Strategy Research Project

Engaging the Nation's Critical Infrastructure Sector to Deter Cyber Threats

by

Commander Brian P. Burrow
United States Navy

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Engaging the Nation's Critical Infrastructure Sector to Deter Cyber Threats

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Commander Brian P. Burrow
United States Navy

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Lynn I. Scheel
Department of Military Strategy, Planning, and Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 6,207

14. ABSTRACT

The United States' national security is at risk. State and non-state cyber actors have increasingly gained and sustained access extending beyond military targets. The exploitation of government and private networks has left the United States vulnerable to cyber attacks on critical infrastructures, theft of intellectual properties, disruption of financial institutions, and has threatened the military's readiness and ability to operate. The secrecy of cyber threats has prevented the United States from effectively defending against those threats capable of targeting critical infrastructures. To defend and counter the cyber threat, in the interest of national security, the United States will have to engage and collaborate with the industries that maintain the nation's critical infrastructure.

15. SUBJECT TERMS
Cyber, Estonia, Georgia, China, Russia, Iran, terrorist, deterrence, exploitation, espionage

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	8 UU	36	**19b. TELEPHONE NUMBER** *(Include area code)*
UU	UU	UU			

USAWC STRATEGY RESEARCH PROJECT

Engaging the Nation's Critical Infrastructure Sector to Deter Cyber Threats

by

Commander Brian P. Burrow
United States Navy

Colonel Lynn I. Scheel
Department of Military Strategy, Planning, and Operations
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Engaging the Nation's Critical Infrastructure Sector to Deter Cyber Threats
Report Date:	March 2013
Page Count:	36
Word Count:	6,207
Key Terms:	Cyber, Estonia, Georgia, China, Russia, Iran, terrorist, deterrence, exploitation, espionage
Classification:	Unclassified

The United States' national security is at risk. State and non-state cyber actors have increasingly gained and sustained access extending beyond military targets. The exploitation of government and private networks has left the United States vulnerable to cyber attacks on critical infrastructures, theft of intellectual properties, disruption of financial institutions, and has threatened the military's readiness and ability to operate. The secrecy of cyber threats has prevented the United States from effectively defending against those threats capable of targeting critical infrastructures. To defend and counter the cyber threat, in the interest of national security, the United States will have to engage and collaborate with the industries that maintain the nation's critical infrastructure.

Engaging the Nation's Critical Infrastructure Sector to Deter Cyber Threats

> "Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."
>
> –2010 National Security Strategy[1]

Since the end of the Cold War, the United States has been involved in numerous major conflicts, from the Gulf War to the Global War on Terrorism. Over the course of these conflicts the US experienced an increase in battle space awareness, a declining role of heavy land forces, and an increasing dominance of precision weapons. Simultaneously, the US experienced vast advances in technologies. As such, these new capabilities have transformed the character of conflict, integrating instruments of modern warfare varying from mechanized artillery to sea power to air power and most recently, to cyber warfare. Over the same period, the type and domains of conflict has evolved. Where wars were once fought by a sizeable, conventional force within geographically defined boundaries, the US is now confronted with operating in cyber space, a virtual realm where barriers to entry are limited and attacks may occur anonymously with minimal or delayed risk of attribution.

The US' national security is at risk. State and non-state cyber actors have increasingly gained and sustained access extending beyond military targets. The exploitation of government and private networks has left the US vulnerable to cyber attacks on critical infrastructure, theft of intellectual properties, disruption of financial institutions, and has threatened the military's readiness and ability to operate. The secrecy of cyber threats has prevented the US from effectively defending against those threats capable of targeting critical infrastructures. To defend and counter the cyber

threat, in the interest of national security the US will have to engage and collaborate with the industries that maintain the nation's critical infrastructure.

Cyber Defined

"Every domain, by definition, has unique features that compel military operations in it to conform to its physical or relational demands."[2] While established tactics, techniques, and procedures have been developed and thoroughly tested in the domains of land, sea, air and space, the cyber domain or cyber space, a metaphor for the non-physical environment fashioned by computer systems, is relatively new. A unique challenge in the cyber domain is the fact that rapid innovations and advances in technology have surpassed the rate of policy development in support of national interests. When compared to the air domain, today cyber could be considered equivalent to the early development of flight on the beaches of Kitty Hawk with the Wright brothers.

Due to limited barriers and low costs to entry, actors have the means to attack with virtual weapons with an increased level of flexibility than ever before witnessed in the history of warfare.[3] This flexibility enables a broad list of actors, whether state or non-state, to challenge US interests through the engagement of cyber warfare. Cyber warfare as defined in the U.S. Army Concept Capability Plan for Cyber Space Operations 2016-2028 is as follows:

> Cyber warfare (cyberwar) is the component of CyberOps that extends cyber power beyond the defensive boundaries of the GIG to detect, deter, deny, and defeat adversaries. CyberWar capabilities target computer and telecommunication networks and embedded processors and controllers in equipment, systems and infrastructure. CyberWar uses cyber exploitation (CyE), cyber attack (CyA), and dynamic cyber defense (DCyD) in a mutually supporting and supported relationship with CyNetOps and CyberSpt.[4]

The Army's definition of cyber warfare essentially identifies the capability as an instrument of power, capable of use on a global scale to not only detect, deter, and deny, but also to defeat adversaries through the degradation, disruption or the control of information affecting critical systems. Cyber warfare may be understood as a means to a variety of ends: espionage, financial damage, manipulation of national critical infrastructures and influencing the course of conflict between governments, citizens, and civil societies.[5]

Cyber Threats

It is estimated that over a hundred countries have initiated some sort of cyber warfare program to deal with the cyber threat.[6] Cyber warfare is unconventional as a domain and permits actors limited in conventional military power with an asymmetric means to offset conventional disadvantages with minimal investment. The infrastructure to conduct cyber attacks is significantly more cost effective then the requirements for mechanized war fighting capabilities. The unique aspect of cyberspace also enables diversity among cyber actors that may similarly be just as diverse as their methods of attack. Cyber targets are not limited to the state apparatus or military forces, but rather include economic, environmental, social and physical domains threatened by militaries, terrorists and extremists, cyber espionage and cyber criminals.[7] The term asymmetric is often commonplace with cyber as resources do not necessarily guarantee an advantage in conflict. In terms of cyber, an individual with a single exploit can cause as much damage as an entire battalion of cyber operators, depending of course on the quality of the exploit and the skill of the attacker.[8] A well planned cyber attack could inflict significant damage, whether it is over political tensions or supporting conventional warfare.[9]

State actors motivated by geopolitics are likely to conduct cyber attacks through government sponsored programs or proxies. Cyber attack is not a new concept; observers have theorized about the concept of cyber attack for the past twenty years.[10] Cyber attacks have ranged from an individual's ego as a test of skill to highly complex and well coordinated attacks with the intent of causing destruction in the physical realm.

Solar Sunrise (1998)

In February 1998, Department of Defense (DoD) networks were exploited through known vulnerabilities of the Solaris computer system.[11] The actors probed the networks, gained access and uploaded a program designed to collect data from the network. The geographic origins of the attack were Harvard University and the United Arab Emirates via Pearl Harbor and a variety of Air Force bases. Additional monitoring of the attack identified international activity in five countries, compromising over 500 computer systems to include military, commercial, and educational sites.[12] Cyber forensics led to the source and ultimately the arrest of the attackers, two California high school students and an Israeli teenager who acted as a mentor from another country. With the use of moderately sophisticated tools, these individuals were able to penetrate DoD networks, ultimately posing a threat to national security. The lessons learned from this attack identified significant vulnerabilities of US information systems, legal implications that delayed the forensic process and the identification of the attackers, and government bureaucracies that delayed a timely response.

Estonia (2007)

During the spring of 2007, Estonia's internet was held hostage to cyber attacks lasting over two weeks. The motivation driving the attacks was over a dispute regarding the movement of a monument of historical significance. Estonia had been under rule of

the Soviet Union from 1940 to 1991. While the Russians may have protected Estonia from falling to Nazi Germany in World War II, the Estonian government viewed the Russian occupation as being illegal. Since gaining independence in 1991, animosity between Estonians and ethnic Russians had escalated over political tensions.[13]

The monument in dispute, located in the city center of Tallinn, Estonia, was a bronze statue of a Russian soldier as a monument to all who sacrificed their lives during World War II. The Bronze Soldier of Tallinn had become a staging site for political demonstrations against the Estonian government, leading to Estonian government's decision to move the monument.[14] As a result of the decision to move the monument, riots ensued accompanied by cyber attacks aimed at the country's internet infrastructure affecting banks, media outlets and government websites. Despite the protests and cyber attacks, the monument was eventually moved to a new location.

The initial attacks were in the form of a denial of service (DOS) with how-to instructions posted on Russian websites specifying which Estonian websites to attack.[15] The initial DOS attacks carried out were considered to be ineffective. However, a second wave of cyber attacks in the form of a distributed denial of service (DDOS) threatened essential services and did considerable damage to the economy.[16] DDOS attacks are based on multiple, malware infected personal computers, organized into networks called botnets, and are directed by hackers to simultaneously send large numbers of requests to a targeted website or websites with the intent to overload the web server and shut it down.[17] The owner of a computer is often unaware his or her computer has been infected and is participating in a cyber attack. The DDOS attacks were conducted with such sophistication that industry experts suspect the attacks were

state-sponsored, originating from Russia. The significance of the attack was not the method or purpose behind the attack, but rather the attack was directed at a country's national security.[18]

Georgia (2008)

Almost one year later the country of Georgia experienced what is thought to be the first ever combined kinetic and cyber attack using many of the same techniques and computers from the attacks against Estonia.[19] On July 20, 2008 the official website of the Georgian president became the target of a DDOS attack. On that same day the Shadowserver Foundation, an internet watchdog group that specializes in tracking malicious online activities, identified DDOS attacks aimed at the Georgian President, shutting down the presidential website for over 24 hours. [20] According to the researchers, the server to launch the attack was based in the US, demonstrating cyber conflicts may occur without the restriction of boarders, additionally questioning the acceptability of retribution.[21]

Approximately one month later on August 8, 2008, a massive wave of cyber attacks was launched targeting Georgia's internet infrastructure. [22] The second attack was inherently different from the first as it was accompanied with a kinetic attack where conventional Russian forces engaged Georgian forces in combat while the cyber attacks were occurring. This is the first time in history armed conflict occurred simultaneously with a cyber attack.[23] At the onset of the war, websites such as stopgeorgia.ru were made available online to hacktivists, a term used to describe politically or socially motivated hackers, and provided a list of Georgian websites to attack with instructions on how to carry out the attacks.[24] The first coordinated online attacks were detected by the Shadowserver Foundation as being from six different

botnets, traced back to locations inside Russia and Turkey, which shut down “websites of the President of Georgia, the Georgian Parliament, the Ministries of Defense and Foreign Affairs, the National Bank of Georgia, and the online news agencies The Messenger and Civil.ge.” [25] Hacktivists defaced websites of the Ministry of Foreign Affairs and National bank with digitally altered images of the Georgian President resembling the Nazi leader Adolph Hitler. [26] In addition to the DDOS techniques used throughout this conflict, another cyber attack, an information operations campaign, was carried out to shape public opinion through phony web sites.[27]

Ambassador David Smith, former US Ambassador at the US-Soviet Defense and Space talks, suggests that when considering “the forensic evidence, geopolitical situation, timing and the relationship between the government and the youth and criminal groups, it is not difficult to conclude that the Kremlin was behind it all.”[28] While the Kremlin denied involvement in the attacks, it did not condemn the actions of those involved.

Of the two attacks on Estonia and Georgia, it was Estonia that had the greatest damage to its economy due to its reliance on information systems and being fully integrated with the internet. Estonia’s internet integration enabled the country to shift its government operations online such as national election electronic voting and cabinet-level meetings. At the time of the attacks, Estonia was ranked 23 in e-readiness ratings, well before its time as a small country. [29] In comparison, the actual damage to Georgia’s internet infrastructure was relatively minimal considering the potential damage that could have occurred if the country was more heavily integrated electronically. At the time of the attack only seven percent of the Georgian population

had access to the internet, ranking the country at 74 of 234 nations integrated with the internet.[30] Even though the attacks were minimal in damage and only lasted for a short time, the attacks were successful in disrupting the country's ability to communicate with the international community.

With most media reports on cyber attacks focused on Chinese cyber activities, the US should not be distracted from the Russian cyber threat. Retired General Richard Clarke, former White House Cyber Coordinator, stated the Chinese cyber threat is not the greatest the US is faced with, but rather the capabilities of the Russians are superior to those of the Chinese and considered to be almost as good as those of the US.[31]

Cyber Espionage

Unlike other warfare domains, cyber warfare is almost always conducted in great secrecy. The concept of cyber warfare being conducted in secrecy aligns with Sun Tzu's deceptive philosophies. Sun Tzu, a strategist, a philosopher, and a Chinese military general, authored circa 500 B.C., *The Art of War*, a book on military strategy and tactics definitive of its time.[32] Cyber aligns with Sun Tzu's philosophies such as "All warfare is based on deception. When able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near."[33] From an intelligence perspective, exploiting an enemy's information systems may be the key to victory in any war. Sun Tzu states, "Know the enemy and know yourself; in a hundred battles you will never be in peril."[34] Information superiority through cyber espionage is the key to success, suggesting a gained access to operational plans, military doctrine, asset location, capabilities and technologies will prove invaluable to offensive forces.

Admiral Mike McConnell, former Director of National Intelligence, addressed congress stating China has a national policy of espionage in cyberspace and is "…the world's most active and persistent practitioner of cyber espionage today."[35] Chinese military doctrine and journals have also suggested cyber attacks are a form of espionage with the intent of extracting adversary intelligence.[36] In 2003 the Chinese announced the development of a cyber warfare program established between two units, the Third Technical Department of the People's Liberation Army (PLA) and the Lingshui Signals Intelligence Facility.[37] These two organizations were responsible for both offensive and defensive cyber operations. Since China's initial announcement of its cyber program, the country has integrated its cyber capabilities within its strategic framework with a focus on cyber espionage and the use of proxy hackers to advance political, economic and security objectives.[38] Recently, China has further integrated its cyber capabilities with a variety of military entities to include the PLA headquarters and each PLA branch to include:

- 2PLA: The Second Department of the PLA General Staff Department (2PLA) is responsible for military intelligence. It may use cyber operations as part of its collection activities.
- 3PLA: The Third Department of the PLA General Staff Department (3PLA) is responsible for the collection of signals intelligence. This includes computer network exploitation, reportedly drawing upon Technical Reconnaissance Bureaus geographically distributed across the country. It may also lead the PLA's computer network defense efforts.
- 4PLA: The Fourth Department of the PLA General Staff Department (4PLA) engages in electronic warfare. In addition, it appears to be responsible for computer network attack.
- PLA services: The PLA Navy and PLA Air Force, like 3PLA, operate Technical Reconnaissance Bureaus that may engage in computer network operations. The Second Artillery Forces, a PLA service-level

branch responsible for nuclear and conventional missiles, may also have cyber-related responsibilities.

- Cyber warfare militias: A subset of the PLA militia has cyber-related responsibilities. These units, usually comprised of workers with high-tech day jobs, focus on various aspects of military communications, electronic warfare, and computer network operations.[39]

It is also estimated state sponsored exploitation is coordinated through independent groups and Chinese corporations involved in information technology and telecommunications.[40]

An earlier report from the Congressional Research Service (CRS) stated, “The Chinese concept of cyber warfare incorporates unique Chinese views of warfare based around the People’s War concept (modern) and the 36 Stratagems (ancient)."[41] The 36 stratagems referenced by the CRS accredit the works of Sun Tzu, emphasizing deception, knowledge-style warfare, and an asymmetrical advantage over an enemy. A 2012 report by the U.S - China Economic and Security Review Commission recognizes leaders of the PLA embrace the theory that successful war fighting is directly linked to the ability to control an adversary’s information and information systems. [42] PLA analysts have specifically identified C4ISR (Command, Control, Communications, Intelligence, Surveillance and Reconnaissance) as centers of gravity as well as a weakness for the US and will most likely target those capabilities in the event of conflict.[43] To prevent the US from intervening in conflict in the Western Pacific, the PLA has integrated cyber warfare and space warfare into operational planning, specifically targeting U.S. satellites and surveillance assets.[44]

Shortly after the announcement of China’s cyber program, an attack identified as Titan Rain had begun. A Federal Bureau of Investigation (FBI) effort indentified the advanced persistent threat as a series of cyber attacks over a three year period. Titan

Rain targeted US government agencies and defense contractor networks, extracting data critical to protecting national security.[45] Attacks targeted Army Research Labs, Lockheed Martin, NASA, the World Bank, Sandia Labs, government agencies, military installations, and defense contractors. An estimated 10 to 20 terabytes of data were stolen.[46] While the specific origins of Titan Rain were unknown, investigators traced the flow of data back to a final server in Guangdong, China.[47] While the attack could be attributed to Chinese hacktivists, the sophistication and techniques used to extract such large volumes of data over several years would suggest a state sponsored cyber attack by the Chinese government.

China's investment in cyber capabilities and actions in cyber space pose a threat to US national security. The United States – China Economic and Security Review Commission's 2012 annual report states:

> In 2012, Chinese state-sponsored actors continued to exploit government, military, industrial, and nongovernmental computer systems. Any individual penetration remains difficult to attribute, but security researchers are increasingly able to group exploitations into ''campaigns'' based on common features and gain better insight into those responsible. Although most China- based activity observed over the past year relied on basic and straightforward techniques, a series of new developments suggest Chinese exploitation capabilities are improving significantly. Irrespective of sophistication, the volume of exploitation attempts yielded enough successful breaches to make China the most threatening actor in cyberspace.[48]

To complement the commission's report, a recent announcement by a US based security company, Mandiant, reported evidence of Chinese hacking activities that involved over 141 organizations and spanned 20 major industries.[49] Targeted organizations included US based corporations, organizations and government agencies as well as defense contractors and utility companies. The report was based on a six year investigation that tracked members of a Chinese hacker group tied to Unit 61398, a

unit within the PLA. Hundreds of terabytes were stolen from targeted industries China identifies as essential to the country's strategic growth.[50] Of the industries targeted, four out of seven were identified in China's Five Year Plan.[51] Most of the attacks occurred over the course of months, some over years, and most concerning was the rise in cyber activity over the past two years to include targeted critical infrastructure such as oil pipelines and power grids.

Both reports identify China's cyber activities as oriented towards the theft of intellectual properties and the collection of economic, financial or other types of data.[52] Cyber intrusions of military and government networks are mostly focused on intelligence gathering.[53] These types of activities require the same access needed for a cyber attack and with little effort, as long as access has been achieved, a compromise of a network could easily become disruptive or destructive.[54]

Cyber as a Physical Attack

Iran has been a significant concern for the US since the Ayatollah Khomeini came to power in 1979 as a result of the Iranian revolution. Since the Ayatollah's rise to power, the Iranian government has portrayed deeply rooted anti-American sentiment towards western civilizations. In that same year, the US Embassy in Tehran was stormed by students and militants taking 52 Americans hostage for 444 days. Almost a decade later in 1988, the USS VINCENNES misidentified an Iranian commercial airliner as a hostile fighter aircraft and shot it down, killing all 290 passengers on board. In 1993 the U.S. implemented a policy known as "dual containment" toward Iran and Iraq in an effort to isolate both countries and restrain their regional ambitions. In 2002 Iran was first accused of building nuclear weapon capabilities. In 2005 Iran resumed its

uranium conversion; the International Atomic Energy Agency reported Iran as violating the nuclear non-proliferation treaty.

As a state sponsor of terrorism, Iran was ultimately responsible for the 1983 bombing of the Marine Corps barracks in Beirut and the 1996 attack on the Khobar Towers in Saudi Arabia, killing a combined 260 US servicemen. Up until 9/11, it was Iran's chief proxy, Hezbollah, which held the mantle of deadliest terrorist organization, killing more Americans than any other terrorist group.[55] Tensions between the US and Iran have remained high as reflected by attempted and actual attacks on Israeli, US, and other western interests as well as coordinated bomb attacks on embassies in Israel, India, and Georgia. More recently, US intelligence prevented an Iranian sponsored plot to assassinate Saudi Arabia's Ambassador to the US.[56] While Iran attempts to distance itself from the incidents, US officials have indicated Iran's involvement with high levels of confidence.[57]

Iran's illicit nuclear program has significantly contributed to the rise in tensions. The US and the United Nations Security Council have been persistent with Iran to end its program of uranium enrichment due to concerns of the development of a nuclear weapon. In 2009, Iran's nuclear program was attacked by a virus known as Stuxtnet, a large and complex virus that targets industrial control systems used on gas pipelines and power plants.[58] Stuxtnet was designed to reprogram industrial control systems by altering the code on programmable logic controllers so the system operates in a manner determined by the attacker while hiding the changes from system operators. [59] Variants of Stuxnet targeted five Iranian organizations with the most probable target suspected to

be the uranium enrichment infrastructure in Iran.[60] The virus disabled centrifuges and delayed enrichment for approximately one year.

Stuxtnet was the first cyber attack to specifically target an industrial process and is a prime example of cyber and physical domains intersecting. Stuxnet demonstrated that critical infrastructures can be physically disabled or destroyed by a motivated adversary. While there is no definitive evidence of Stuxnet's origin, speculation points to a combined attack coordinated by the US and Israel. Since the initial Stuxnet attack, Iran's nuclear program has been infected by four additional types of malware to include, "Stars, a software script targeting execution files; DuQu, a successor to Stuxnet aimed at gaining remote access to Iran's nuclear systems; another piece of malware named Wiper, which attacked internal Internet communications; and, most recently, Flame, a cyber espionage virus."[61]

At a joint hearing on the "Iranian Cyber Threat to the U.S. Homeland", the Subcommittee on Counterterrorism and Intelligence reported Iran had conducted cyber attacks on news organizations, BBC and Voice of America, the Chinese search engine Baidu, Iranian websites managed by the opposition Green Movement and attempted to exploit a major Israeli financial institution.[62] Iran has also been publically testing its cyber capabilities within its region with high visibility, suggesting the use of cyber proxies by the Iranian Revolutionary Guard Corp (IRGC). Elements of the IRGC provide the manpower for Iran's cyber operations by openly recruiting hackers for the regime. [63] More recently, Iran is believed to have been behind a series of attacks in late 2012 through a massive DDOS attack taking down websites for banks based in the US.[64] Additionally, in 2008 a security-contracting firm rated Iran's cyber capability as

being among the top five globally. [65] Another report from 2011 indicated that Tehran invested over one billion dollars in new cyber warfare technologies.[66] That same year an Iranian newspaper claimed cyberwarfare was not an exclusive capability of the US and the Islamic Republic should not be underestimated.[67] The paper additionally implied the US should be concerned of an attack against its critical infrastructure from an unknown actor, insinuating Iran's intentions to conduct a cyber attack against the US.

When considering the history between Iran and the US and the regime's abrasive foreign policy, it is likely Iran will initiate cyber attacks against the US or other western interests. A breakdown in diplomatic negotiations, an increase in economic sanctions, or the use of force against Iran's nuclear facilities may compel Iran to retaliate through cyber means. [68] While Iran may lack the cyber sophistication to conduct a complex attack against the US, it maintains a relationship with proxies that offer cyber capabilities to those with intent and monetary resources.[69]

Strategy

The *2010 National Security Strategy* identifies cyber security threats as representative of one of the most serious national security, public safety, and economic challenges Americans face as a nation.[70] The reliance on the Nation's information infrastructure is enormous; the DoD alone operates over 15,000 networks and seven million computing devices among hundreds of installations in countries all around the world.[71] The American way of life and public safety are dependent on critical infrastructures that control power, water, transportation and financial institutions, all susceptible to cyber vulnerabilities capable of permitting disruption on a colossal scale.

State and non-state actors continuously probe critical U.S. infrastructure with the intent to deny, degrade or destroy.

To provide guidance to counter the cyber threat, in 2011 the DoD released the *Department of Defense Strategy for Operating in Cyberspace* on the premise cyber attacks will be a significant component of future conflicts. The document provides an assessment of the challenges and opportunities of an increasing reliance on cyberspace for military, intelligence, and business operations. The strategic approach to the DoD cyber mission is outlined with five strategic initiatives:

- Strategic Initiative 1: Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential
- Strategic Initiative 2: Employ new defense operating concepts to protect DoD networks and systems
- Strategic Initiative 3: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy
- Strategic Initiative 4: Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity
- Strategic Initiative 5: Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation[72]

Part of the DoD strategy is to share situational awareness and warning capabilities with federal agencies and international allies to establish a united cyber defense and enhanced collective deterrence. [73] According to the Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, deterrence is defined as, "The prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits."[74] This definition consists of two basic principles. The first principle of

deterrence is the perception, by the actor, of futility in attempting to achieve the objective. In terms of cyber, an impenetrable, hardened network would be a form of deterrence. The attacker acknowledges his or her efforts would be ineffective and not worth the cost or level of effort required to conduct the attack. However, while some networks are more secure than others, the thought of an impenetrable network is not very realistic. The proliferation of capabilities and resources greatly reduces the level of effort required to conduct a cyber attack and will not likely deter an actor if the cost is perceived to be low to non-existent and the potential benefit is significant.

The second principle to deterrence is to impose costs, a form of retribution using the national instruments of power to include military action in the form of a cyber or kinetic attack. In regards to nuclear armed nation-states, an effective form of deterrence during the cold war was based on the concept of mutually assured destruction (MAD). MAD is perhaps the most iconic form of deterrence the US has leveraged over the past fifty years as a nuclear power. The idea is the US can withstand an initial attack long enough to counterstrike with nuclear weapons. As world powers pursued supremacy over the nuclear arms race, the second strike deterrence fell short of expectations and was essentially replaced by the notion that all nuclear powers, if engaged in nuclear war, faced mutual destruction. In this situation, "… the probability of nuclear war is reduced not by the balance (number of forces of both sides) but rather by the stability of the balance. The balance is stable if neither opponent, in striking first, gains the advantage of destroying the other's ability to strike back."[75]

It would appear the US is in a similar situation with regards to cyber space. As world powers continue to build offensive cyber capabilities, the theory of deterrence

essentially eliminates cyber aggression through the trepidation of retaliation. However, there are significant differences between nuclear MAD and cyber deterrence. First, in terms of a nuclear deterrence, the aggressor is known and retribution is assured. Whereas in cyber space, actors maintain anonymity through the use of false IP addresses, aliases, and hide behind multiple servers in foreign countries, making it difficult, if not impossible to determine the origin of the attack, as demonstrated in Estonia and Georgia. Second, the aggressor has to believe the opponent has the means and will to conduct a more costly counter attack as a form of retribution.

Deterrence through retribution comes with significant risks. The US must, without a reasonable doubt, accurately identify the attacker. A mistaken identity will not only have negative consequences in the international community but will likely ignite tensions and possibly a conflict with an unintended opponent. However, a policy of deterrence, to include retribution, will be disregarded if unchallenged and will likely draw an increase of cyber attacks aimed at the US. The US will have to weigh the risks of taking action versus inaction and the political acceptability of retaliation, whether it is in the form of a cyber or kinetic response. Ultimately, the US has the inherent right to defend itself from hostile acts, to include cyber attacks, and should exhaust all available courses of action before applying force.[76]

Critical Infrastructure

Until recently, the US compartmentalized its cyber defenses and investigation of cyber attacks to military and government organizations, leaving civilian owners and operators of various critical infrastructures to fend for themselves. The private sector does not have the capability or the resources to defend against current and emerging cyber threats as outlined in recent reports by Mandiant and the United States – China

Economic and Security Review Commission. To bring the private sector into the equation, the US needs to expand programs permitting collaboration between government and private entities.

In April of 2012, the Cyber Intelligence Sharing and Protection Act (CISPA) was passed by the House of Representatives. This proposed law would have permitted the sharing of internet traffic between the US government and certain technology companies in the private sector. However, the Senate did not pass the bill over concerns of confidentiality and civil liberties. The bill, if passed, would have assisted government agencies in the investigations of cyber threats and the security of networks against cyber attacks.[77] However, it was not until February 2013 that the President of the US issued an Executive Order to improve cyber security.

Executive Order 13636, Improving Critical Infrastructure Cybersecurity, is aimed at enhancing the cybersecurity of critical infrastructure, a term defined to include systems and assets "…so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[78] A Presidential Policy Directive further identifies 16 industries as components of the nation's critical infrastructure: chemicals, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems, water and waste water systems.[79] The EXORD includes four basic

components; Cybersecurity Information Sharing, Cybersecurity Framework, Critical Infrastructure Cybersecurity Program, Privacy and Civil Liberties Protections.

Cybersecurity Information Sharing. This component directs the government to "increase the volume, timeliness, and quality of cyber threat information shared with private sector entities."[80] This information would contain classified and unclassified information regarding cyber threats to critical infrastructure entities. Procedures will also be developed to expand on the Enhanced Cybersecurity Services program, a program coordinated between the DoD and the Department of Homeland Security (DHS) to protect information on defense industrial based company systems. This expansion will be made available to all critical infrastructure sectors and will provide "classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure."[81]

Cybersecurity Framework. The National Institute of Standards and Technology (NIST) will take the lead in developing a framework of baseline "standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[82] The framework will be based on best practices and industry standards to the fullest extent possible and will also provide technology-neutral guidance to account for differences amongst organizations.

Critical Infrastructure Cybersecurity Program. The DHS, in collaboration with sector specific government agencies will establish a voluntary program to incentivize adoption of the framework by critical infrastructure owners and operators. Government

agencies will assess the benefits and effectiveness of the proposed incentives and determine whether or not further legislation is required to legally offer the incentives.

Privacy and Civil Liberties Protections. Privacy and Civil-Liberties Protections incorporate privacy safeguards. Federal agencies will be required to ensure the privacy and civil liberties of critical infrastructure activities are adhered to in accordance with existing policies, principles, and frameworks. Additionally, the DHS Chief Privacy officer and the Officer for Civil Rights and Civil Liberties are required to assess risks to privacy and civil liberties and provide recommendations to reduce such risks.

In the absence of legislative action, the EXORD is a significant step in the right direction for protecting critical infrastructures and is the first of its kind since the Federal Information Security Management Act of 2002.[83] However, mandates or requirements to strengthen critical infrastructure cybersecurity are lacking in the EXORD. To secure effectively the nation's critical infrastructures, a unity of effort is required to counter the cyber threat. Without legislation, participation is strictly voluntary. Therefore, information may flow unilaterally and while the organization may be entitled to receive threat information from the government, it has no legal obligation to report cyber threats or adopt the framework standards set forth by the NIST. To establish a collective defense, the private sector of critical infrastructure should be required to collaborate with federal agencies to ensure standards are applied and cyber anomalies are reported.

The greatest obstacle for approving this legislation is the concern over privacy. While the EXORD provides guidelines for protecting privacy and civil liberties, it does not discuss the extent or level of accountability for protection in the event of cyber threat

activities. To move forward, the federal government will have to increase transparency in the handling of privacy data if such an event were to occur.

Until cybersecurity legislation for critical infrastructure is passed, per the EXORD, incentives will have to be implemented to maximize an organizations' adoption of the cybersecurity framework. Tax breaks and liability protection are two effective incentives for organizations whose primary concerns are profit margins. Another option is the collaborated use of technical resources and capabilities. While some organizations may have an advanced cybersecurity monitoring system, others who are lacking in sophistication would benefit from the use of tools and services provided by the government, e.g. intrusion detection systems, forensic analysis tools and forensic services. Trial programs should be adopted in the sense organizations may be more inclined to participate if further clarity of the cyber threat was provided.

Conclusion

Adversaries are as diverse in their capabilities as they are in their motives and while network vulnerabilities have permitted the theft of intellectual property, it is those same vulnerabilities that expose the US to a cyber attack on critical infrastructure. The US reports of Chinese activities against US organizations prove the US is vulnerable and countries such as Iran are likely to take advantage of those vulnerabilities. The term "the best defense is a good offense" does not apply here. Retribution is not likely to deter a cyber attack or have any impact at all, at least not until the US demonstrates it has the will and the capability and to effectively retaliate against an aggressor.

While the US continues to harden government networks, hire talented and skilled cyber operators, and develop a whole of government approach to combating the cyber threat, it is active engagement with the private sector that will lead to a paramount

cyber defense of the nation's critical infrastructure. It is the sharing of cyber activities, malicious threat signatures and information on cyber threats that will lead to a shared situational awareness, a collective cyber defense and a collective deterrence.

Endnotes

[1] Barrack Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 27.

[2] Keith B. Alexander, "Statement of General Keith B. Alexander, Commander, United States Cyber Command, Before the Senate Committee on Armed Services", (March 27, 2012), http://www.armed-services.senate.gov/statemnt/2012/03%20March/Alexander%2003-27-12.pdf (accessed February 27, 2013).

[3] Kenneth Geers, *Sun Tzu and Cyber War*, (Cooperative Cyber Defense Centre of Excellence 2010), http://www.ccdcoe.org/articles/2011/Geers_SunTzuandCyberWar.pdf, (Accessed September 24, 2012).

[4] U.S. Department of the Army, *The U.S. Army Concept Capability Plan for Cyberspace Operations 2016-2028*, TRADOC Pamphlet 525-7-8, (Washington D.C.: U.S. Department of the Army, February 22, 2012), 21.

[5] Kenneth Geers, *Sun Tzu and Cyber War*.

[6] Don Eijndhoven, *Cyber Deterrence – