8

NAVAL WAR COLLEGE
Newport, R.I.

Operational Impacts of a Contested Cyber-Environment

The need to assess and mitigate the impacts of a hostile cyber-environment on the operational capabilities and combat potential of a Joint Task Force or Combatant Command

by
LCDR Josh Fagan, USN

5/13/2013

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy

Signature:_____

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
20 - 05- 2013	FINAL	

Operational Impacts of a Contested Cyber-Environment

The need to assess and mitigate the impacts of a hostile cyber-environment on the operational capabilities and combat potential of a Joint Task Force or Combatant Command

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LCDR Josh Fagan, USN

Paper Advisor (if Any): CDR Chad Piacenti, USN and LtCol Larry Floyd, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES
A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The global cyber environment is quickly evolving and growing. U.S. military forces have become significantly enabled and dependent on the complex software systems and computer networks that comprise this landscape. Much has already been written recently on the concept of applied operational art in cyberspace; on the operational effects on space, time and force that can be achieved through the direct application of offensive and defensive cyber tools. This paper considers, instead, the indirect impact of hostile activities in cyberspace on the combat potential of a commander's forces at an operational level. This paper highlights the impacts of degraded peripheral cyber-equipment and software on a unit's ability to conduct their tactical missions, and how that may impact the operational plans of higher echelon commanders. Finally, this paper offers a potential mechanism that commanders can employ to assess and mitigate these potential vulnerabilities while they prepare for military operations in a world that is growing more interconnected, dynamic, and dependent on increasingly complex cyber-systems.

15. SUBJECT TERMS
Anti-access, Area Denial

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		20	19b. TELEPHONE NUMBER (include area code) 401-841-3556

ABSTRACT

Operational Impacts of a Contested Cyber-Environment

The global cyber environment is quickly evolving and growing. U.S. military forces have become significantly enabled and dependent on the complex software systems and computer networks that comprise this landscape. Much has already been written recently on the concept of applied operational art in cyberspace; on the operational effects on space, time and force that can be achieved through the direct application of offensive and defensive cyber tools. This paper considers, instead, the indirect impact of hostile activities in cyberspace on the combat potential of a commander's forces at an operational level. This paper highlights the impacts of degraded peripheral cyber-equipment and software on a unit's ability to conduct their tactical missions, and how that may impact the operational plans of higher echelon commanders. Finally, this paper offers a potential mechanism that commanders can employ to assess and mitigate these potential vulnerabilities while they prepare for military operations in a world that is growing more interconnected, dynamic, and dependent on increasingly complex cyber-systems.

Introduction

> ***The importance of properly evaluating the factor of force in planning for and conducting a campaign or major operation cannot be adequately emphasized. Yet no task is more difficult than correctly evaluating the capabilities of one's forces, both before and during combat…Operational commanders and their staffs should always face realities (when assessing their own forces' combat potential), no matter how unpleasant; otherwise, the planned campaign or operation is bound to fail.***[1]
>
> ***-Dr. Milan Vego***

Full spectrum situational awareness is one of the most important tools that a commander can have while conducting operational planning. In order to have accurate situational awareness of the true combat potential of their assigned forces, Geographic Combatant Command (COCOM) and Joint Task Force (JTF) Commanders are in need of a tailored, in-depth (unit-level and system-wide) cyber-vulnerability assessment and operational impact analysis capability. This aspect of the operational force available to a commander is not currently addressed or analyzed adequately because history and experience have not yet exposed its importance. Although our entire military force has recently begun a revolutionary transformation in equipment, tactics, doctrine, and training that revolves around the incorporation and dependence on cyberspace; the true nature of the cyber-environment has been greatly misrepresented by our experiences in the relatively calm and cooperative commercial world of the consumer, and by our recent military conflicts against enemies who held no significant power against our computer networks or cyber-enabled capabilities.

[1] (Dr. Vego 2009), (III-46)

Our current military force is being increasingly shaped by commercial cyberspace, while our forces have yet been forced to operate in an environment where our ability to conduct military operations through cyberspace has been significantly challenged. Meanwhile, the cyber-landscape has become increasingly complex, the power and proliferation of cyber-weapons has exploded, and our military forces have become extremely enhanced and dependent on cyber-enabled and net-centric capabilities[2]. As stated in the Department of Defense's Cyberspace Policy Report in 2011, "Cyberspace is a critical enabler to Department of Defense (DoD) military, intelligence, business and, potentially, civil support operations; While the development and integration of cyber technologies have created many high leverage opportunities for DoD, our increasing reliance upon cyberspace also creates vulnerabilities for both DoD and the Nation[3]." This dependence has been forged primarily in an entirely permissive global cyber-environment, has demonstrably allowed for improved efficiency and effectiveness, but also serves as a potential critical vulnerability that enemy forces can exploit in future conflicts.

Throughout the recent evolution towards net-centric warfare, the U.S. has not faced a significantly hostile cyber environment while conducting or preparing for military operations. Concurrently, the complex attack surface of the military network, and the sophistication of cyber-infiltrations and attacks have all continued to grow. Meanwhile, the majority of effort in cyber offense and defense has been geared towards the goal of maintaining our ability to operate at will in the cyber domain, otherwise called "cyber dominance." Recent paradigms have shifted,

[2] (VADM Cebrowski 1998)
[3] (Department of Defense 2011)

however, and it is now understood that it must be assumed that in spite of our best defenses, our cyber networks *will* be compromised to some extent[4,5].

The U.S. military trains flight crews to execute missions in spite of aircraft equipment degradations, we train artillery units to operate while being attacked by chemical weapons, and we prepare our special operations forces to conduct operations autonomously in environments where we do not hold military superiority. Large-scale joint military exercises and operational plans incorporate these and other impacts of the fog and friction of war. The kinetic actions of the enemy, the environmental and weather effects on communications and combat equipment, even the operational impacts of fatigue and morale on the combat potential of warfighting units, are all considered in the development of operational plans and exercises.

Recently, the military has even begun to prepare for hostile cyber-attacks on critical networks through in-depth cyber-exercises and increased efforts at cyber-defense. Unlike most other aspects of warfare that might impact the joint force's ability to achieve military objectives on the battlefield, cyberspace still seems to be perceived as a primarily parallel and separate domain. This seems to exist in direct conflict with the reality that today's military forces are becoming increasingly net-centric and software dependent.

The potential operational impacts of a contested cyber-environment, and the resultant effects on warfighting units and joint forces, are not adequately analyzed or incorporated into operational plans and exercises. While current cyber-exercises are becoming better at identifying cyber-vulnerabilities resident in our networks, and of discovering ways to strengthen our cyber-defenses against such attacks, the effects of these compromised and degraded cyber-systems on a

[4] (Mick 2010)
[5] (Yasin 2012)

warfighting unit's ability to conduct their mission effectively and efficiently is not tested or adequately analyzed.

One final complication is that unlike other domains, the possibility of achieving true cyber-dominance during any military operation seems to be becoming increasingly difficult, if not impossible. This reality, combined with the U.S.' growing dependence on sophisticated networks and cyber-systems, along with the global proliferation of increasingly powerful cyber-tools, makes the need to prepare for a contested and hostile cyber-environment all the more urgent. Our increasingly networked systems, platforms, and peripheral computers WILL be compromised in future military operations. COCOM Commanders need an organic capability to conduct in-depth cyber vulnerability and threat analyses in order to assess the true combat potential and effectiveness of combined joint forces operating in a hostile cyber environment.

The Indirect Cyber-Threat

> ***I don't think that we would think that we could keep spies out of our country. And I think we've got this model for cyber that says, 'We're going to develop a system where we're not attacked.' I think we have to go to a model where we assume that the adversary is in our networks. It's on our machines, and we've got to operate anyway.***[6]
>
> ***-Dr. James S. Peery, director of the Information Systems Analysis Center at Sandia National Laboratories, in testimony to Congress in 2012***

[6] (Donohue 2012)

The operational impacts on traditional warfighting capabilities through indirect and peripheral cyber exploitation are becoming increasingly significant[7]. The enemy may be prevented from completely disabling or even significantly degrading our front line weapons systems during a conflict. They may, however (and recent experience shows this to be likely), be able to significantly disrupt our "softer" nodes in cyberspace; our printers, email systems, peripheral software programs, etc. As cyberspace expands, as more commercial cyber-systems become part of normal military operations, the collective vulnerability exposed by these "soft" nodes becomes more significant.

