Cyber Superiority: Overcoming Strategic and Operational Vulnerabilities in Future War

Over the past few decades, the Department of Defense (DoD) has integrated the cyber domain into all of the warfighting functions. Cyberspace operations represent the potential to gain significant technological advantage. Throughout history, military forces have worked to establish superiority in each of the warfighting domains to win wars. Establishing cyber superiority will be necessary to win future wars. While providing many advantages, the DoD’s integration of the cyber domain into all of the warfighting functions may develop into significant strategic and operational vulnerabilities. If the United States military is unable to establish cyber superiority, its overreliance on cyberspace creates significant vulnerabilities that may prevent the United States from winning future wars.

Cyber superiority, cyber warfare, asymmetrical warfare, irregular warfare, command and control.

<table>
<thead>
<tr>
<th>REPORT DATE (DD-MM-YYYY)</th>
<th>REPORT TYPE</th>
<th>DATES COVERED (From - To)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>AUTHOR(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alanis, Oscar, Major, United States Marine Corps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>USMC School of Advanced Warfighting Marine Corps University 3070 Moreell Avenue Quantico, VA 22134-5068</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DISTRIBUTION AVAILABILITY STATEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlimited</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SUBJECT TERMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber superiority, cyber warfare, asymmetrical warfare, irregular warfare, command and control.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SECURITY CLASSIFICATION OF:</th>
<th>LIMITATION OF ABSTRACT</th>
<th>NUMBER OF PAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unclassified</td>
<td>UU</td>
<td>23</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAME OF RESPONSIBLE PERSON</th>
<th>TELEPHONE NUMBER (Include area code)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marine Corps University / School of Advanced Warfighting</td>
<td>(703) 432-5318 (Admin Office)</td>
</tr>
</tbody>
</table>
FUTURE WAR PAPER

Cyber Superiority: Overcoming Strategic and Operational Vulnerabilities in Future War

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF OPERATIONAL STUDIES

Author

Major Oscar Alanis, USMC

AY 2013-14

Mentor: Dr. Gordon Rudd, Ph.D.
Approved: [Signature]
Date: 28 MAY 2014
DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE SCHOOL OF ADVANCED WARFIGHTING OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.
From the time David defeated Goliath by slinging his stone until now, history is rich with examples of technological advantages being critical to winning conflicts. The side that can take advantage of technological advances by properly integrating them into relevant operating concepts tends to win. Over the past few decades, the Department of Defense (DoD) has integrated the cyber domain into all of the warfighting functions.\(^1\) Cyberspace operations represent the potential to gain significant technological advantage.\(^2\) Throughout history, military forces have worked to establish superiority in each of the warfighting domains to win wars. Therefore, establishing cyber superiority will be necessary to win future wars.

Should the DoD fail to dominate within cyberspace, a commander could be placed in a significantly disadvantageous position. While providing many advantages, the DoD's integration of the cyber domain into all of the warfighting functions may develop into significant strategic and operational vulnerabilities.\(^3\) The DoD recognizes the risks of integrating cyberspace into the warfighting functions. According to a redacted copy of the 2006 National Military Strategy for Cyberspace Operations, “The DoD's reliance on cyberspace renders this domain an avenue of exploitation for adversaries to gain strategic, operational, and tactical advantages over the U.S.”\(^4\) In that regard, one could make an argument that the DoD may become over-reliant on the cyber domain to enable operations in the physical domains. If the United States military is unable to establish cyber superiority, its overreliance on cyberspace creates significant vulnerabilities that may prevent the United States from winning future wars.

There are a number of difficult issues in gaining and maintaining cyber superiority. The first is that cyber superiority is not adequately defined. Another issue is an argument of whether war can exist solely in the cyber domain. A third issue is how the DoD's emerging overreliance on the cyber domain creates a number of strategic and operational vulnerabilities that will vex
the most savvy operational planner. Further, weaker states will likely be able to affect the United States more in the cyber domain because of how the DoD has embedded the domain into each of the warfighting functions. Finally, gaining and maintaining cyber superiority will be difficult because of unclear command and control issues, the ambiguity of activity within the domain and the time needed to shape the domain for future operations.

To gain a useful advantage, the DoD will need to take both offensive and defensive actions to establish both general and local cyber superiority. The actions do not need to be limited to the cyber domain. In fact, actions in the other domains can and should be mutually supporting aspects of a campaign in a future war. The real value of the cyber domain is its contribution to the overall combined arms effect that the DoD can bring to bear on an adversary in achieving policy objectives.

LACKING CLARITY IN THE DOMAIN

The DoD has not clearly defined cyber superiority. A current definition is “The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary.” This definition is inadequate and creates more questions than it answers. What this degree of dominance looks like both in the physical and cyber domains remains unclear. The DoD’s current Cyber Operations Joint Doctrine, JP 3-12 remains classified. Without transparency in the doctrine, the DoD will not benefit from the ideas that many without access could provide. The Air Force’s cyber doctrine does indicate that a commander must articulate the degree of dominance. In some respects, the Air Force is providing its commanders with some measure of flexibility. The Joint definition is also silent about whether the dominance should be general or local. The DoD should, therefore, clarify
what cyber superiority might look like so that it can retain any advantages the cyber domain provides. Otherwise, significant confusion will remain about what cyber superiority is and how to best employ resources within the cyber domain in future wars.

A concept that is adding to the confusion is the idea of war within the cyber domain. Much is currently being written about the subject of an impending “cyber war”, “a cyber Pearl Harbor,” or “cyber 9/11”. It is unlikely that cyber war will take place because cyber war cannot exist in the traditional sense. If one subscribes to the notion that war is only as a continuation of policy with its inherent violence to accomplish policy objectives, then cyber war in isolation cannot exist. Violence within this manmade domain is not possible. There is a current debate whether violence and lethality are inextricably linked. Nonetheless, the DoD does not appear prepared to change how it views the nature of war.

A campaign within the cyber domain in conjunction with efforts in the physical domains is possible. One must not disconnect actions within the cyber domain from their relationship to efforts in the physical domains. An action within cyberspace must support a higher purpose. Cyber domain campaign goals will likely be shaping actions for the other domains or they might be for intelligence gathering. Activities conducted through the cyber domain should ultimately support achieving the country’s policy objectives through one of the physical domains.

WHERE AN OVERRELIANCE ON THE CYBER DOMAIN CREATES STRATEGIC AND OPERATIONAL VULNERABILITIES

As leaders consume information from intelligence summaries or operations orders, they must be able to trust that the information is truthful and relevant. Through the cyber domain, belligerents may be able to disrupt situational awareness and decision-making. As the DoD continues to integrate cyberspace into combat operations, an adversary could modify critical
intelligence reports, common operating pictures, or issue erroneous orders. Adversaries might have the ability to directly affect a commander’s thinking in ways not previously possible without elaborate deception efforts. While an adversary accessing a critical operation order might be undesirable, a more significant danger is if an adversary modified a critical file enough to retard or alter a commander’s decision, causing him or her to make an erroneous decision or delay a critical one.

Another example of an overreliance of the cyber domain is that many current and planned weapons systems rely on computers and associated technologies to function properly. For example, an infantryman on the ground can now make in-flight course corrections of smart munitions using a combination of GPS, radio and computer technologies. The results are that he can now destroy individual targets with minimal collateral damage and fewer resources. Additionally, the munitions expenditures and maintenance requirements can be tracked and collated by higher headquarters for trends analysis and improve logistical efforts. Specifically, the F-35 Joint Strike Fighter is being developed with what is called an Autonomic Logistics System which will provide aircraft health to a network of maintainers. The cyber domain enables the DoD to perform these functions in near real time. Should an adversary gain the ability to affect how our weapons systems function, the loss of confidence in certain weapons systems in the future would place a commander at a disadvantage. The process for a commander or his combat forces to regain confidence in a weapon during combat could delay decisive action. Weapons malfunctions could also increase the potential for collateral damage. A precision weapon striking an unintended target could lead to strategic pressure on the United States to withdraw from a conflict prematurely.
The DoD also relies greatly on outside partners to provide critical support functions. A way to counter the DoD's technological might is to target the soft underbelly of industry partners. More specifically, weaker states can now take advantage of targeting critical DoD capabilities at low cost. According to strategist Joseph S. Nye, "[D]ependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by non-state actors."\(^{10}\)

A way to target industry support partners is to exploit their computer networks as a means to access DoD networks or glean operational intelligence. Adversaries may try to attack the supply chain outside of the DoD in an effort to disrupt the flow of resources or they may be able gain a better picture of U.S. operations by monitoring partner networks. Leading cyber analyst Martin Libicki believes that, "The indirect effects might be greater if a cyber attack caused a large loss of confidence...."\(^{11}\) Thus, the overreliance on the cyber domain creates strategic, and operational vulnerabilities for the DoD.

The vulnerabilities would apply to both regular and irregular war. Because the DoD would use the same operating concepts and resources for both regular and irregular war, the vulnerabilities would apply to both contexts. The U.S. military would be more vulnerable during irregular war because most adversaries who are weaker states and extremist groups will not have integrated the cyber domain into their operations to the degree the DoD would; thus, they would not be subjected to the effects of cyber weapons as much as the DoD would. In that regard, a weaker adversary could use an asymmetrical advantage against the United States for little relative cost.

Some countries, which have integrated the cyber domain into their critical infrastructure and military operations, have taken measured steps to protect themselves more than the United
States has. China in particular has established a network configuration that allows them to isolate themselves from the Internet during a conflict. This bold action can be easily accomplished by authoritarian regimes. The United States has not implemented this strategy because it has the potential to legitimize authoritarian governments’ censorship of the Internet. Thus, this condition places the adversaries at an asymmetrical advantage over the United States. As Nye writes, “The largest powers are unlikely to be able to dominate this domain as much as they have other [domains] like sea, air, or space.” This asymmetry may prevent the United States from winning future wars.

Weaker countries and extremist groups can exploit the cyber domain because they can afford to buy adequate cyber capabilities to disrupt the United States’ technological advantages. Barriers to entry for weaker nations and extremist groups are and will continue diminishing. Additionally, for-hire criminal organizations and sympathizer groups can offer significant offensive cyber capabilities to weak countries. These factors provide weaker states significant capabilities without significant investment in research and development of offensive cyber capabilities.

A growing vulnerability is that the DoD is placing its cyber eggs into fewer baskets. A trend towards cloud computing and centralized data centers as a strategy to reduce costs and improve security is something that may continue in the coming years. In some respects, this action makes business sense and addresses some security concerns. The implication is that an adversary could cripple DoD capabilities by striking a centralized cloud computing facility. Should the DoD continue centralizing cyber resources due to budgetary concerns, potential adversaries could attack via the cyber domain at relatively little cost or risk.
REASONS GAINING CYBER SUPERIORITY IS DIFFICULT

The first reason establishing cyber superiority will be difficult is because there is not a single entity within the United States responsible for defending the U.S. cyber domain. From an operational design perspective, the Department of Defense is limited in its ability to establish general and local cyber superiority to properly defend the country within the cyber domain. The issues stem from how the United States presently organizes responsibility for protecting computer networks supporting critical resources. There is disagreement about what should be done to remedy the problem.

For example, the U.S. Government is hesitant to direct minimal security requirements for private companies that provide strategic resources or critical infrastructure. Some argue that industry can and should self-regulate and does not require government protection. It is unclear if industry will do so. According to Nye, “Firms have an incentive to provide for their own security up to a point, but competitive pricing of products limits that point. Moreover, firms have a financial incentive not to disclose intrusions that could undercut public confidence in their products and stock prices.”

Others argue the Department of Defense has an obligation to defend all of the United States in cyberspace just as it would in the other warfighting domains. In a recent Joint Forces Quarterly article, David Hollis of U.S. Cyber Command suggests that if the United States were physically invaded, the DoD would not just defend New Jersey. The DoD is responsible for defending the whole country. His argument centers on the idea that the DoD should take a larger role for defending the U.S. cyber domain. It is unclear where the limits should be. One has to wonder if an open society like the United States can avoid ceding large portions of a
warfighting domain while protecting personal privacy. The United States manages to balance the requirement for security and living in an open society in the other warfighting domains. It remains to be seen if the same can be done in the cyber domain.

There is a paradox in the cyber domain: On the one hand, one can traverse the domain from one end of the planet to the other in seconds; on the other, it can take a significant amount of time to shape the environment to achieve a cyber effect. This paradox makes it difficult to design operations that can raise a commander's comfort level to know if his or her cyber efforts are achieving the desired effect.

Another reason achieving cyber superiority will be difficult is that the DoD may not know if it has achieved cyber superiority. Nevertheless, it must be able to thrive in an environment of ambiguity. Operating without perfect knowledge of the environment is not new. Only in recent history has the DoD tried to assert that technology would eliminate obscurity and uncertainty. The absence of adversary activity may be enough to declare local cyber superiority, but is probably inadequate to declare general cyber superiority.

Another reason establishing cyber superiority will be difficult is how one must defend in the cyber domain. Most defensive methods require access to all of the data that traverses the networks. This requirement causes concern among privacy advocates. While there is potential for abuse, the volume of data on any DoD network at any given time normally precludes an individual from doing so. Computers and software tools within the cyber defense organization will continue to scan data to determine whether threat conditions exist. Finding a threat in network traffic must be done based on known vulnerabilities or established heuristics. The process is normally slow and reactive. Thus, an attacker holds an important advantage—time.
Interpreting intent in cyberspace is also difficult. Espionage and intelligence gathering by nation states is generally viewed as normal behavior. However, sabotage and employing “cyber weapons” are not generally viewed as acceptable behavior outside of declared conflict. Gaining access to a computer network for intelligence gathering purposes and employing cyber weapons involves the same kinds of steps. Someone must break into a network device, establish an electronic foothold, exfiltrate data, or install a software program. Nye makes the point that it will be some time before international norms are established for intrusions for the purposes of espionage and intelligence preparation of the battlespace.\textsuperscript{18} This ambiguity between normal espionage and using a cyber weapon could provide the DoD with maneuver and decision space.

Another reason establishing cyber superiority is difficult is how much the strategic, operational and tactical levels of war overlap within the cyber domain. The overlap presents military commanders with span of control problems that are difficult to determine with accuracy or relevance to what a military commander’s area of influence and area of interest should be. The decision to determine these areas is not as simple as looking at a map and making a decision based on experience. These decisions will be important in future operations as commanders will need to know what action within the cyber domain is within their authority. It is unlikely that these kinds of decisions will be resolved in the near term largely because commanders at all levels are reluctant to yield control of assets and capabilities.

There is an element of time in the cyber domain that is different than the physical domains. In identifying adversarial cyber vulnerabilities, a warfighter must correctly identify from a nearly countless combination of software and hardware systems to determine which, if any, cyber weapons can be employed. This process is more time consuming than traditional reconnaissance and intelligence functions in the physical domains due to the volume of possible
options. The process is also dynamic because an adversary can update software and hardware configurations potentially changing the attack vectors. In that regard, a cyber weapon may be useful before crossing the cyber line of departure only to be made inert if the adversary patches a vulnerability in his system just prior to execution.

The DoD must be able to accurately predict future adversaries. While only so many potential foes have the kinds of capabilities that would be subject to cyber attack, the scope of work inhibits the DoD’s ability to have prepositioned offensive cyber capabilities in a resource constrained environment. The DoD will have to assume a level of risk that is different from the physical domains because of the time required to develop the conditions to use offensive cyber weapons.

**CYBER SUPERIORITY MIGHT LOOK DIFFERENT**

Since the cyber domain is manmade, cyber superiority will look different from what commanders and planners are accustomed to seeing. It is nearly impossible to provide any assurance that superiority has been established. In many respects, the validation of cyber superiority will be contrived. Several authors have proposed what cyber superiority might look like. The problem with the models is that they focus solely on military networks and are largely silent on how the DoD would or should defend the remaining American networks. Perhaps general cyber superiority should be reserved for networks outside of the DoD’s responsibility whereas local superiority would be the DoD’s purview. There have been some efforts to gain the cooperation of critical infrastructure providers to improve defenses in coordination with the Department of Homeland Security. Unfortunately, there are no effective enforcement mechanisms associated with this effort.
It is natural to look to the efforts in the other domains to try to frame what cyber superiority might be. In the air domain, combatants have reduced adversary aircraft and air defenses or they have not. Similarly on the land and sea, the adversaries’ capabilities have been reduced to a degree where the United States can accomplish a desired task with minimum disruption from an adversary. Conversely, Air Force Major Merna Hsu, while at the School of Advanced Air and Space Studies wrote, “Except for its hardware infrastructure, cyberspace is intangible to human senses. Activity is inherently veiled, masked, or otherwise obscured by cyberspace’s vastness and dynamic boundaries. Like the maritime environment, it may be impossible to discern all activity, much less identify and halt hostile operations, without negating all activity, such as through an EMP blast or nuclear strike over a physical locale.”20 In cyberspace, the process of establishing superiority is not clean.

Superiority in the cyber domain manifests itself as a commander’s confidence in the information his fighting force is operating under. She goes to add how difficult it will be to have any assurance superiority is achieved by writing, “[T]here must be verifiable proof that the data, was uncorrupted and unhindered (e.g., temporarily intercepted for file copying, then re-transmitted) from the point of transmission to receipt.”21 This level of proof is a fairly tall order, but she is correct. Thus, cyber superiority may exist only in the mind of the commander because he or she will not be able to assess an adversary’s cyber capabilities; he or she will only be able assess his own.

ESTABLISHING CYBER SUPERIORITY

There is an instinctive desire to have both general and local cyber superiority. However, both contexts may not be achievable or necessary because of the paradox of being able to reach an opponent at near light speed and not really observing the effects of a cyber weapon for some
time. Nevertheless, operational planners will need to clearly identify what the conditions for both general and local cyber superiority are and describe how they may be achieved. Otherwise, military forces will be left wondering what the degree of dominance the current Joint definition suggests.

In establishing air, naval, or fire superiority, a military task force would need to take both offensive and defensive measures. Establishing cyber superiority would require the same. Offensive cyber operations would be necessary to destroy or degrade adversary cyber capabilities. The activity should not be limited to using only offensive cyber weapons. It may be more beneficial and timely to use kinetic weapons to destroy or degrade an adversary’s cyber capabilities.

There is a question of resources that must be addressed in offensive cyber operations. The DoD must resolve where the appropriate level of authority for the use of a cyber weapon resides to achieve the greatest combined arms effect. There is an opportunity cost if the level is too high in the chain of command. For example, a tactical commander who quickly uncovers a requirement to employ a cyber weapon, but is unable to do so in a timely manner may surmise that weapon is not worth the effort if the designated target is no longer vulnerable. However because many cyber weapons are of one time use, weapons release authority normally resides high in the chain of command. A Catch-22 exists. Therefore, the DoD should develop a continuum of weapons release authority for a tactical commander in order to realize the potential combined arms value cyber weapons could provide.

Policy makers will need to determine whether cyber weapons are just another weapon or a game changer that have the potential to quickly escalate a conflict. It is understandable that senior decision makers want to retain release authority of cyber weapons due to current political
considerations. If the DoD is going to be allowed to use these weapons in the future, military leaders and planners must know what is within the realm of the possible in order to begin shaping operations.

Similar to naval warfare, the DoD will need to start early to create alternatives in the cyber domain. Since it takes a significant effort to identify vulnerabilities, operational planners will need to begin shaping actions early. Otherwise, a commander will not have set the conditions adequately to achieve an effect through the cyber domain prior to a crisis.

Defensive cyber operations might take several forms. The first would be moving more routine traffic to classified networks. It is not necessary to have only classified material on these networks. While this action does not address the inherent vulnerabilities in software, it does reduce the ability of adversaries to access DoD information by introducing another layer of security. This recommendation may be difficult to implement in the near term, but the long-term benefits can only be advantageous to the DoD.

Another defensive action the DoD could take is to mandate network security requirements of trusted vendors. This recommendation may become part of the cost of doing business with the DoD. These trusted vendors would be subject to similar inspections for security procedures comparable to DoD networks. Some vendors are already subject to this requirement. However, this recommendation may need to be expanded to more routine activities so it would become more difficult for adversaries to exploit security vulnerabilities in supply chain providers.

The DoD should invest in designing and building better defensive hardware and software for military use only. The DoD certainly benefits from economies of scale by buying from commercial vendors. However, continuing to do so places the DoD at the mercy of vendors
whose motivation normally revolves around profit and loss statements. The DoD could invest in software development exclusively for military networks as it invests in aircraft manufacturing and ship building. In fact, most cyber warfare techniques originate in the private sector for criminal purposes. The DoD can learn a great deal from actively monitoring criminal behavior in the commercial networks. These techniques are normally the same ones used for military purposes by nation states. The expense will be significant, but the risks of relying on commercial software to operate in the cyber domain exceed the benefits.

The DoD professes a defense in depth strategy in the cyber domain.²⁵ If this is the case, it is incumbent for the DoD to develop a means of an immediate counterattack against an adversary’s efforts. Otherwise, the DoD will continue to be subjected to an adversary’s effort to erode the DoD’s cyber defenses. An immediate counterattack should include something more than a simple block of an IP address. A counterattack will necessitate an offensive cyber effort to have any useful effect.

The DoD should be prepared to regain the initiative against any successful attack in the cyber domain. It should be able to string together enough small victories in the correct sequence to achieve an overall victory.²⁶ Stringing together small victories is harder than it seems because it is difficult to actively defend in the cyber domain.

A policy solution, which may contribute to general cyber superiority, could be a mobilization effort within the cyber domain. Should the United States become involved in a major war, it could establish a national security policy for critical infrastructure and key vendors that would place the defense of their networks under the DoD’s purview. This temporary step would help mitigate the risk at the strategic level and contribute to general cyber supremacy. The
DoD would naturally need to develop doctrine for defending U.S. private networks during times of crisis or verified cyber attacks.

A solution could be broader international agreements of acceptable behavior within the cyber domain. Nye believes there are inherent risks in this option. He writes, “Such efforts could actually reduce national security if asymmetrical implementation put legalistic cultures like the United States at a disadvantage compared to societies with a higher degree of government corruption.” The prospect of putting the United States in either an actual or perceived disadvantage would be difficult to implement. Although unpopular, such agreements may ultimately place the DoD in an advantageous position in the end, as it would then be able to employ the full potential of its military technological advantages.

Another solution would be developing operating concepts that do not require massive amounts of computer networks. Since the cyber domain is only a supporting domain, the DoD should be able to function at critical moments without access to the cyber domain. It is unrealistic to expect the DoD to cede the domain. Nevertheless, the DoD should be able to operate for sustain periods in a highly contested cyber environment.

Training will be a critical component to achieving this operational capability. This idea is easier said than done. There tends to be a hesitancy to negatively impact a major training exercise due to a compromised cyber domain. When resources are limited, the hesitancy is natural. Nevertheless, the DoD will need to balance the requirement to complete an exercise as scripted with providing realistic training experience to the training audience. Realistic training can provide the DoD resilience in future wars.

The DoD should develop doctrine for validating and authenticating critical data during critical moments of a conflict. It may be time to begin authentication procedures in other
aspects of contingency operations that were previously reserved for nuclear weapons. This recommendation may seem cumbersome. However compared to the loss of confidence in the data that a key decision makers needs, it is less costly.

CONCLUDING THOUGHTS

The DoD has many issues within the cyber domain that it must overcome to succeed in future wars. An asymmetry exists and will continue to exist because the United States relies heavily on cyberspace not only for defense needs, but also for everyday functions. Militaries in developing countries are not vulnerable to the degree the U.S. military is. This is where potential adversaries have an advantage. They can use cyber weapons to affect U.S. operations and strategic goals. Conversely, the use of cyber weapons on them may have limited effect. Other countries such as China have established national security infrastructure to protect themselves during a time of conflict. If these asymmetries and vulnerabilities are not properly resolved, the United States will likely remain in a disadvantageous position relative to its adversaries in the cyber domain and may find it more difficult to prevail in future wars.
Notes

13 Nye, 35.
14 Nye, 20.
16 Nye, 28.
18 Nye, 32.
21 Hsu, 47.
24 Hsu, 52.
26 Leonhard, 103.
27 Nye, 34.
Bibliography


Cartwright, James. USMC, Vice Chairman of the Joint Chiefs of Staff, *Memorandum, Joint Terminology for Cyberspace Operations*, Department of Defense, Washington, DC.


Hersh, Seymour M. “The Online Threat: Should we be worried about a cyber war?” *The New Yorker* (November 1, 2010): 44-55.


Stone, John, “Cyber War Will Take Place!” *Journal of Strategic Studies,* Vol. 36, Iss. 1, 2013, 100-108.


