Published by Cyber Magazine, 22 June 2017,
http://magazine.milcyber.org/stories/developingastrategyforcyberconflict

Developing a Strategy for Cyber Conflict

By Arnold J. Abraham, Institute for Defense Analyses

Introduction

History teaches the importance of developing the right strategy to adapt to a changing situation on the world stage. At the dawn of the last century, a significant shift in the global balance of power began to emerge. Germany's power was rising, but it still faced significant rivals on both her Eastern and Western borders. The Schlieffen Plan was developed as a strategy to meet this challenge and was put to the test in World War I. The strategy called for Germany to leverage its military and infrastructure strengths to rapidly mobilize and concentrate forces to quickly defeat the French army on one front before shifting east to face the Russians. The strategy failed and the results were catastrophic. Almost ten million soldiers died in that war, far exceeding any conflict to date, and the unresolved struggle soon led to another war, which was even more devastating.

Now, in the early 21st century, the United States is the sole global superpower, but new concerns require non-linear extrapolation to develop a strategy to overcome current and future adversaries. In particular, the emergence of the cyberspace domain presents unprecedented opportunities and challenges for national security. Nations around the world have begun to recognize the significance of this dynamic, but the United States has the most at stake due to its premier position. With this in mind, U.S. Cyber Command is in the process of training and deploying a cyber force. But to optimize that force, the right strategy is needed.

This paper explores the question, "*How do we develop the right force optimization strategy for cyber conflict*?" It is important to invest time and effort to work through the concepts because the stakes are enormous. The first issue to address is the significance of conflict in cyberspace, not just as an aspect in the evolution of modern warfare, but as an integral element of today’s society and world. Within this context, optimal approaches for conducting cyber warfare are explored, including the best ways to posture and utilize the cyber force. Ultimately, a risk management approach is proposed to allow for leverage against many unknown factors. In the absence of hard-earned lessons learned through full-scale conflicts, simulation, exercises, and war games become the vital ingredients for developing successful strategies. But these tools can only go so far—the objective strategy may require a significant restructuring and rebalancing effort. The scale of the change seems daunting, but as cyber conflict transcends military conflict, the change should be dealt with in a revolutionary manner that does not underestimate the growing importance of cyberspace in global affairs.

What is Strategy?

Why bother to discuss strategy after the April 2015 publishing of the Department of Defense Cyber Strategy to guide the development of DoD’s cyber forces and strengthen its cyber defense and cyber deterrence posture? That document did an excellent job of describing the drivers behind the need for a strategy and articulated a set of five strategic goals and over a dozen detailed objectives. However, it is better characterized as a “strategic implementation plan” rather than a strategy itself. It is a good roadmap, but one based on the assumption of a known objective end state. Alternatively, this paper calls for an examination of underlying premises because even the best map cannot be used to chart a path if one is not yet sure of the ultimate destination or method of travel.

Developing a Strategy is the art of balancing Ends, Ways, and Means against Risks. Ends are the objectives (what is to be achieved), Ways are the courses of action or methods (how and when are the available tools used to get the job done), and Means are the resources (what tools are to be acquired and used). Assessing Risk involves recognizing the Strengths and Weaknesses and the Opportunities and Threats presented by the environment and the actors. Unfortunately, U.S. leaders sometimes overlook the importance of using this model to develop optimal strategies. Instead, over-reliance on superior technology and greater resources is seen as the path to victory. When it comes to Cyber Strategy, these advantages are no longer determinative, and thus pressure is building for a more astute approach.

What is the significance of cyber conflict in modern warfare and society?

For much of human history, nations fought over control of territory. Fertile land, rich mineral deposits, navigable rivers, and safe harbors were the early prizes that eventually evolved into vital industrial and population centers. Land and sea forces were the predominant means to seize and maintain these objectives. As technology advanced, control of the airspace became an important contributor to determining the outcome of battle. Similarly, the automation of command and control mechanisms added the potential for actions in the cyberspace domain to affect conflicts between air, land, sea, and space forces. But cyber power now also offers a potential approach to conflict independent of military engagement in the traditional air, land, maritime, and space domains.

Where will the most significant struggles play out for dominance in the cyberspace domain?

Virtually all modern battlefield weapon systems have some connection to cyberspace. This means existing arsenals of air, land, and naval weapons themselves represent potential direct targets in cyber conflict at the tactical level. Similarly, administrative, logistical, and other support networks essential to conducting military operations are reliant on cyberspace and therefore are potentially vulnerable to cyber attacks as part of theater-wide campaigns. Finally, critical civilian national infrastructures that provide the foundations for military force projection now also have cyber vulnerabilities that can be exploited at the strategic level. Thus, cyberspace operations must take place at the tactical, operational, and strategic levels of conflict.

The ability for cyber power to be applied across all levels of war has led several strategists to consider the development of airpower as an analogy. Aircraft offer a similar range of options, starting with air-to-air or air-to-ground engagements (e.g., dogfights, tank plinking), moving up to targeting military installations (e.g., airfields, logistics depots), and finally to directly disrupting strategic infrastructures (e.g., petroleum-oil-lubricants and ball bearing plants). As airpower developed, significant debate ensued as to where along this spectrum it would be most effective. Even after more than 100 years of using airpower, the debate continues. A similar debate has begun on the application of cyber power. However, instead of expecting a definitive answer, the lesson to be applied from the airpower analogy is that we must be prepared to use cyber power across each level of war from the tactical to strategic.

The cyberspace domain is more than the newest realm for extending traditional military conflict to achieve military ends. The pervasive nature of cyberspace in modern society has led to challenges beyond those that typically fall within the purview of a military force. First, the age-old struggle between the concepts of freedom of information/transparency versus personal privacy has been amplified significantly through the emergence of cyberspace. Second, the entire global economy is increasingly intermeshed with cyberspace, and the competition for information advantage has become an essential ingredient of private sector profitability. The cyberspace domain has become an integral part of modernity. Given this unique dynamic, the airpower analogy falls short when trying to extend lessons beyond the military dimension. Instead, we must look to other models.

Deterrence and Cyber Conflict

The theory of deterrence, which is as old as war itself, has been applied with varying degrees of success to avoid conflict entirely or discourage use of particular weapons and attack techniques. During the Cold War, much thought went into nuclear deterrence theory in an attempt to grapple with the extreme consequences of atomic weapons. The “Wizards of Armageddon” developed concepts such as the strategic triad, massive retaliation, and mutually assured destruction, which became part of national strategy.

The potential to apply deterrence to cyber conflict has garnered interest, and “deterrence of cyberattacks” is discussed in the DoD Cyber Strategy. However, much work remains to be done, starting with determining what goal is really being sought. Is this a version of “cyber arms control” or “de-escalation?” Or does the United States seek to retain freedom of action to use cyber power as it deems necessary while restricting any potential adversary’s range of options? Answering these questions requires first figuring out our strategic concept for the use of cyber power.

Additionally, deterrence requires predictable actors whose decisions can be influenced through the right combination of words and deeds targeted to affect their interests. This is particularly challenging for future cyber conflict, which may include unpredictable and radical non-state actors, some of which remain unidentified, while others may not yet exist. Thus, discussion of cyber deterrence should be pursued within the context of developing an overarching strategy for cyber conflict – the optimal mix of “ends,” “ways,” and “means.”

What will the primary nature of future cyberspace struggles involve? What are the “Ends” we should strive to achieve?

Military. As noted above, conflict in cyberspace can have multiple dimensions. First, there is the application of cyber operations as a component of military power to enable, supplement, or replace use of other capabilities. This can be done through either force-on-force attacks or by directly attacking other military targets. As cyber weapons mature and proliferate, these types of attacks will likely become a standard part of military conflicts. Providing information assurance for conventional weapon platforms will be as vital as providing an air defense umbrella for land and sea forces and rear areas. The ability to disrupt an adversary’s weapon platforms through cyber-attack will also be a valuable tool, but possibly less vital in most cases due to the availability of existing kinetic options to service the same potential targets. Cyber-attack options will be most valuable when political considerations constrain the use of traditional military force. Although the application of cyber power can lead to casualties and physical destruction, there is also the potential to launch attacks whose effects are intentionally limited to being non-kinetic, temporary, reversible, or all three, and that may be more suitable for the early stages of an international crisis. On the other end of the scale, military cyber-attacks may provide the only feasible means to penetrate hard targets without paying too high a price in terms of friendly force attrition against heightened physical defenses. However, to date, no direct cyber casualties have been recorded.

Intelligence/Counterintelligence. While cyber power will grow to be a significant complement to kinetic force application during military conflict, it will have even greater roles in other areas as evidenced by recent events. Cyber capabilities have already radically altered the landscape for intelligence and counterintelligence. The amount of digitized information far exceeds what has previously been available, and the center of gravity for the intelligence world has already shifted to the cyberspace domain. If a nation wishes to keep its secrets, it must first provide adequate security for its networks. A single insider with wide network access can wreak havoc, as has been demonstrated on more than one occasion (e.g., Snowden, Manning). On the other end of the spectrum, a determined power can develop remote accesses that lead to transfers of valuable information on an unprecedented scale. In 2012, General Keith Alexander, Director of the National Security Agency and Commander of U.S. Cyber Command, described the loss of industrial information and intellectual property through cyber espionage as the “greatest transfer of wealth in history.” Thus, conventional weapon platforms may still dominate current and future military conflicts, but the tide has already turned in the world of espionage and the role of cyber power within it.

