2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy

David T. Fahrenkrug
Office of Net Assessment
Office of the Secretary of Defense
Arlington, VA, USA
david.fahrenkrug@gmail.com

Abstract: Current accepted wisdom in cyberspace is that the attacker has the decisive advantage. The number of detected intrusions across public and private networks is increasing at an alarming rate, while the costs to defend against these intrusions are rising exponentially. Today’s best cyber security costs nearly ten times as much as the malware it is designed to protect against. This strategy is unsustainable. Drawing from defensive strategies used in other domains, this paper will offer an integrated defensive strategy for cyberspace that could even yield a decisive advantage over the offense.

An integrated defense begins by first trying to avoid the attack by actively dispersing the networks and information using IP and frequency hopping, data fractioning, cloud dispersal, and steganography. Second, an integrated defense includes hardening the infrastructure and date using encryption and shielding of electronic components. Finally, an integrated defense is able to detect and respond to intrusions and attacks. This requires an accurate and continuously updated awareness of the network’s configuration and activity as well as the ability to recover and respond to the attack.

Keywords: *defense, maneuver, dispersal, encryption, hardening, detection*

1. INTRODUCTION

On the morning of Nov 17, 1917, the British commenced an attack against the Germans in a little town of Cambrai. This battle marked the first time tanks, artillery, infantry, and aircraft were combined in a coordinated, synchronized campaign to outmaneuver the heavily fortified defenses of World War I trench warfare. Twenty-two years later, the Germans used those same technologies and capabilities to sweep across Europe with a revolutionary concept of warfare they referred to as *Blitzkrieg*. By organizing these very different combat arms into a combined

The views presented in this paper are of the author and not necessarily representative of the view or policies of the Department of Defense or the Office of Net Assessment.

form of maneuver warfare, the Germans were able to defeat the most sophisticated—and expensive—defensive system in the world, the French *Maginot Line*. The failure of the *Maginot Line* to withstand the German attack was primarily the result of a static defensive strategy that did not anticipate the speed of maneuver *Blitzkrieg* would be able to achieve on the battlefield.

Today's current cyber defenses suffer from a similar lack of flexibility and maneuverability. Like the *Maginot Line*, today's cyber defenses are not failing due to a lack of new technologies. In fact, sufficient capability and technology exist today to counter and possibly reverse the advantage of the attackers. Instead, today's cyber defenses are failing because they lack the organizing concepts that can integrate current capabilities into a flexible and adaptive strategy. From a military point of view, the ability to organize and integrate capabilities to achieve specific objectives is known as the operational art of war. Commanders and operational planners bring together various capabilities and tactics and integrate them into lines of operation designed to achieve specific operational objectives that ultimately contribute to the overall campaign strategy. Drawing from defensive strategies used in other domains, this paper will offer an integrated defensive strategy for cyberspace.

The first section of this paper provides a description of cyberspace that will become the basis for crafting a defensive strategy. The next section will then review defensive concepts from other domains and introduces four principles of an integrated defensive strategy. The remaining sections will then apply these four principles to cyberspace to illustrate how an integrated cyber defense could be implemented. The paper concludes with a brief discussion on the critical next steps that should be pursued.

2. CYBERSPACE

Before introducing new ways to improve the defense, we must first understand what we are defending, why we are defending it, and where we are defending it. Even though cyber is most often used as a metaphor for the internet, computers, or hacking in general, a more useful understanding of cyberspace is reflected in the United States Department of Defense definition [1]. "Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers". From this definition, we see that cyberspace is a variety of networked systems that were created by connecting electronic components using signals (electromagnetic energy) and software. More importantly, cyberspace was created so that we could more easily and rapidly create, store, modify, and transfer data and information. This description of cyberspace allows us to distinguish the place—cyberspace—from the activities that occur within that place. The principle roadblock to gaining greater understanding of warfare and competition in cyberspace has been simply conflating the networks with their functions. What we do with networks is fundamentally different than the network itself.

So, we must distinguish between cyberspace and how cyberspace is used. The pervasiveness of networks and the number of systems and functions that now rely on the rapid transfer of data is a testament to how important this new "terrain" has become. While networks vary significantly from one another by the type of hardware, software, or signals that are used to create the connections, they all exist for essentially the same reason; to improve and increase our ability to transfer data and information. Thus, we are interested in not only protecting our ability to access and use cyberspace, but more importantly we want to protect the functions and data that are resident in cyberspace. These are not the same thing and protecting them may require very different approaches.

