


5-27-2013

# The Rising Digital Missile Gap: the Security Threat of the United States' Cyber Inactivity

Christian Pedersen

*Pepperdine University, School of Public Policy, [Christianpedersen@alumni.pepperdine.edu](mailto:Christianpedersen@alumni.pepperdine.edu)*

Follow this and additional works at: <http://digitalcommons.pepperdine.edu/ppr>

 Part of the [Defense and Security Studies Commons](#), [Economic Policy Commons](#), [Military Studies Commons](#), [Other Public Affairs, Public Policy and Public Administration Commons](#), [Peace and Conflict Studies Commons](#), [Policy Design, Analysis, and Evaluation Commons](#), [Public Administration Commons](#), [Public Affairs Commons](#), [Public Policy Commons](#), [Social Policy Commons](#), and the [Social Welfare Commons](#)

---

### Recommended Citation

Pedersen, Christian (2013) "The Rising Digital Missile Gap: the Security Threat of the United States' Cyber Inactivity," *Pepperdine Policy Review*: Vol. 6, Article 11.

Available at: <http://digitalcommons.pepperdine.edu/ppr/vol6/iss1/11>

This Article is brought to you for free and open access by the School of Public Policy at Pepperdine Digital Commons. It has been accepted for inclusion in Pepperdine Policy Review by an authorized administrator of Pepperdine Digital Commons. For more information, please contact [Kevin.Miller3@pepperdine.edu](mailto:Kevin.Miller3@pepperdine.edu).

**The Rising Digital Missile Gap:**

**The Security Threat of the United States' Cyber Inactivity**

Christian Pedersen

In 1960, Senator John F. Kennedy campaigned on the issue that under the watch of President Eisenhower, a missile gap had develop between the United States and the Soviet Union. The fear of nuclear war was a grim reality, which most politicians and citizens alike understood the dire consequences. Policymakers witnessed the devastation of atomic weapons in the wake of World War II. The vaporization of two Japanese cities, awoken the world to the power of nuclear weapons. In efforts to prevent the duplications of these disasters, policymakers committed themselves to the mastery of space, international treaties, and the development of defensive measures and alert systems. While the threat of nuclear weapons is far from over, policy makers understood the severity of these weapons, the consequences of their use, and worked to prevent annihilation. The arms race was a key component of the deterrence strategy which defined defense policy in that era. It rested on the principle that the Soviet Union should not develop technological superiority over the United States. The belief was that should a missile gap develop and the Soviet Union was to gain more weapons then the United States, America would be doomed in nuclear holocaust. A competing viewpoint was held by the Soviet Union which feared the American's nuclear superiority as well.

We stand at the threshold of developing a new arms race -- one represented no longer by a gap of nuclear warheads, but a gap in digital supremacy. The world is evolving into a dangerous new world, with stakes higher than ever. Perhaps since policymakers have never witnessed the devastation of a large scale cyber-attack, they do not truly understand the serious

threat which a cyber-attack presents. The United States' failure both to dominate the electromagnetic spectrum for military purposes, the failure to secure our digital infrastructure, in wake of the rapid cyber development of other nations, presents the most immediate threat to national security. We are only as safe as we allow ourselves to be, and we need to act quickly to begin removing the vulnerabilities within our computer systems. It only takes one successful hacker, to end the way of life in America we know. The National Nuclear Security Administration, which oversees the U.S. nuclear weapon stockpile, is attacked nearly 10 million times a day (Koebler, 2012). In an ever grimmer reality, one successful attack could end all life on earth. Is this a risk we are willing to take? National Security depends upon cyber-security.

One of the best examples of this of the threats of society comes from August 2008, during the South Ossetia war between Russia and Georgia. During the military campaign in Georgia, Russian naval hackers methodically launched cyber-attacks on Georgia (Bukkvoll, 2009). These hackers destroyed Georgian internet servers crippling and disrupting communication throughout Georgia (Walsh, 2009). The Georgian government could not match the technical superiority of Russia, and was forced to rely upon Estonia and Poland for technical assistance (Markoff, 2008). The Russian Naval hackers then infiltrated the Georgian Power grid; block by block they powered down cities as Russian ground forces moved in for occupation.