Homeland Security. Homeland security is another area of which cyber power has become a crucial component. Critical civilian infrastructures in sectors such as power, transportation, banking, and communications increasingly rely on cyberspace components. The increased efficiency of the advances has benefited society, but it comes with a price that has not yet been fully realized. A whole new class of vulnerabilities exists, which requires attention beyond the physical protective measures we have traditionally relied on to remain secure. Further, unlike in the physical world, the potential to exploit those vulnerabilities is not limited to those actors in close proximity to the facilities. This is a particularly irksome challenge for the United States to face after having enjoyed the buffer of its oceans for two centuries. Hostile actors from anywhere across the planet now represent a direct potential threat. Such actors may have no affiliation with foreign militaries or intelligence services. They may not even be part of any recognized terrorist organization and could remain “under the radar” from the perspective of traditional geopolitical security interests.

Law Enforcement. On a day-to-day basis, law enforcement is the one area that has been affected by the cyberspace domain even more notably than espionage or homeland security. The vast majority of cybersecurity incidents are not traced back to foreign military forces, intelligence agents, or terrorists—they are simple criminal acts, often committed by low-level perpetrators, including some who may not even have malign intentions. Hackers are everywhere today, ranging from the teenage lone-wolf script kiddies in competition for bragging rights to international criminal syndicates organizing multimillion-dollar embezzlement schemes. This ubiquitous challenge is complicated by the fact that the technical signatures of malicious cyber activity are often hard to distinguish when first detected (*if they are detected at all*). This means that activity appearing to be a criminal breach may ultimately be traced to state-sponsored action with political or military motives. While national security concerns continue to grow, the predominant cyber threat to guard against today remains criminal activity, which now costs the global economy over $400 billion per year.

Regulation. The final area for consideration is the most mundane and most removed from the high-adrenalin crisis-oriented world of military conflict. In fact, the greatest risks and destructive impacts within the cyberspace domain to date have been crises that neither the military nor homeland security or law enforcement forces could prevent. Instead, the greatest damage has been due to inadvertent technical failures, which are more akin to acts of nature and natural disasters than acts of a determined adversary. These threats are best addressed by regulation and safety measures. The most prominent example was the self-inflicted wound of “Y2K” and subsequent remediation, which cost over $300 billion worldwide. Industry generally riles against government regulation of cyberspace, but as the risks to public safety grow, the role of regulation and oversight will inevitably increase. Cybersecurity managers will eventually find solace in regulations that help to define standards of due care considered by the courts to determine liability with some predictability. The traffic safety model offers an analogy of where things may be headed in cyberspace. Before the automobile, anyone with the physical ability and resources could ride a horse with little interference from the government. As the automobile became prevalent, an entire regulatory scheme and supporting infrastructure evolved to ensure safe transit (speed limits, traffic lights, highway guard-rails, vehicle registration, license plates, driver's licenses, mandatory insurance, etc.). Unfettered access by any and all to the "information super-highway" may soon become a risk society can no longer afford. How to manage that risk through optimal regulatory means and enforcement mechanisms may be the most daunting cyberspace challenge faced by the government.

What are the optimal organizational approaches (i.e., the "Means") to help achieve and maintain dominance in cyberspace?

While some conflicts between nations consist primarily of military contests, it is clear that the struggle for dominance in cyberspace involves multiple axes of effort as noted above. Given the widely varied nature of the threats faced in the cyberspace domain, the question of how to best posture our capabilities becomes crucial. Defending the network on one day may mean blocking hostile attempts to overload a system with denial of service traffic, but on the next day, it could require enforcing maintenance of a firewall standard on a private company's server. It could involve discovering and countering malware implanted in critical platforms, or strikes against the source of such attacks to cut off their command and control. Cyber threats continue to evolve and escalate at a pace beyond what we are used to in the physical domain. The struggle for dominance in cyberspace will require a versatile force that can operate within and across the variety of challenges found in the military, homeland security, intelligence, law enforcement, and regulatory realms.