Even when hostile cyber-tools and weapons are not engineered or directed specifically against military weapons systems and operations, the effects can be significantly disruptive. A Microsoft Windows virus inadvertently infected the mission planning software systems utilized by certain French Air Force squadrons, and led to a temporary grounding of their fleet of fighter aircraft[8]. A virus originally designed to target commercial video game systems infected the U.S. Predator drone fleet, exposing a potential Operational Security (OPSEC) vulnerability in the complex system even while the aircraft were conducting sensitive combat operations in Iraq and Afghanistan[9,10]. Computer workstations inside the Pentagon were recently discovered to be infected by hidden viruses[11], and the incorporation of military cloud computing and mobile media systems will only serve to increase the certainty of intentional and inadvertent cyber-infiltration across the entire military network[12].

---

[7] (Whitehead 2013)
[8] (Willsher 2009)
[9] (Schactman 2011)
[10] (AP - Associated Press 2011)
[11] (Gertz 2012)
[12] (Kenyon, DOD still wrestling with scalability, security for wireless networks 2011)

While future conflicts may one day be waged largely or exclusively through cyberspace, today's wars are still fought and won through the application of conventional kinetic warfighting power. Alarmingly, however, today's conventional warfighting capabilities and platforms rely increasingly heavily on integrated and peripheral computer networks and systems. Today's Joint Force is ill-prepared to adequately assess the cyber vulnerabilities of its warfighting platforms in an evolving cyber threat environment, defend those systems against increasingly sophisticated and subtle infiltration, or to analyze the potential operational impacts that indirect cyber-attacks may have on a Commander's ability to employ combat power.

In today's software-enabled network-centric military, the impact of the cyber-environment on the mission effectiveness of military units and commands is often now as real as the physical effects of weather and the natural environment. We have developed the ability for much of our combat power to be sustained through harsh weather, in day or night conditions, and in most physical environments on the planet. We have achieved this by fully accounting for the physical environments we operate our forces in, and by designing our equipment and doctrine around the limitations imposed by weather, terrain and contact with the enemy. Natural and environmental barriers to victory or efficiency on the battlefield are mitigated through detailed operational planning that shapes the composition and tactics of our joint force in response to these external influences.

A Commander, in order to effectively leverage the forces under their command, must know the full combat potential of each element, and must also understand how that potential is affected by external environmental and enemy factors. While planning an operation in the mountains of Afghanistan, for example, a commander must understand that the operational potential of the helicopter units under his charge will likely be degraded by the high altitude and

temperatures of the coming summer season. This will potentially affect the time and force required to execute air mobility operations, the potential radius of space in which operations can be conducted, and would likely increase the logistics and refueling requirements for long range strike operations.

In 2012, it was discovered that several Chinese-manufactured computer chips then being used throughout the Department of Defense in military weapons systems had been deliberately modified with a nano-scale "backdoor" accessibility feature that could be exploited by hackers to modify or disable the software running on the chips themselves[13]. In today's and tomorrow's net-centric joint battlefields, a commander will increasingly be required to have situational awareness of the potential impact of a hostile cyber environment on the combat potential of the units involved in any operation. In planning for a joint defense of Taiwan against a Chinese invasion, for example, a commander should be provided with the situational awareness that an allied ISR capability provided by a drone contractor relies heavily on a commercial control and data relay software system that is less than ideally secure. While planning operations against a military force that has demonstrated the ability and will to degrade similar systems, a good operational planning staff and commander armed with this information should prepare for the possibility that this system will become compromised, should allow for sufficient flexibility in the operational plan to execute the mission without ISR coverage, prepare for ISR services to be augmented by additional distinct forces, and to train their forces ahead of time to operate with this specific degradation.