One way to increase our understanding of the difference between place and function is to draw from theoretical treatises concerning other domains. For example, Julian Corbett [2] offers an elegant theory on naval warfare to include a perspective on the sea domain. Due to the lack of differentiation between information and cyberspace within the literature on information warfare, a key principle of warfare has been misunderstood—control of the operational domain. Julian Corbett describes this as the "object" of warfare. Regardless of the domain, the object of warfare in that domain is the attainment of some level of control over access and use of the domain. Corbett describes the principle most clearly in his discussion of maritime strategy. "The object of naval warfare must always be directly or indirectly either to secure the command of the sea or to prevent the enemy from securing it." Other theories also describe a requirement for controlling the domain first and then using it to achieve other objectives. Giulio Douhet [3] identified achieving "command of the air" as the first priority and the reason a nation needed an independent air force. In modern military doctrine, and in particular Air Force doctrine, this principle is often described as superiority.

A significant difference, however, from the other domains is the flexibility of the terrain in cyberspace and the lack of requirement to defend *specific* terrain. In other words, cyber defenses are not bound by territory. Rather than defending a piece of territory or area of airspace, cyber defenses are concerned with protecting content and function. If organized, planned, and exercised properly, any compromised component of a network could be isolated and even discarded while the functions and data continue to exist in the remaining elements or are rerouted to new infrastructures. This means cyber defense can become just as agile as the offense. This unique characteristic of cyberspace should figure prominently in any integrated defensive strategy.

3. INTEGRATED AIR DEFENSES

In the period between the Battle of Cambrai and the deployment of *Blitzkrieg* warfare, the necessary technology had already been discovered. Yet only the Germans had adopted this new form of maneuver warfare. The innovation did not come from new technology, but from employing new concepts of operation that integrated existing technologies to achieve greater speed and agility on the battlefield. The Germans developed and practiced a combined arms approach to create synergy between the tank, infantry, air, and artillery components that resulted in a maneuver advantage that was difficult to overcome in the early years of World War II. In the same way, sufficient technologies exist today to overcome the offensive advantage that is overwhelming current defenses. As Paul Williams [4], executive director of security services for White Badger Security, confidently claimed when asked at a recent conference about Stuxnet, "There's absolutely no way it would have happened with just a reasonable dose of off-the-shelf commercial technology." This "reasonable dose", however, needs to be employed using an integrated operational concept in order to be effective against a maneuvering adversary.

Similarly, the tragedy of Pearl Harbor was that we were not ready to fight through an attack. With no warning of attack, aircraft parked closely together on open taxiways, and aircrew not prepared to respond immediately, the Japanese easily and swiftly destroyed most of the combat capability located at Pearl Harbor. Since that time, militaries have responded to the potential devastation that could be suffered from an air attack by developing integrated air defenses. Everywhere in the world, countries with sufficient resources have built integrated defensive systems based on a layered and responsive approach. With the United States military, despite the fact that no bases, or ground forces for that matter, have come under attack by aircraft in more than fifty years, the Air Force still trains as if they will.

An integrated defense begins with radar capable of detecting the threat to potentially provide early warning and direct a response against the attacker. The defense uses these warning and detection systems to cue aircraft flying defensive combat air patrols as well as surface to air missiles to counter the incoming attack. In preparation for the possibility that at least one attacker will get through, buildings and aircraft shelters are hardened, and personnel are trained on how to conduct rapid runway repairs. In addition, aircraft, support equipment, and even the runways, are dispersed to increase the number of targets and decrease the likelihood that any single attack could wipe out all capabilities. Finally, aircrews are trained to scramble and get their aircraft airborne as soon as possible. Applied to cyberspace, this means developing network sensors, offensive responses, and protection and recovery procedures for critical data and operating systems. More importantly, this means exercising and training for the eventuality of an attack.

4. INTEGRATED CYBER DEFENSE

During World War II, a key objective of the Allies was to secure the transfer of critical parts and supplies. In the face of a persistent German campaign, this meant at times actually escorting some of the ships with cruisers and submarines. The U.S. Navy did not try to secure all the sea lanes, all the time. In fact, there were certain aspects of the ocean that the Germans had free access to all the way up to the coast of the United States. Not all data is critical, and not all networks need to be secured. The key is ensuring that the mission can be accomplished. This concept of mission assurance is gaining traction throughout the military, but there is still a lack of operational concepts [5]. The following sections will describe each aspect of an integrated operational concept to improve cyber defenses.