Can existing structures be adapted to meet the new challenges? Currently, the bulk of the U.S. Government's cyber resources reside within the Department of Defense (DoD), including the National Security Agency, U.S. Cyber Command and Cyber Command's Service Components. The Federal Bureau of Investigation, the Central Intelligence Agency, and Department of Homeland Security (DHS) also have key roles. However, none of these elements have the complete range of authorities and capabilities to deal with the full scope of the challenge. The Commander of U.S. Cyber Command, Admiral Mike Rogers, recognized this reality when he described cyber as "the ultimate team sport" because no one organization has all the answers or the capability to solve all problems.

Bolstering any one of the existing elements, a combination of them, or even all of them will still fail to address the seams and inherent frictions of interagency bureaucracy. But there is no need to accept the status quo and rely on virtual "pick-up" teams drawn from across a sprawling network of independent agencies. Instead of trying to wedge cyberspace into the existing apparatus, a new model should be explored. Cyberspace presents many new and unique challenges, but this is not the first time that the nation has had to struggle with problems that do not present themselves neatly within current frameworks. Organizations such as the United States Coast Guard, the Merchant Marine, and the Public Health Service provide useful models that could be templates for building a cyber force to address all of the nation's concerns. Those organizations were formed to fill crucial gaps that once existed, and they continue to provide unique services today.

The Coast Guard is a uniformed, armed military service that resides within the Department of Homeland Security during times of peace, but can operate under the Department of Defense when war is declared, or by direction of the President. Its missions fall within the categories of maritime safety, security, and stewardship. The Coast Guard is the pre-eminent law enforcement authority within its domain. In addition to securing waterways against intrusion by unauthorized personnel or materials, the Coast Guard develops and enforces vessel construction standards and domestic shipping and navigation regulations. To ensure compliance, it reviews and approves plans for ship construction, repair, and alteration, and it routinely inspects vessels, mobile offshore drilling units, and marine facilities for safety. Finally, the Coast Guard provides aids to navigation and search and rescue services that are welcome by all legitimate mariners.

Unlike any other military force, the Coast Guard has a pervasive domestic presence, interacting in an authoritative manner on a day-to-day basis with civilians operating in their domain. The public not only accepts the Coast Guard's role, but generally embraces and depends on it as a valued partner in maritime pursuits. The cyber force of the future should have a similar ability to transition smoothly from regulatory, to law enforcement, to security functions, adapting to different challenges as they present themselves. Strong relationships with the private sector are likewise essential, because the primary domain for conflict is not a remote battlefield across the globe, but the server farms and databases of companies forming the backbone of the new digital economy. A future "U.S. Cyber Guard" (or an independent "Cyber Agency" or a new cabinet-level "Cyber Department") could be postured to directly repel attacks on critical infrastructures, aid the private sector and government in remediation efforts or resiliency measures, and help set and enforce day-to-day standards in cybersecurity for issues that impact the nation’s security. The Coast Guard model deserves careful study because, despite the pressing need, the public is not inclined to endorse DoD or the Intelligence Community with the broad responsibilities needed for true effectiveness in cyberspace. Thus, a new organization outside of those elements is needed at the Agency or Department level—independent, yet interdependent. Regardless of what it is called, the new organization must have mixed authorities and responsibilities for cyberspace in a manner similar to those the Coast Guard has in the maritime domain.

Two other important organizations that offer lessons learned are the Merchant Marine and the U.S. Public Health Service. These organizations are relatively minor components of the Federal Government today, but they have rich histories going back to the early days of the United States. They were established outside of the predominant organizations to perform vital niche functions that contribute to national and homeland security. On one end of the spectrum, the U.S. Public Health Service is a small cadre of experienced medical personnel who are commissioned as officers and distributed to serve across numerous federal organizations. Taking the opposite approach, today’s federal component of the Merchant Marine exists only in the form of a training academy that teaches new mariners, who can then work as civilians manning vessels. Following one of these models, a “U.S. Cyber Academy” could be established to train the finest network security engineers, who would then fulfill their federal obligations by serving in key cybersecurity positions for the private sector. In the other model, a “U.S. Cyber Hygiene Service” could be created to manage a cadre of operations experts who would be assigned to work within each federal department to fill key cybersecurity roles.

Merchant Marine – a Model for Integrated Government and Private Sector Cyber Partners

The United States Merchant Marine is a fleet of over 400 U.S.-registered, privately owned civilian merchant vessels that carries imports and exports during peacetime, and that can become a naval auxiliary during wartime to deliver troops and war materiel. The Merchant Marine is complemented by the National Defense Reserve Fleet, which consists of "mothballed" ships that can be activated during national emergencies, either military or non-military, such as commercial shipping crises.