The aggregate cyber-attack surface and vulnerability windows provided by the military's reliance on commercial software systems make it increasingly difficult to assess the potential

[13] (Reed 2012)

tactical and operational impacts of a hostile cyber environment. While completely securing all open ports and points of cyber-access may be impossible in today's military, especially with the proliferation and dependence on peripheral cyber-equipment on normal operations[14], it is becoming all the more relevant to train and assess our forces in executing their missions with these systems degraded or disabled. While the cyber vulnerabilities of a remotely piloted drone unit may seem intuitive, or the defense of a critical piece of software that manages network-wide IFF position reporting may already have critical attention directed towards it, the increasingly ubiquitous nature of software-enhanced and software-dependent systems within every military unit exposes a potential soft spot in our defensive perimeter as well as our ability to project offensive power.

A fixed wing cargo and mid-air refueling unit, for example, may have a significant reliance on a specific software program, a suite of computer programs, or a set of information technology (IT) products that enables them to do their pre-mission planning and coordination extremely effectively and efficiently in an uncontested cyber environment. If, however, a relatively unsophisticated virus is introduced into their printer network that severely degrades their ability to print out mission planning products and drop-zone (DZ) area charts for their flight crews, their overall mission effectiveness may be impacted. Likewise, their ability to execute resupply/refuel missions with the same level of efficiency, accuracy and timeliness may also be degraded. With a more limited level of high resolution DZ imagery, crews on the ground may be exposed to greater risk of loads delivered in less than ideal locations. Similar types of indirect mission-degrading effects are less likely to garner attention than the potential for direct cyber-

[14] (Freedburg 2013)

attacks on primary critical networks and software systems, but the operational impacts of these degradations still need to be adequately assessed and mitigated by operational planners.

The Need for an Operational Impact Assessment Mechanism for Cyber

Currently, there is no mechanism in place that identifies and assesses the tactical and operational impacts of direct and indirect degradations of the cyber-vulnerabilities of traditional warfighting elements[15]. Current Cyber vulnerability assessment resources are targeted at identifying vulnerabilities to the military network as a whole and mitigating them; not identifying or analyzing how vulnerable a *military unit* is to being operationally impacted by degraded cyber equipment and software[16,17]. Military units are evaluated on their ability to execute combat missions under all potential environmental and physical threat environments they might encounter on the battlefield. They are not, however, widely evaluated or exercised on their ability to support combat operations in this physical environment while simultaneously weathering cyber-attacks leveraged against the full spectrum of their computer-enabled infrastructure. Current cyber-exercises focus almost entirely on cyber-warfare and cyber-defense[18,19].

While the effect of hostile cyber-warfare on a commander's ability to utilize the cyber domain is critical to analyze, the impact of hostile cyber-operations on the commander's non-cyber forces is relatively neglected. This effect on the commander's operational function of force can, and should, impact a commander's operational plans. A commander should be able to assess which cyber systems and networks are currently utilized by assigned units to conduct their

[15] (Lt. Col. Lanham 2012)
[16] (U.S. Army 2010)
[17] (Kenyon, Army cyber pros pitch in with network evaluation 2012)
[18] (Montalbano 2011)
[19] (TSGT MCNabb 2012)

missions, and how the loss of functionality or reliability of these systems impact the unit's ability to conduct tactical operations.

How much would a unit's planning cycle time and operational response time be impacted, for example, in a degraded cyber-environment? How would each unit's ability to employ certain weapons or achieve certain tactical effects be degraded? How much risk would now be introduced into operations as units are presented with degraded or non-existent cyber-enabled imagery, intelligence, and planning products? How does a degraded cyber-environment impact a unit's ability to communicate or relay data to the joint force on secure channels? For each of these cyber systems identified, are there alternative or backup capabilities identified and exercised? Do flight crews train on inputting flight plans, cryptography codes and weapons release coordinates manually? Do ground and flight crews train on utilizing paper charts – executing missions without access to software or network-based systems? Even if some units or organizations do plan for and practice conducting operations with the aforementioned degradations, there is currently no standardized doctrine or coordinated plan to assess their performance or incorporate the realized potential operational impacts into the calculus that a commander's staff conducts to measure the total combat potential of their assigned force.

The bottom line is that a commander must be given the situational awareness required to balance the appropriate level of military force at the appropriate time and place to achieve operational objectives. The true combat potential of each of the units under their command must be presented in relation to the expected operating environment. Under current paradigms, we risk giving commanders artificially inflated values for the combat potential of the units under their command, as we generally assume that these units will operate at a constant level of performance, regardless of the amount of degradation that may be expected in the cyber-

environment throughout an operation. Every training exercise, even all recent combat experience, furthers this misconception, and has lulled the entire enterprise into complacency.

Recommendations

COCOMs need to incorporate the responsibilities of interfacing with each combat unit and computer system utilized in their AOR or incorporated into potential Joint Operations, analyzing their cyber vulnerabilities, and the potential impact of cyber-security breaches or infiltrations on these systems' mission effectiveness. This analysis then needs to be applied against the current and expected cyber environment that may exist during operations in the AOR (current offensive cyber capabilities of potential enemies and rogue actors, the likelihood of their employment, and current friendly cyber-defensive capabilities and/or cyber-response/repair) and presented to the Commander on a regular basis.

All individual units need to establish cyber departments that will be responsible for assessing the unit's own comprehensive cyber-posture. Cyber departments will be responsible for assessing the unit's functional dependence on cyber systems, identifying and mitigating vulnerabilities, and for providing performance impact estimates of degraded cyber-systems to higher echelon commanders' communications departments (J6). J6 departments will compile all unit analyses, and coordinate with Cyber Support Elements (CSEs) to analyze total force cyber vulnerabilities and potential functional impacts in the expected cyber-environment. CSEs will coordinate with the commanders' intelligence departments (J2) for enemy disposition and provide net assessment of cyber-induced operational degradations to forces to the commanders' operations departments (J3). J3 will incorporate the cyber-induced potential effects into initial

net force operational assessments and periodic Commander's Update Briefs (CUBs) to be provided to the commander.

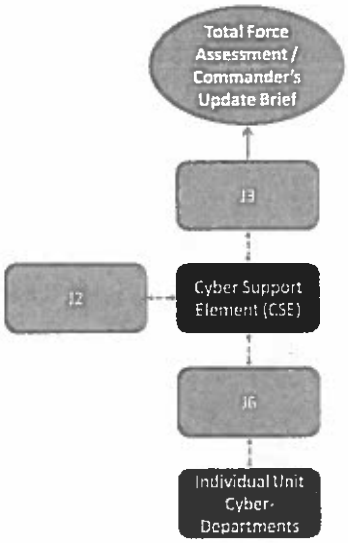

Fig.(1): Proposed Operational Cyber-Vulnerability and Impact Assessment Process Flow

The level of technical proficiency required, as well as the evaluative nature of the cyber-analysis function, may dictate that external "floating" military resources or hired contractors may be required at the unit level for adequate cyber-analysis, or for periodic assessment and training. COCOM and JTF commanders should work with service chiefs and individual units to stress the importance of unit-level situational awareness of the cyber environment, unit-level cyber vulnerabilities, and the potential impacts of a hostile cyber environment on that unit's ability to conduct their mission and support higher level commanders.

Operational exercises should incorporate the types of cyber-degradations that might be expected to occur during combat operations in theater. Units that rely on cyber and software systems should exercise their ability to execute missions with these capabilities degraded or eliminated. The impact of cyber-related degradations on unit and joint force combat potential

should be quantified and recorded in as much detail as possible in order to provide guidance to military leadership that can be used to address and prioritize identified areas of vulnerability. Controlled and engineered cyber-attacks may be able to be developed and incorporated by USCYBERCOM Cyber Support Elements (CSEs) during exercises. Units should be evaluated on how quickly they are able to identify and react to cyber-related mission degradations during ongoing operations, and how effectively they are able to execute assigned mission responsibilities while "fighting through" a degraded and hostile cyber-environment.

Conclusion

> ***So it is said that if you know your enemies and know yourself, you can win a hundred battles without a single loss. If you only know yourself, but not your opponent, you may win or may lose. If you know neither yourself nor your enemy, you will always endanger yourself. – Sun Tzu (The Art of War)***

The potential operational impact of peripheral cyber-attacks on military forces, and individual unit mission effectiveness, is increasing in scope and significance. The total force is becoming increasingly reliant on cyber infrastructure, especially commercial cyber systems. Civilian, government, and military networks are all becoming increasingly complex, more difficult to comprehensively defend, and more critical to normal operations[20]. The number of sophisticated cyber-attacks and exploitations is growing, the cost of entry into cyberspace is low, and the power of cyber-weapons and effects is increasing. In a historic announcement, the United States has recently identified China as a nation-state that is actively targeting American interests and exploiting U.S. vulnerabilities in cyberspace[21,22]. As the global population becomes more

[20] (Donohue 2012)
[21] (Chumley and Waterman 2013)

dependent on cyber-capabilities learned in a relatively permissive cyber environment, the entire U.S. military force will find it more difficult to adapt to operations conducted in a suddenly hostile cyber environment, with compound degradations to critical cyber-systems.

Warfare is not conducted within a single domain; cyber-attack and defense capabilities are only as relevant as their ability to enable a commander to achieve their operational objectives. As long as conventional military forces bear the brunt of responsibility of action in executing operations, cyber must be viewed primarily through the lens of its impact on these forces' ability to wage war. As long as the potential exists for a hostile cyber environment to negatively impact the operational capabilities of military forces, this potential must be thoroughly analyzed and prepared for. In order to adequately balance and manage the forces under their command, joint force commanders need to have full situational awareness on the combat potential of each unit and the force as a whole. Understanding the potential tactical degradations and operational impacts caused by a hostile cyber environment is increasingly important to this overall calculus. This can only be done by establishing the capability for assessing the potential operational vulnerabilities and impacts within a command.

A force will largely wage war in the manner in which it is trained. More realistic training must be incorporated into conventional warfighting exercises. Cyber-exercises should not be limited to cyber-forces. The impact of cyber-attacks on cyber-assets is fairly meaningless without fully assessing what those cyber-degradations subsequently do to the abilities of warfighting military forces to conduct operations.

[22] (Chan 2013)

As technology continues to advance, the landscape of potential military interaction is only going to continue to grow in scope and complexity. Commanders in the future will not only need to become experts on the impact of a hostile cyber environment on the operational capabilities of the forces assigned. A commander will also need to become expert at the evolving nature of the cyber-landscape that their forces will be navigating through in order to conduct both cyber-exclusive and traditional military operations. As the battlespace evolves, a commander will need to evolve their ability to gather intelligence and maintain situational awareness. The recommendations offered in this paper are an example of how a commander may be able to do this.

Bibliography

AP - Associated Press. *Military says virus not directed at drones.* October 12, 2011. http://www.airforcetimes.com/article/20111012/NEWS/110120302/Military-says-virus-not-directed-at-drones (accessed May 12, 2013).

Chan, John. ""Asymmetric Warfare": Pentagon Accuses China of Cyber Attacks and Espionage." *Global Research.* May 9, 2013. http://www.globalresearch.ca/asymmetric-warfare-pentagon-accuses-china-of-cyber-attacks-and-espionage/5334452 (accessed May 12, 2013).

Chumley, Cheryl K, and Shaun Waterman. "Meet China's super-secret military hacking unit." *The Washington Times.com.* February 19, 2013. http://www.washingtontimes.com/news/2013/feb/19/chinese-military-unit-blame-141-hackings-virginia-/ (accessed May 12, 2013).

Department of Defense. "Department of Defense Cyberspace Policy Report." *Defense.gov.* April 2011. http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf (accessed May 12, 2013).

Donohue, Brian. *Experts Tell Senate: Government Networks Owned, Resistance Is Futile.* March 21, 2012. http://threatpost.com/experts-tell-senate-government-networks-owned-resistance-futile-032112/ (accessed May 12, 2013).

Dr. Vego, Milan. *Joint Operational Warfare: Theory and Practice.* Newport, RI: U.S. Naval War College, 2009.

Freedburg, Sydney J., Jr. "Navy Battles Cyber Threats: Thumb Drives, Wireless Hacking, & China ." *Breaking Defense.com.* April 4, 2013. http://breakingdefense.com/2013/04/04/navy-cyber-threats-thumb-drives-wireless-hacking-china/ (accessed May 12, 2013).

Gertz, Bill. "Pentagon Attacked by Computer Virus." *Free Beacon.com.* September 6, 2012. http://freebeacon.com/pentagon-attacked-by-computer-virus/ (accessed May 12, 2013).

Kenyon, Henry. *Army cyber pros pitch in with network evaluation.* May 1, 2012. http://defensesystems.com/articles/2012/05/02/army-cyber-personnel-assist-nie.aspx (accessed May 12, 2013).

—. *DOD still wrestling with scalability, security for wireless networks.* December 23, 2011. http://gcn.com/articles/2011/12/23/dod-wireless-networks-scalability-security.aspx (accessed May 12, 2013).

Lt. Col. Lanham, Michael J. "When the network dies: The Army lacks the battle drills that would help it fight on." *Armed Forces Journal.* December 2012. http://www.armedforcesjournal.com/2012/12/12178431 (accessed May 12, 2013).

Mick, Jason. "NSA Switches to Assuming Security Has Always Been Compromised." *Daily Tech.com.* December 17, 2010. http://www.dailytech.com/NSA+Switches+to+Assuming+Security+Has+Always+Been+Compromised/article20424.htm (accessed May 12, 2013).

Montalbano, Elizabeth. "U.S. Cyber Command Practices Defense In Mock Attack." *Information Week.com.* November 30, 2011. http://www.informationweek.com/government/security/us-cyber-command-practices-defense-in-mo/232200508 (accessed May 12, 2013).

Reed, John. "Proof That Military Chips From China Are Infected?" *DefenseTech.* May 30, 2012. http://defensetech.org/2012/05/30/smoking-gun-proof-that-military-chips-from-china-are-infected/ (accessed May 19, 2013).

Schactman, Noah. *Exclusive: Computer Virus Hits U.S. Drone Fleet.* October 7, 2011. http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/ (accessed May 12, 2013).

TSGT MCNabb, Scott. "AFCYBER takes part in second USCYBERCOM Cyber Flag exercise." *24th Air Force.* November 21, 2012. http://www.24af.af.mil/news/story.asp?id=123327388 (accessed May 12, 2013).

U.S. Army. "The U.S. Army's Cyberspace Operations Concept Capability Plan 2016-2028." *Army.mil.* February 22, 2010. http://www.tradoc.army.mil/tpubs/pams/tp525-7-8.pdf (accessed May 12, 2013).

VADM Cebrowski, Arthur K. "Network-Centric Warfare - Its Origin and Future." *USNI - U.S. Naval Institute.* January 1998. http://www.usni.org/magazines/proceedings/1998-01/network-centric-warfare-its-origin-and-future (accessed May 12, 2013).

Whitehead, Tom. "Cyber attacks could 'fatally' wound computer dependent military, MPs warn." *Telegraph.co.uk.* January 9, 2013. http://www.telegraph.co.uk/news/uknews/defence/9787979/Cyber-attacks-could-fatally-wound-computer-dependent-military-MPs-warn.html (accessed May 12, 2013).

Willsher, Kim. "French fighter planes grounded by computer virus ." *The Telegraph.* February 7, 2009. http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html (accessed May 12, 2013).

Yasin, Rutrell. *As BYOD gains fed acceptance, assume devices been hacked, protect the data.* August 22, 2012. http://gcn.com/Articles/2012/08/22/BYOD-CIO-panel-technology-legal-issues.aspx?Page=2 (accessed May 12, 2013).