Russia is not the only nation to demonstrate such capabilities. The United States began flexing its own cyber-muscle during the Bush Administration. Late in 2007, the National Security Agency (NSA) launched one of the largest and most successful cyber-attacks to date (Harris, 2009). The NSA attacked cell phones and computers that counter insurgents in Iraq were using to plan and coordinate roadside bombings (Harris, 2009). This operation was not only a

successful military strike on enemy forces, but it was successfully achieved without risking the safety of American personnel.

While cyber-warfare is still secondary to traditional warfare, there are graver threats lurking in cyberspace. Cyber-spying is one of these prominent threats. In an incident referred to by the Defense Department as “moonlight mazes”, hackers traced to Russia were found to have infiltrated the Defense Department’s network in an attempt to steal military secrets (Vistica, 1999). Terabytes worth of data were stolen on the development of Lockheed Martin’s revolutionary Joint Strike Fighter (Sweetman, 2009). Due to the complexity of the project, and the involvement of thousands of personnel, information was transmitted and stored electronically over public networks so all necessary personnel could access it (Sweetman, 2009). While it would have been safer to use a specialized network for this project, it was not practical or possible. Once the network was compromised, it became vulnerable to repeated attacks (Sweetman, 2009).

Combating cyber-spies can be more challenging than their cold war counterparts, as all the secured hangers, sealed buildings, and secret bunkers in the world cannot keep cyber-spies from accessing information in the same ways they could prevent traditional spying methods (Sweetman, 2009). The cyber-spies do not simply steal information, as did spies of the past, but copy it (Sweetman, 2009). For this reason, these acts of espionage are more difficult to detect. Nothing is broken, nothing is missing, nothing is stolen, so it is exceedingly difficult to tell when something has been compromised (Sweetman, 2009). The other difficulty with cyber-spies is that while it is suspected that most hackers work for foreign governments, it is impossible to prove (Wright, 2009). The fact that the IP address of a computer used in a cyber-attack is located in a foreign country is not indisputable evidence of a foreign government’s involvement. The recent

attack on the South Korean banking and broadcast systems is evidence of this (China, 2013).

Though the attacks appeared to have originated in China, it is suspected that they were initiated by North Korean Hackers masking their point of origin (China, 2013).

In recent years there has been a significant increase in the frequency of attacks on military, governmental, and civilian computers from both governments and independent hackers (Walsh, 39). In June of 2007, fifteen hundred of the Department of Defense's computers were taken offline after a cyber-attack (Fox, 2007). The Department of Homeland Security reported roughly eight hundred successful attacks in a two month window surrounding the same period of time (Fox, 2007). The Pentagon itself is attacked roughly one hundred times a day. These attacks are separate from the attacks on Naval Intelligence, Air Force Intelligence, the NSA, the CIA, and the other government agencies responsible for National Security (Miklaszewski, 1999). The Air Force estimates that roughly ten terabytes of top secret data have been stolen from Defense computer systems by hackers within a two year period (Wright, 2009).

What makes this new digital arms race different from the past is the fact that the players in this race are no longer only nation states, but terrorist organizations, hacker groups, and teenagers in basements. There are instances when novice hackers have been responsible for stealing information and compromising systems in an attempt to prove simply test, or prove capabilities (Wright, 2009). Computer hackers can come from anywhere, and possess the power to steal secrets and launch attacks against secure networks.