Merchant mariners move cargo and passengers between nations and within the United States, and they operate deep-sea merchant ships, tugboats, towboats, ferries, dredges, excursion vessels, charter boats, and other waterborne craft on the oceans, the Great Lakes, rivers, canals, harbors, and other waterways.

During World War II, the U.S. Government controlled the cargo and the destinations, contracted with private companies to operate the ships, put guns and armed Navy personnel on board. The U.S. Maritime Service trained the men to operate the ships and assist in manning the guns. Over 240,000 served, and they suffered one of the highest casualty rates of any Service in the war. Today, the uniformed Merchant Maritime Service exists only at the U. S. Merchant Marine Academy, a federal service academy that educates licensed Merchant Marine officers who serve U.S. marine transportation and defense needs in peacetime and war. Graduates are obligated to serve aboard vessels or be commissioned as officers in the military or National Oceanic and Atmospheric Administration Corps.

A cyber equivalent of the Merchant Marine could involve a range of options. To mirror its current form, a U.S. Cyber Academy would provide trained cyber experts who would populate private cybersecurity firms upon graduation, but they would have reserve commissions and be on tap for recall in the event of crises. On the far extreme, significant investments could be made in a dual-purpose cyber infrastructure that would not only aid in commerce but also bolster resiliency and be subject to direct government re-purposing in the event of national need.

U.S. Public Health Service (USPHS) – a Template for National Cyber Hygiene?

The USPHS consists of a uniformed commissioned corps of 6,500 public health professionals who serve within federal agencies such as the National Institutes of Health and the Centers for Disease Control and Prevention. The USPHS provides rapid and effective response to public health needs, leadership in public health practices, and advancement of public health science. USPHS traces its beginnings back to the U.S. Marine Hospital Service, which protected against the spread of disease from sailors returning from foreign ports and screened the health of immigrants entering the country. Today, USPHS officers are involved in health care delivery to underserved and vulnerable populations, disease control and prevention, biomedical research, food and drug regulation, mental health and drug abuse services, and response efforts to natural and man-made disasters as an essential component of the largest public health program in the world.

A cyber equivalent of the USPHS would consist of a new uniformed Cyber Service, separate from the Army, Navy, Air Force, and Marines. Just as when the Air Force was formed, this does not mean every cyber operator would need to be pulled from his or her current home. Instead, the Cyber Service could be a small cadre that focuses on only advanced offensive or defensive cyber operations—and like current USPHS professionals, they could be embedded within other elements of government to aid those organizations.

None of these examples are sufficient to serve as complete solutions, but they highlight the potential for unconventional approaches. It is clear that cyberspace conflict is not just a military issue. A successful strategy begins with recognizing the scope of the problem, and posturing correctly to address the challenge. Whatever form it would take—U.S. Cyber Guard, U.S. Cyber Service, or U.S. Cyber Academy—it cannot be just another element of DoD. Beyond Title 10 warfighting responsibilities, strong law enforcement, regulatory, and intelligence authorities are also needed. A hybrid element bridging both DoD and DHS, like the Coast Guard, holds the most promise to handle the full range of issues.

What are the best "Ways" to strategically posture and operationally utilize the Cyber Mission Force?

Once the overarching challenges are addressed, there will still be a need for a military cyber force devoted to military missions. The U.S must first choose whether the cyber force currently under development should become the kernel of a new comprehensive solution or focus solely on the military mission. The former requires significant political advocacy for changes in authorities and organizational structures that are unlikely to materialize without an external catalyst (e.g., a "Cyber Pearl Harbor" or "Cyber 9/11") to force new thinking. The latter means ceding ground on which most of today's cyber conflicts and internal controversy resides, but it allows a focus on the military's traditional spheres of expertise.

A force optimization strategy that confines the Cyber Mission Force to a military focus requires evaluating cyber weapons' utility as a substitute for or complement to other military capabilities. The key question is whether cyber weapons provide "another arrow in the quiver" or a whole different method of conflict. Do cyber weapons simply provide another means to take out existing priority targets, or do they represent something entirely different—such as the next stage in the evolution of combined arms warfare?

Employing a combination of military techniques to leverage the strengths of particular weapon systems against the weakness of others is a mainstay of modern conflict. This approach, known as "combined arms" (originally conceived to involve infantry, mounted cavalry, and artillery), continues to evolve as technology brings new weapons to the battlefield. Today, military officers are still taught the critical importance of synchronizing attacks through different means to defeat adaptive adversaries.

When applied to airpower, combined arms meant that one could not rely solely on anti-aircraft artillery to defend airspace but also needed the ability to scramble fighters to intercept and engage in air-to-air combat with intruding bombers. In turn, the bombers were given fighter escorts to aid in penetration of enemy defenses.

At sea, a complex network of specialized vessels and aircraft has been developed, including attack submarines, frigates, destroyers, cruisers, and aircraft carriers. No fleet sails without the appropriate combination of these platforms to ensure capability against a range of threats.

Inclusion of cyber attack and defense in combined arms warfare will apply to land, sea, and air combat. Just as ground forces learned to consider their vulnerability to air strikes, all military forces must now become prepared for cyber attacks. Under this construct, future Army Divisions may each require their own cyber battalions, responsible for tactical offensive and defensive cyber maneuvers within their areas of operation. The same would be true of Navy, Air Force, and Marine equivalent forces.

An alternative way to envision cyber forces is as specialized strategic capabilities limited to certain extreme cases, in a manner such as chemical, biological, radiological, or nuclear weapons. These weapons, judged by society as particularly gruesome means of causing death and destruction, are generally reserved for dire circumstances. In most cases, their use is tightly controlled by treaty, agreement, or public policy. Unlike the combined arms model, which would lead to inclusion of cyberspace engagements in practically any and all conflicts, this method of employment would see offensive cyber power become highly restricted.

While cyber attacks may someday be viewed as similar to attacks by other weapons of mass effect, they do not currently carry such a stigma and are therefore relatively free of internationally recognized restrictions on battlefield employment. However, the fear of potential widespread secondary and cascading effects do bring significant political pressures to bear when using cyber power against civilian targets or other networks connected to the Internet. Therefore, cyber power may best be employed in a hybrid manner. The first method is on a tactical and operational level, in conjunction or integrated with other military forces, in a counter-force role to disrupt or otherwise defeat adversary military weapon systems and forces. The second method is on a strategic level, independently as a counter-value capability to directly affect an adversary's national power through cyber attacks on civilian and economic centers of gravity.

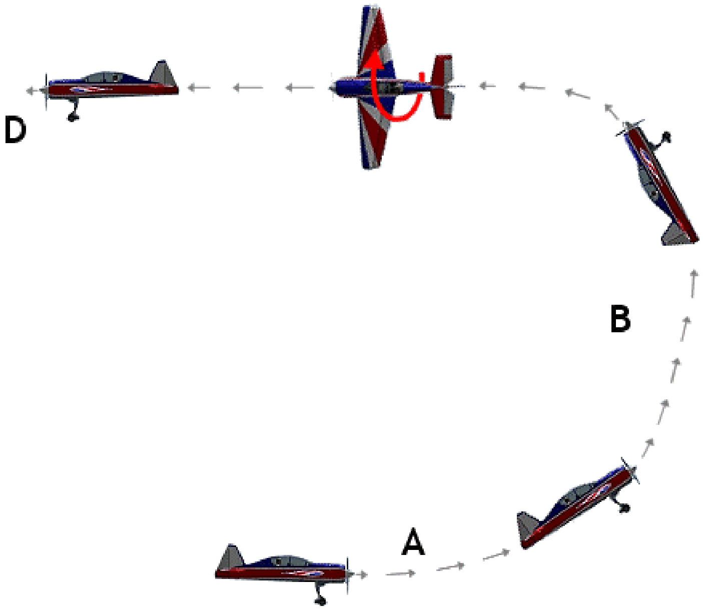
There is another fundamental question beyond determining how cyber forces best fit in alongside and integrated with other military forces to achieve objectives. Within the cyberspace domain itself, the individualized tactics to achieve optimal effects remain a vital issue. Other weapon systems are limited by geography and many other physical constraints, but these do not apply in cyberspace. For example, there is no need to conserve firepower due to the logistical strains behind storage and transport of available rounds of ammunition. There are also no circles to be drawn on the map to depict the maximum effective range where targets can be held at risk before fuel or gravity holds sway. Additionally, there is no need to apportion the physical terrain as a means to avoid friendly fire and fratricide. Instead, the limiting variables are access to detailed intelligence, maintaining access on extremely dynamic networks, and perishability of exploits once specific attack mechanisms become public or after first use.

Within these new constraints, the most effective means to employ cyber power will likely vary because of the fluid nature of the domain. However, certain techniques may be worth using as the default. For example, a basic question is whether it is more effective to concentrate firepower or distribute it. The “deep and narrow” approach and the “shallow and wide” approach (e.g., precision-guided weapons versus carpet bombing) each has its benefits and detriments in different scenarios.

Similarly, one must consider whether to apply “strength versus strength,” or is it better to use one’s strongest force to exploit weaknesses in an adversary’s defense? Sun Tzu wrestled with these questions 2,500 years ago, and his sage advice stood the test of time in the physical domain, but it may or may not translate well to the virtual world.

Another consideration is the sequencing of attacks. Should cyber power be held in reserve for the turning points in battle, or can it be best used as the preliminary strike? Or should it be applied as a constant unrelenting barrage throughout an engagement?

Some answers are known already. For example, the classic “3:1” ratio of forces needed for offense to defense, developed as a gauge for ground combat, is clearly not applicable in the cyberspace domain. But other warfighting principles and techniques, from the basic through the advanced, remain to be discovered. For example, what is the cyberspace equivalent of the “Immelmann” air maneuver that came out of World War I dogfighting, or the “Crazy Ivan” developed by Cold War submariners?



Defensive strategies must also be further developed. For example, when should fixed-point fortifications be relied on versus mobile defensive countermeasures? These and many other combat strategies cannot be relied on using a default solution based on the first idea presented or the program that is cheapest or quickest to implement. Instead, dedicated and concentrated effort must be applied to development of cyberspace strategies and techniques, as was done in other realms of conflict. Many modern battle techniques have emerged from Service War Colleges and Command and Staff schools.

While it is too early to determine the optimal strategic, operational, and tactical employment of cyberspace forces, we do not need to wait until after a major conflict to find the answers. Instead, a robust simulation, war game, and exercise program should be pursued as the primary line of effort. Sun Tzu’s ancient prescription to “know your enemy, know yourself, and in 100 battles you will not be defeated” must be adapted to the virtual test range. Even though a particular technique or formation may appear to be working, the alternatives must be considered until every feasible angle is investigated. While it is true that exercises, simulations, and war games do have a role in today’s military, they are often seen as a drain on resources away from the day-to-day operational mission. This dynamic needs to be reversed for cyberspace to ensure the right investments for the future.

Conflict in the cyberspace domain does not benefit from the natural evolution mankind experienced in the physical domain. We are used to judging distance and speed by eye and can readily apply such lessons. Similarly, hundreds of years of experience in structural engineering yields, as a byproduct, the ability to calculate the destructive effects of explosives against facilities. In comparing the domains, even our most advanced cyberspace practitioners are still novices when it comes to fully understanding the terrain and methods of maneuver. The potential risks and rewards are too great to wait to learn these lessons the hard way—in the course of battle. Therefore, while simulation, war games, and exercises are part of every military mission, they must play an even more extensive role for cyber conflict.

Instead of selecting a particular strategy now and pursuing it straight away, a sizable portion of the cyber force should be devoted to developing the path ahead. For much of the Cold War, a majority of military forces focused on getting ready for a battle they fortunately never fought. A return to this type of model may be prudent for cyber forces, filling the calendar with a variety of realistic exercises and virtual force-on-force simulations. Strategic Air Command was the pinnacle of this approach, being well-known (one could say almost “infamous”) for its rigorous exercise, training, and evaluation program to support readiness. The procedures for nuclear conflict had been finely honed, but painstaking practice was needed to ensure precise execution of the plan if called upon. The current state of cyber conflict requires a similar level of intense effort, far beyond the current level of commitment to exercises and training.

Cyber teams should be developed along different conceptual approaches and tested against each other—again, and again, and again. It may seem counterintuitive to take troops "off the line" when cyber incidents are occurring on a daily basis, but the long-term risk must be balanced against that of the present day. When the time comes to execute a major cyber conflict, we can ill afford to be surprised by major developments.

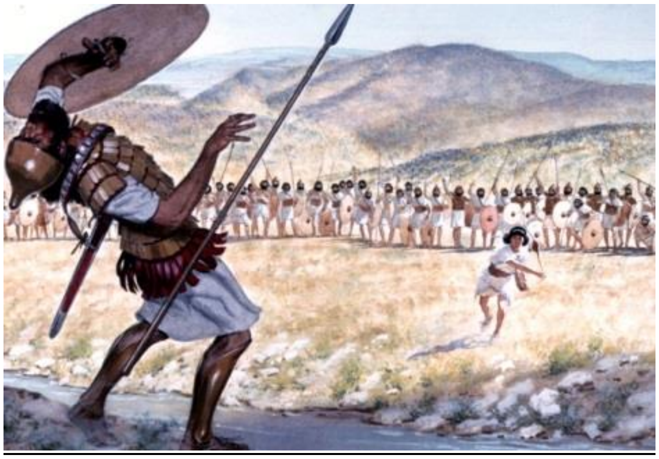
Conclusion

While the United States currently enjoys military superiority across the globe, developing the right strategy for cyberspace operations can mean the difference between victory and defeat in future conflicts. In the early 1600s, a tiny nation rose to pre-eminence in global affairs. The Dutch Gilded Age saw a transformation of the Netherlands from a minor possession of the decaying Holy Roman Empire into the world's foremost maritime and economic power. The Dutch East India Company was at the heart of the "Dutch Miracle"—it was the world's first multinational corporation financed by the first modern stock exchange. The story is relevant today because it is essentially a tale of new technologies and new organizational concepts being combined in a game-changing strategy, altering the global balance of power. Such stories are inspiring to some, but are potentially foreboding for the United States today.

The 21st century is no longer a time for business as usual when considering the shifting balance of power in cyberspace. Today, the United States, Russia, and China dominate, but tomorrow it could be smaller but highly advanced technical powers such as Israel, Japan, and Singapore that take the fore. Alternatively, the very essence of national power may be redefined as super-empowered individuals and international non-state actors such as the Islamic State in Iraq and Syria (ISIS), *Anonymous*, and Google seize the initiative in a rapidly evolving landscape…as the Dutch did 400 years ago.

Without a crystal ball, it is impossible to know what the right strategy is. But we do know that the wrong strategy can lead to disaster. It is necessary to adapt to the changing situation readily apparent across the spectrum of day-to-day affairs. Today's environment requires a non-linear extrapolation. The best swordsmen of their day, with the most training and finest steel, could not stem the tide of firearms and explosives. Now is not the time to just keep sharpening the sword. But it is also not the time to throw down the sword and take up an entirely new type of arsenal. Instead, a risk-management approach to balance the right ends, ways, and means of strategy demands spreading efforts across the range of potential outcomes to guard against both likely and unforeseen contingencies.

Rather than waiting for the aftermath of a major cyber conflict to show the way, a robust simulation and exercise program must explore a range of alternatives. This will require some sacrifice of readiness to execute current missions, but it is an investment in the future to avoid outcomes with the potential for much greater harm. The answers cannot be constrained to existing paradigms, so an important part of the future investment is to establish an organization free of ties to legacy structures and policies. DoD and U.S. Cyber Command should lead the charge in calling for a new organization to be their vital partner in developing the optimal cyberspace strategy for the nation. While U.S. Cyber Command focuses on its military role, another non-DoD element will be able to transcend the military, intelligence, law enforcement, and regulatory functions. Even while the Cyber Mission Force is still being fleshed out, it is time to raise the flag of the "United States Cyber Guard."



David and Goliath

The story of David and Goliath is well known as a classic example of the improbable victory of an underdog over a more powerful foe. The author Malcom Gladwell, whose works focus on unexpected implications of social science research, recently published a book which concludes that giants are sometimes not as powerful as they seem, and history is replete with examples of unexpected outcomes of this nature. Gladwell suggested the hidden weakness of "Goliath" enterprises is their tendency to assume that the strategy that made them great will keep them great. The Goliath story shows that someone perceived as an underdog may actually have an advantage by employing an alternate strategy.

Favoring the underdog is a part of American tradition, but when it comes to cyber conflict, the United States is the "Goliath" of the tale. The February 2015 National Security Strategy states, **"We possess a military whose might, technology, and geostrategic reach is unrivaled in human history."** From our 21st century telecommunications infrastructure and $13 trillion economy to our $600 billion DoD budget (which represents more than one-third of the entire global market), and seemingly omnipresent Intelligence Community, the United States rests atop a perch as the world's sole superpower. But many are actively seeking to change the status quo, and a range of potential new foes is on the horizon. Developing the right strategy for cyber conflict is crucial because the United States cannot continue to rely on its size and strength to defeat future "cyber-Davids."

About the Author

Mr. Abraham is a Distinguished Graduate of the National War College, a Principal Attorney with The CyberLaw Group, and member of the MCPA's Board of Advisors. He previously served as a Senior Executive in U.S. Cyber Command, the Department of Homeland Security, and the Office of the Director of National Intelligence. He wrote this paper based on research sponsored by the Institute for Defense Analyses.

Photo credits (in order of appearance): AFCEA International, onthenetgang.com, Huffington Post, Littlegate Publishing, Duffel Blog, Eder Flag, Department of Defense, GameSpy, RC Airplane World, Cryptome, silist.com.