likely to contend also with economic actions, like blockades or sanctions; rallying allies or international organizations; and with their intelligence forces, even through hostilities had ceased (Figure 6).

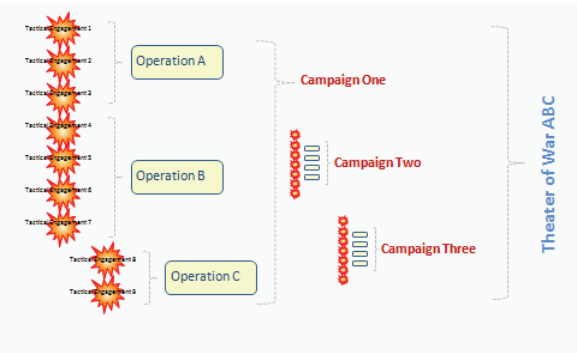

FIGURE 4 Traditional View of Warfare

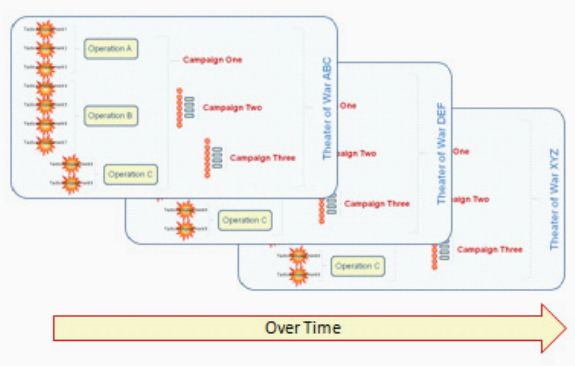

FIGURE 5 Traditional View of Warfare

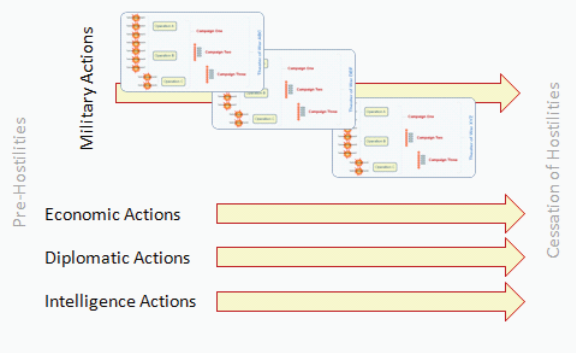

FIGURE 6 Traditional View of Warfare