Terrorists are now going high-tech and finding unique uses for cyberspace, such as the recruitment of new members. Salman Al-Awdah, a friend of Osama bin Laden and one of the early founders of radicalism against the United States, uses his website to spread his ideology to the next generation of jihadists (Belz, 2009). Terrorist organizations have used Google Earth to

plan attacks against Coalition forces in Afghanistan and Iraq (Rollins, 2007). Once these attacks were coordinated and executed, videos depicting the violence were then posted online (Harris, 2009). Terror cells use popular games, such as *Second Life* and *World of Warcraft* to plan meetings (O'Brien, 2007). In these virtual worlds terrorist can meet via avatars, digital manifestations of themselves existing online. These meetings can involve participants from all around the world and, shrouded in the cover of game play, are virtually undetectable. Meetings conducted in game provide secrecy and security they could never experience if they were to occur in the physical world, as these virtual environments cannot be monitored by traditional surveillance techniques (Rollins, 2007).

Terrorist groups have created thousands of websites to fundraise, recruit, and educate (Rollins, 2007). Al Qaeda has created websites with gigabytes full of information educating potential terrorist on everything from building safe houses to planning suicide bombings. They even teach how to mix lethal chemicals and what to do if captured (Rollins, 2007). Such groups now educate new recruits on computer hacking techniques in order to prepare them for the coming “electronic jihad” (Rollins, 2007). What might this electronic Jihad look like? It is possible that it could look something like attacks on power grids, which have resulted in widespread power outages (Gorman, 2009). It could be far more advance than that though, an attack on power systems could involve the reversal of water filtration, the blocking of oil pipelines, the jamming of communications, and the crippling of transportation systems -- all the makings of a manmade national disaster (Shea, 2004).

Despite attacks like this, U.S. infrastructure remains vulnerable to attack; since the industrial control systems are ridden with vulnerabilities and the security of these systems has been a low priority (Shea, 2004). The Supervisory Control and Data Acquisition (SCADA)

systems are the computer systems responsible for monitoring infrastructure and communication systems within the United States. The SCADA systems operate everything from cellphone towers to electricity, and water treatment to traffic lights. Interestingly enough, an al Qaeda computer was discovered in Afghanistan containing detailed analysis of SCADA systems within the United States (Shea, 2004). While the SCADA systems are protected systems, the consequences would be dire if any part of the system were to be compromised. While some professionals feel that the chances of success of an attack on these systems would be rather minimal given the procedures already in place for naturally occurring system failures, this is not the consensus (Shea, 2004). Following an attack, no one knows for how long the systems would be compromised. If multiple systems were attacked at once, a cyber-attack on the United States' infrastructure could be more devastating to the nation than any sort of bombing or traditional attack. For this reason alone national security is increasingly relying upon cyber-security.

In November of 2012, Defense Secretary Panetta warned about the severity of the coming "Digital Pearl Harbor" (Bemiller & Shanker, 2012). Whether this will come from independent hackers, a terrorist organization, or other nations; precautionary measures need to be taken. The Director of National Intelligence, James Clapper, has argued that the threat of a large scale cyber-attack is marginal, as Nations like Russia and China – those most capable of launching successful large-scale attacks – seem uninterested in attacking the United States (Zetter, 2013). Clapper argues that massive attacks will most like occur only in conjunction with military conflict between capable nations and the United States (Zetter, 2013). Clapper did warn of potential cyber-attacks from smaller actors, who will likely attack smaller systems such as power grids (Zetter, 2013). These attacks he argues could have "significant outcomes," such as unexpected consequences or effects from the attacks affecting additional systems (Zetter, 2013).

Looking towards the future, the United States Air Force committed itself to building a force capable of dominating cyberspace, and protecting the country from all cyber-attacks (Theohary, 2009). The U.S. Strategic Command -- the unified military command responsible for overseeing intelligence, missile defense, and combating weapons of mass destruction -- added to its list of responsibilities information warfare, overseeing electronic warfare, and conducting information operations (Theohary, 2009). One problem, however, is that current Air Force and Department of Defense protocol emphasizes cyber training as opposed to a cyber-education (Williams, 2009). Defense personnel are only trained to deal with a limited range of scenarios (Williams, 2009). This is not a practical strategy for defeating an educated enemy. Such a system is inferior to a cyber-education program, which would allow personnel to do more than just react, but would enable them to better defend against and implement cyber-attacks. While the Air Force expressed its intentions for developing a program capable of defending against all threats across the electromagnetic spectrum, it is estimated that a successful cyber-warrior education program could take approximately fifteen years to become fully functional (Williams, 2009).