A. Dispersal

When considering how to disperse forces and capabilities, we must once again first identify what we are dispersing and distinguish that from where we are dispersing it. Some networks are purely functional and do not directly affect information, while other networks exist only to store data and information. In the first case, we want to disperse the *functions* of the network, while in the latter, we want to disperse the *data or information*. The purpose in both instances is to make targeting that much more difficult for an adversary.

When dispersing the network, all aspects of the network environment must be considered for dispersal. Operating systems can be dispersed as virtual machines within the network or outside the network to mitigate a software attack. Communication lines, both wired and wireless, can be dispersed by increasing the number of fiber lines available or by using a greater range of frequencies of electromagnetic energy to transmit the data. Hardware components can also be distributed across multiple platforms to reduce the possibility that any one system becomes a single point of failure for the entire network.

For example, the recent STUXNET case highlighted the vulnerability of SCADA devices with only one algorithm for controlling a critical process. Keith Stouffer, Joe Falco, and Karen Scarfone [6] suggest a possible solution is to disperse functionality within the integrated control device. "Maintaining functionality during adverse conditions involves designing the ICS [integrated control system] so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS or other networks, or does not cause another problem elsewhere, such as a cascading event." The objective is to build resilient and survivable control systems through automated sensors, pre-established algorithms, and defined responses.

Similarly, storing complete sets of data and information in a single location simplifies that attacker's problem and in some cases even singles out the information as being more important. Cloud storage solutions offer the possibility of hiding data and information by placing it in a noisier environment. Ken Sorrels [7] argues that we need to inventory the functions and content of the network and then segment them off into different areas based on characteristics like confidentiality, integrity and availability. "This keeps an entire system from being at risk when a certain zone is breached."

Just as camouflage and decoys are effective ways to disguise the location of physical targets, so the expanding number of storage solutions presents an opportunity to disperse and hide information and functions resident in the network. The ability to disperse also provides an added benefit of increasing confidence levels in the veracity of the information. The more the information is fractioned and dispersed, the less likely an adversary will be able to corrupt or deny access to all of that information. Again, this is where it is important to understand and prioritize the information on the network or the functions the network is supporting.

For some information, the content is more critical than how quickly it can be accessed, while other information is only useful at a specific time and moment. For example, a flight of F-22s connected by a tactical data link share situational and targeting data that is time sensitive and often very perishable. What is most critical is that the data is received on time and in the format that is required to complete the kill chain.[1] The more perishable the data becomes, the more important timely reception of the data becomes. This places less emphasis on securing the signal, and more importance on ensuring sufficient pathways to deliver the data.

Rather than transmit data across a single, highly encrypted frequency (or narrow band of frequencies) that simplifies the adversary's detection and jamming problem, the data link and the data being transmitted should be dispersed across a range of frequencies within the

[1] The military has codified the chain of events required to acquire and target an adversary. The kill chain is summarized by the phrase "find, fix, track, target, engage, assess" or the acronym F2T2EA.

electromagnetic spectrum. This type of spectral agility was explicitly identified in a recent military report [8] that identified the requirement for "jam-resistance, low-probability-of-detection/ intercept, and cyber resilience in the increasingly congested spectrum environment and increasingly contested electronic warfare environment." This accomplishes two things: first, the likelihood that an adversary can detect and then target each of the signals is decreased; and second, the veracity of the data is increased because an adversary must intercept and alter each instance of the data that has been transmitted. A simple voting scheme that compares each of the transmissions of the data can be used to verify the validity of the information that the other aircraft is receiving. In this case, nothing about the network or the data has to be "secured" because the information is perishable and of little use beyond that instance of time. Instead, dispersal of the signal and the data preserves the *ability* to transmit and receive data with increased confidence that the data has not been compromised.

In other cases, the same flight of F-22s may be sharing positional information of the formation available on the same tactical data links that could compromise the mission if intercepted by an adversary. The challenge then becomes one of securing the information *and* ensuring its availability to all members of the flight. This will require some level of encryption of the data, but not necessarily for the network itself. The point, once again, is we have to first identify and prioritize the data and functions that are dependent on the network and then choose the most effective way to distribute them using a combination of hardware, signals, and software.

B. Hardening

In addition to dispersal, the functions of the network and the information resident in the network need to be hardened. Dispersal increases the probability of avoiding the attack, while hardening increases the probability of surviving the attack. Again, existing technology is available that could be used to decrease the likelihood of an attacker accessing a network or affecting the contents of the network. While public key encryption is increasingly being used, the use of hash and private key encryption for information stored and transmitted on their networks needs to increase as well. Rather than trying to secure every network or computer system, businesses and organizations need first to prioritize their networks and information and then apply appropriate levels of encryption to ensure operating systems, data, and automated commands are not compromised.

Available encryption practices and an extensive number of software solutions can radically reduce the vulnerability of data and operating systems. For example, IBM has developed a secure processor chip that protects the operating system from physical or software attacks with no known compromises after fours years and millions of chips operating word wide [9]. Despite this success, not all encryption methodologies will be perfect all the time. In the most sensitive networks, containing the most sensitive data, encrypting across all aspects of the network adds layers of defense that greatly compounds the attacker's problems. Potentially, encryption methods could also incorporate steganography to further hide or disguise data or software even while it is being hardened through encryption.

For some networks, the hardware will need to be protected against electronic attack or persistent intrusion sets. In both cases, there are current and emerging technologies which can increase the resiliency of chips, processors, and control devices from malicious attacks. During the

Cold War, electronic components that could potentially be exposed to an electromagnetic pulse following a nuclear detonation (i.e., navigation and communication components on a B-52 bomber) were specifically designed to survive such a situation. In an effort to increase the speed of our chips and processors, these components have become even more vulnerable to some type of electromagnetic inference. While costs and weight clearly prohibit the hardening of every component within a network, there are ways to harden the most critical components.

When combined with dispersal, the chances that an attacker will be able to affect the data or the functions of the network are significantly reduced. In fact, the cost and time required to attack networks configured with these defenses will likely deter most potential attackers. Still, a determined adversary will get through eventually, such that an integrated defense must have the ability to detect the intruder and then respond.

C. Detection

At no time in the history of warfare has any commander had perfect awareness of the battlespace. Despite our best efforts to gain “information dominance” it will always elude us. Fog, friction, and uncertainty are fundamental characteristics of war that we may be able to mitigate in some circumstances, but never completely eliminate. Instead, our objective is to anticipate and prioritize those situations and locations where we require the absolutely best awareness we can acquire. This is true for cyberspace as well.

During the interwar period, fear of an attack from the air spurred several nations to bolster their nascent radio wave detection research program to improve their ability to detect an incoming air threat. The efficacy of building an elaborate detection network was put on display during the Battle of Britain. Their effort focused on detecting the threat as far away as possible, concentrating on the most probable avenue of attack. Similarly, in the early days of the Cold War, the United States used Ballistic Missile Early Warning sites to detect incoming Soviet intercontinental or submarine launched nuclear ballistic missiles. Physics determined the limited number of ways the Soviet Union could employ ballistic missiles against the US which in turn determined the number, type, and location of sensors we would have to build. Initially, only three sites were required to give adequate coverage against the threat. In both cases, geography, threat, and response time determined the type of detection required to defend against an attack.

Current efforts in cyberspace have focused heavily on Intrusion Detection Systems to identify when a network has been compromised. Unfortunately, while these sensors are necessary, they do not provide sufficient response time to react to a malicious attack. Ultimately, we would like to conduct deep packet inspection as far away from our network as possible, potentially in an isolated environment. Several technologies hold promise for conducting this type of early warning.

Still, at some point, network security will be breached. Just like there are no perfect radars or fences, there are no perfect intrusion detection systems that will detect 100% of the intrusions. For that reason, it is not sufficient to simply scan the borders of the network. Williams [4] suggests that the real damage of an intrusion is caused by the widespread and silent compromising of a system. “Organizations must monitor their systems for changes in connections between computers and servers, as well as patterns of mutations that seem to spread on their own.”

Understanding the configuration of the network and the types of communication taking place on the network is a critical aspect of any defense.

Many "closed" networks operate under the assumption that whoever is on the network is authorized to be there. Situational awareness of the network becomes even more important for a "closed" network because of the sensitivity of the information on the network or the critical function it supports. For example, no matter how secure or "closed" the nuclear command and control network becomes, the possibility always remains that someone will get in. As networks proliferate and integrate, the ability to access a system undetected becomes easier. These types of critical networks require constant validation of all activities and processes occurring on every device within the network. Obviously, this is no small feat especially considering that these types of scans will compromise speed without a corresponding increase in computational capacity. Still, a mobile and active defense demands this level of situational awareness in order to respond to the intrusion threat.

D. Recover and Respond

Even the most sophisticated air defense systems are breached and facilities attacked. Stealth aircraft and advanced electronic warfare capabilities can be used to effectively blind the defense. In the same way that there are no perfect defenses against illegal border crossings or stealth aircraft, our networks will never be perfectly secured. With enough determination, an adversary will eventually defeat any defense, especially if it remains static. Like other types of defenses, we must anticipate the possibility that someone will eventually get into even our most secure networks. If done sufficiently, hardening and dispersal, will mitigate, if not defeat all together, the initial effects of most attacks. However, the adversary will adapt and the defense must react quickly. Once the network is breached, it becomes imperative to recover from the damage, find the threat, and respond.

Unlike any other domain, cyberspace can be redesigned. IP addresses can be changed, signals disrupted and new connections established, and routers, servers and switches taken off line while new ones are brought on. By reconfiguring the network and possibly moving data and functions to new segments or even new networks, cyberspace has the potential to be the most flexible and adaptive domain of warfare. For example, when components cannot be hardened against an electronic attack, alternate systems need to be available so that the network can be reconfigured or the data and functions rapidly moved to another network. Again, this is a capability that exists today. A recent study [10] demonstrated the ability to rapidly move functions across heterogeneous operation systems and platforms.

Maneuver warfare involves moving in relation to the adversary and conducting integrated movement across multiple domains [11]. Moving in relation to the adversary requires understanding the characteristics and physics of cyberspace as well as how a potential adversary uses cyberspace. At a tactical level, understanding movement in cyberspace means first understanding what is moving and how it is moved. Earlier, cyberspace was described as the place where data is created, stored, modified, and exchanged. What is moving is the data and how it is moved is through signals and electronics. Movement in cyberspace is accomplished by modifying either the signal (wireless or wired) or the software and hardware that manages the signal. If an adversary is targeting a particular signal frequency or internet protocol address to disrupt or attack the data, then moving to a different type of signal or IP address would counter his attack tactically.

These concepts were recently summarized by a former chief scientist of the United States Air Force. In his final report [8], he concluded that a fundamental shift from protection to mission effectiveness would emphasize “technologies such as IP hopping, network polymorphism, massive virtualization and rapid network re-composition that can make cyber systems inherently resilient to intrusions entering through the network layer. These convert the currently static network layer into a highly dynamic one, in which the hypervisor mapping between the hardware and functional layers changes constantly in a pseudo-random way, perhaps hundred of times every second. A cyber adversary who finds vulnerabilities in the physical layer thus has virtually no time to use them for mapping the network before its topology has changed.”

5. ANTICIPATING THE FUTURE

The current offensive advantage results from the ability to maneuver against a network combined with rapidly adaptive tools to attack networks and information. Current defense measures just simply cannot be prepared for the unknown and seemingly limitless ways to penetrate and attack a network. Increasingly, the most vulnerable networks are mobile. This past year, more smart phones were sold in the world than personal computers. This trend will continue across all types of networks; private, commercial, government and military. In fact, the US military is currently making plans to extend command and control infrastructures and increase access to information—including classified information—by distributing smartphones and tablet devices to individuals operating throughout the battlefield [12]. Even some of the newest satellites being tested are nothing more than smart phones placed in a box and launched into space [13]. Governments and private industry are exploring ways to use smartphones to build on orbit communications and sensor networks.

This expansion of network capability will provide a greater tactical and operational advantage, but also risks introducing even more vulnerability to the battle networks. The rapidly changing configuration of these highly mobile networks will be both a blessing and a curse for attackers and defenders. Implementing dispersal and hardening techniques however, could achieve a level of agility and protection for these types of networks that could result in an advantage for the defender rather than the attacker. In the same way that highly mobile, integrated air defense systems present a formidable challenge to attacks from the air, so too can data and communication networks achieve a similar level of capability.