Another part of the problem with waging cyber-warfare is that most military commanders were raised prior to the digital age. Consequently, they have a great deal of trouble understanding and utilizing non-traditional methods of warfare (Harris, 2009). For this reason, the U.S. military has found adapting to the new digital world a challenge. The U.S. has been slow in not only repelling cyber-attacks, but also initiating them. General David Petraeus was one of the first in the military to actively embrace the power of cyber-space (Harris, 2009). Under Petraeus' command, the United States began shutting down computer servers and hijacking phone systems as a part of military information operations (Harris, 2009). Cyber-security is not just the responsibility of the Defense Department. The security of the digital infrastructure is



dependent upon the involvement of other government agencies and the civilian computer systems, which makes the collaboration with Congress essential. Congress can take actions such as requiring the Intelligence Community to produce reports on current and potential cyber-threats (Theohary & Rollins, 2009). Congress should also use its legislative role to determine which entity should hold the government's primary cyber-security responsibilities (Henning & Rollins, 2009). In addition, Congress can create civil liberty and privacy regulations for consideration when implementing further cyber-security reform (Henning & Rollins, 2009). Congress also has the power to address comprehensive network security reform (Henning & Rollins, 2009).

Congress introduced a number of bills on the Hill to bolster digital defenses. These are aimed at either heightening security standards or implementing preventative measures. These include the Transportation Security Administration Authorization Act (H.R. 2200), which requires the TSA to rank the cyber risk's associated with different modes of transportation across America (Theohary & Rollins, 2009). Both HR 2165, the Bulk Power Systems Protection Act, and HR 2195, designed to amend the existing Federal Power Act, were drafted to prevent cyber-attacks on the national energy grid (Theohary & Rollins, 2009). The Continuing Chemical Facilities Antiterrorism Security Act (HR 2868) would have changed the standards of digital security on all Chemical facilities (Theohary & Rollins, 2009). The Cyber-security Act of 2009 (S. 773) proposed in the Senate would have created regional cyber centers to implement cyber-security standards and help implement them at state and local levels (Theohary & Rollins, 2009). The FEMA Independence Act (HR 1174) would have created a division of the Federal Emergency Management Agency solely responsible for handling cyber-attacks, and the Cyber-security Education Enhancement Act (HR 266) was designed to establish a cyber-security professional development program (Theohary & Rollins, 2009). While no single piece of the

legislation is enough to overhaul the national digital infrastructure, each represents a formidable start at finding a solution. Unfortunately, all of these bills failed to become law.

It seems that one of the biggest issues contributing to the continuation of this problem is the lack of leadership, with neither the legislative or executive branch taking the lead. This is surprising, as President Obama himself was a victim of cyber-attacks while on the campaign trail (Obama, 2009). The President stated that “some of the most serious economic and national challenges we face as a nation” are weaknesses in our digital infrastructure, and that maintaining a technological advantage is the key to military success in the future” (Obama, 2009). The President outlined a number of steps to improve cyber-security. These plans included increasing public awareness through safety and education campaigns, attracting and retaining federal employees with expertise in cyber-security, and increasing partnerships between the private sector, the government, the academic world, and civil liberty groups to establish a secure and thriving digital infrastructure (Cyber-security, 2009).

While the Administration did conduct a review of the government’s efforts at “defending the information and communication infrastructure” and appointed a cyber-czar as the President planned to, it does not seem to have done much more (Obama, 2009). Now entering a second term, the Obama Administration’s official plans for improving cyber-security can be found on the White House’s website. Two goals are identified: improving Americans resilience to attacks and improving and reducing threats (National Security Council). The achievement of these goals is outlined in a ten step plan, which includes everything from the appointment of an official to coordinate national policy, updating the national security strategies, establishing performance parameters to measure national performance, preparing an incident response plan, and implementing awareness and education campaigns to promote security (National Security

Council). The same vague rhetoric and lack of direction which characterized the President's plans when he first entered office still continues to dominate the White House's current plans.

However, all the blame cannot be placed on the Obama Administration. This same lack of interest, and leadership, plagued the Executive Branch in their approach towards cyber-space since the emergence of the Internet. In 1996, military delegations from both Russia and the United States secretly met in Moscow to discuss a treaty that would dictate policy and approach towards cyberspace, as both nations realized the infinite potential of these new technologies (Markoff, 2009). The Russian's took this matter very seriously, and appointed a four-star Admiral to lead their delegation, the Clinton Administration sent a college professor (Markoff, 2009). While the professor was an expert in his field, this illustrates the lack of serious commitment from the military and White House regarding cyber-space. Their attitude resulted in insufficient policy creation. One possibility for the continued lack of tangible results is that the Federal Government lacks a starting point for creating cyber-security reform.

Since writing of this article began, further developments arose in cyber-security, which encouraged the President to issue an executive order to improve cyber-security (Obama, 2013). Under this new executive order, the President recommitted the government to evaluating the most critical infrastructure threats (Obama, 2013). The Department of Justice, the Department of Homeland Security, and the Office of National Intelligence are now committed to greater information sharing regarding cyber-security (Obama, 2013). The federal government will begin developing cross government minimum standards of cyber-security (Obama, 2013). While this is an important move in the right direction, it is not enough. The President himself has realized this, and asked Congress in his state of the union address to begin taking the next step to further secure our digital infrastructure (Transcript, 2013).

When moving forward in further evaluating the threats of cyber-space, the United State should mimic the example of Russia. While Russian policies towards human rights and individual liberties leave much to be desired, Russian cyber policy is an optimal example of a nation adapting to meet the challenges of a digitized world. After the collapse of the Soviet Union, the Russian people and the Russian government were poorly prepared for the information technology revolution, lacking both the skills the technology necessary to harness the power of cyberspace (Saunders, 2004). An economically and militarily weak Russia needed a plan to rebuild successfully and sustainably. Russia looked to the future, and committed itself to the domination of cyberspace. More importantly, the Russian government recognized the potential of cyberspace, and considered the threats residing there as secondary only to nuclear war (Thomas, 1996).

In the cyber world, war is about gaining an information advantage over one's opponent. This is done through disabling an opponent's information and control systems, by crippling their ability to make decisions, and immobilizing the enemy's ability to command the soldiers on the battlefield (Grau, 1996). The Russian military recognized the importance of understanding cyber-warfare technologies since the 1990s and has sought to prepare itself accordingly (Grau, 1996). The military believed the successful use of computer viruses and other cyber-attacks could compensate for other military weaknesses such as a disadvantage in manpower and outdated weapons systems (Grau, 1996). More importantly, the military understood that this was the key to winning a conflict with the west should one ever occur.

Russia has since made remarkable strides forward, as is evidenced by the rapid growth of Russian as a language on the internet from the 1990s to the early 2000s (Saunders, 2004). The increased online presence of the Russian population helped bolster the Russian economy, and

continues building the Russian cyber community (Saunders, 2004). As a result, the largest number of computer hackers living in cyberspace now resides within Russia (Saunders, 2004). This rapid technical growth within Russia is the direct result of a serious commitment taken by the Russian Government. In 2000, Russian President Vladimir Putin signed *The Doctrine of the Information Security of the Russian Federation* (The Military Doctrine, 2010). This comprehensive plan to prepare Russia for the future, described the reconstruction of the digital infrastructure, and ways to train and equip Russian personnel to better understand information technologies (Doctrine, 2000). It committed the government to better understanding and utilizing these new technologies by both evaluating its own digital weaknesses and developing defenses within the next ten years (Doctrine, 2000). It also called for the creation of a new governmental entity responsible for monitoring and protecting the digital infrastructure through the creation of uniform policy (Doctrine, 2000). Additionally, it mandated security improvements to protect both the Russian financial sector and the military-industrial plants (Doctrine, 2000).

Russia currently has the best cyber-warriors on the planet, and the Russian government developed the best strategic sense on how to utilize cyberspace as an effective tool during war. For years, Russia has been leading western nations significantly in cyber-war capabilities (Thomas, 2000). Hoping to duplicate this success, specifically those of Russian Naval Hackers, nations like China and North Korea began to develop similar education programs to prepare their militaries for cyber-warfare (Williams, 2009). This is done out of necessity, in the hopes of advancing their own military capabilities to replicate and repel the attacks of Russian hackers.

In the Russian military doctrine released in February of 2010, the government once again addressed cyber-warfare (The Military Doctrine, 2010). Russia acknowledged information warfare and cyber-attacks as an important part of warfare in the modern world, and announced

its intention to use cyber-attacks as the first response to all political conflicts in an effort to prevent the use of traditional military forces (The Military Doctrine, 2010). Russia once again committed itself to further improve its information systems and technology, so that its military forces can better prepare for combat in this new world (The Military Doctrine, 2010).

We are living in a dangerous new world. Threats which once only appeared in the pages of Ian Fleming novels and in science-fiction films now threaten our safety and security. In the 20th century, the missile gap was a pillar of defense policy, because policy makers understood the consequences of inactivity. More importantly, policymakers were eager to prevent the nuclear war. As the United States enters the 21<sup>st</sup> century, cyber-security should be the major cornerstone of our new defense policy. Unfortunately, cyber-security has not become the security concern that it should be. While the threats of nuclear war are infinitely more petrifying than the threats of cyber-war, inadequate cyber-protection can lead to detrimental consequences (including attacks on nuclear launch systems). Without the development of a comprehensive and appropriate response to these growing threats, others nations and non-state actors will continue to gain an advantage over the United States, threatening American livelihood and lives.

## REFERENCES

- Belz, M. (2009, December 5). Feeding jihadi fever. *World*, 36.
- Bemiller, E., & Shanker, T. (2012, October 11). Panetta Warns of Dire Threat of Cyberattack on U.S. *New York Times*.
- Bukkvoll, T. (2009) Russia's Military Performance in Georgia. *Military Review*. 57-62.
- China IP address link to South Korea cyber-attack (2013, March 21). In *BBC News Asia*. Retrieved March 21, 2013, from <<http://www.bbc.co.uk/news/world-asia-21873017>>.
- Doctrine of the Information Security of the Russian Federation (2000, September 9). Retrieved April 18, 2010, from <<http://www.embrusscambodia.mid.ru/doc-information-e.html>>
- Pentagon Cyber Attack Forces 1,500 PCs off line." (2007, June 22). In *Fox News*. Retrieved January 3, 2013.