One way to gain a position of advantage, particularly against a superior adversary, is to move to where he is weakest. This indirect approach applies force against an adversary’s vulnerabilities. The social use of cyberspace represents another vulnerability but also an opportunity. Identifying who is part of an organization and their relation to others inside and outside the organization is essential to developing access to that organization. Prior to the explosion of information technology, this attack method was primarily conducted by covert agents who co-opted a member of organization to gain access and information. The ultimate covert action was to gain membership to the organization so that information could be accessed directly. Once inside, they would have varying degrees of access to different types of information or even sensitive assets.

The prevalence of email and social networking sites make cyberspace an ideal medium to gain access to an organization. Unlike strangers, people who use information systems tend to trust the information they are presented. At the moment, it is relatively easy to deceive people in cyberspace and gain their trust. Further, the designed openness of social network sites introduces vulnerabilities to any organization's network. While social networking sites are typically riddled with malware and simply should not be accessed from mission critical systems, there is an opportunity to use these same vulnerabilities to expose potential adversaries. Configuring honey-pot networks using virtual machines, networks, and even cloud environments, may offer some ways to gain early warning of an attack and adversary techniques.

6. CONCLUSION

Sufficient capabilities exist today to counter the offensive advantage in cyberspace. What is lacking is an operational concept that can organize and integrate these capabilities into a posture that makes the defense more capable than the offense. This paper has introduced an integrated cyber defense strategy that increases network resiliency by dispersing and hardening the functions and data resident on the network. This includes taking advantage of network diversity to further complicate an attacker's problem. In addition, the defensive strategy relies on detecting the threat and adopting recovery procedures to respond the eventuality that a network will be breached. Together, these four characteristics of a integrated defensive system increase the strength of the defense and may even yield an advantage against the offense.

The uniquely dynamic nature of cyberspace, however, will ultimately shift the balance in favor of the defense. Highly mobile and hidden systems are extremely difficult to target. Despite the highest priority given to the mission, coalition forces were largely unsuccessful in eliminating the SCUD threat in Iraq during DESERT STORM. The Iraqi systems were easy to move and disguise which made them virtually impossible to find and target. Cyberspace has even more potential to be highly mobile allowing the defense to stay one step ahead of the offense and avoid an attack outright.

Networks continuously change and this change can be incorporated into a defensive strategy. The *tactical* advantage in cyberspace goes to those countries that can increase the speed and agility of their networks through more precise timing and increased processing power. However, the ability to rapidly establish, reconfigure, and distribute networks as well as the data and functions on the network will yield the *strategic* advantage in cyberspace.

REFERENCES:

[1] Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, September 2010.

[2] Julian. S. Corbett, *Some Principles of Maritime Strategy*, Annapolis: Naval Institute Press, 1988.

[3] Guilio Douhet, (1942) *The Command of the Air*, Washington, D.C.: Office of Air Force History, 1942.

[4] Paul Williams, Remarks given at FOSE information-technology exposition and conference in Washington, D.C., July 2011. Available: http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=478

[5] Kamal Jabbour and Sarah Muccio, "The Science of Mission Assurance", *Journal of Strategic Security*, Vol IV, Issue 2, 2011, pp. 61-74.

[6] Keith Stouffer, Joe Falco, and Karen Scarfone, *Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology, Special Publication 800-82, June 2011, p. 3-2.

[7] Ken Sorrels, Remarks given at FOSE information-technology exposition and conference in Washington, D.C., July 2011. Available: http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=478

[8] "Technology Horizons: A Vision for Air Force Science & Technology During 2010-2030". [Online] Available: http://www.aviationweek.com/media/pdf/Check6/USAF_Technology_Horizons_report.pdf

[9] P. Williams and R. Boivie, "CPU Support for Secure Execution", Trust 2011, 4th International Conference on Trusted Computing, June 22-24, 2011, Pittsburgh PA.

[10] Hamed Okhravi, Adam Comella, Eric Robinson, Joshua Haines, "Creating a cyber moving target for critical infrastructure applications using platform diversity", *International Journal of Critical Infrastructure Protection*, 5, 2012, pp. 30-39. Available online: www.sciencedirect.com

[11] Richard D. Hooker, Jr., *Maneuver Warfare: An Anthology*. Novato, CA: Presidio Press, 1993.

[12] Steven Pugh, "A Top-Secret Smartphone Could Become Reality", *Signal*, November 2011, pp 15-16.

[13] "NASA ARC is Testing Cubesats on Balloons", SpaceRef Interactiv Inc. DBA SpaceRef Interational Group, [Online] http://www.spaceref.com/news/viewsr.rss.html?pid=36489