- Gorman, S. (2009, April 8). Electricity grid in U.S. penetrated by spies. *The Wall Street Journal*. Retrieved January 7, 2013.
- Grau, L. W., & Thomas, T. L. (1996). Russian View of Future War: Theory and Direction. *Journal of Slavic Military Studies*, 501-518.
- Harris, S. (2009, November 14). The Cyber-war plan. *National Journal*, 19-25.
- Henning, A. C., & Rollins, J. (2009, March 10). Comprehensive national cyber-security initiative: Legal authorities and policy considerations. *Congressional Research Service*.
- Koebler, J. (2012, March 20). U.S. Nukes Face Up to 10 Million Cyber Attacks Daily. *U.S. News and World Report*. Retrieved January 5, 2013, from <<http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily>>.
- Markoff, J. (2008, August 11). Georgia Takes a beating in the Cyberwar With Russia [Electronic version]. *The New York Times*.
- Markoff, J. D., & Kramer, A. E. (2009, June 27). U.S. and Russia Differ on a Treaty for Cyberspace. *The New York Times*.
- Miklaszewski, J. (1999, March 5). Pentagon and hackers in 'cyberwar'. In *ZDNet: Technology News*. Retrieved January 3, 2013, from <<http://www.zdnet.com/news/pentagon-and-hackers-in-cyberwar/101740>>.
- National Security Council: Cyber-security (n.d.). In *The White House*. Retrieved January 7, 2013, from <<http://www.whitehouse.gov/administration/eop/nsc/cybersecurity>>.
- Obama, B. (2009, May 29). Remarks by the President on securing our Nation's cyber infrastructure. In *The White House*. Retrieved January 4, 2013, from <[http://www.whitehouse.gov/the\\_press\\_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/](http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/)>.
- Obama, B. (2013, February 12). Executive Order: Improving Critical Infrastructure Cybersecurity. In *The White House*. Retrieved February 18, 2013, from <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>
- O'Brien, N. (2007, July 31). Virtual terrorists. *The Australian*. Retrieved January 2, 2013
- Rollins, J., & Wilson, C. (2007, January 22). Terrorist capabilities for cyber-attack: Overview and policy issues. *Congressional Research Service*.
- Saunders, R. A. (2004). Nationality: Cyber-Russian. *Russia in Foreign Affairs*. Retrieved April 17, 2010, from <<http://eng.globalaffairs.ru/numbers/9/716.html>>
- Shea, D. (2004, January 20). Critical Infrastructure: Control Systems and the Terrorist Threat. *Congressional Research Service*.
- Sweetman, B. (2009, November). H4XOR3D! Means hacked. *Defense Technology International*, 30-31.
- The military doctrine of the Russian Federation approved by Russian Federation Presidential Edict on 5 February 2010 (2010, February 2). In *The School of Russia and Asian Studies*. Retrieved January 4, 2013, from <[http://www.sras.org/military\\_doctrine\\_russian\\_federation\\_2010](http://www.sras.org/military_doctrine_russian_federation_2010)>.
- Theohary, C. (2009, March 17). Information operations, cyber-warfare, and cyber-security: Capabilities and related policy issues. *Congressional Research Service*.

- Theohary, C., & Rollins, J. (2009, September 30). Cyber-security: Current Legislation, Executive Branch Initiatives, and Options for Congress. *Con.*
- Thomas, T. L. (1996). Deterring Information Warfare: A New Strategic Challenge. *Parameters*, 81-91.
- Thomas, T. L. (2000). The Russian View Of Information War. *The Russian Armed Forces at the Dawn of the Millenium*,. Retrieved April 17, 2010, from <<http://fmso.leavenworth.army.mil/documents/Russianvuiw.htm>>
- Transcript: Obama's State Of The Union Address As Prepared For Delivery (2013, February 12). In *NPR*. Retrieved February 18, 2013, from <http://www.npr.org/2013/02/12/171841852/transcript-obamas-state-of-the-union-as-prepared-for-delivery>.
- Vistica, G. (1999, November 20). We're in the middle of a cyber-war. *Newsweek*.
- Walsh, D. C. (2009, November) Know Thine Enemy, National Consensus Needed on Network Protection. *Defense Technology International*. 39-40.
- Williams, P. D. (2009, Winter) Cyber ACTS/SAASS: A Second Year of Command and Staff College for the Future Leaders of Our Cyber Forces. *Air and Space Power Journal* 23, no. 4. 21-29.
- Wright, A. (2009, December). The unseen Cyber-War. *National Defense*, 29-32.
- Zetter, K. (2013, March 12). Spy chief says little danger of cyber 'Pearl Harbor' in next two years. In *Wired*. Retrieved March 14, 2013, from <<http://www.wired.com/threatlevel/2013/03/no-cyber-pearl-harbor/>>.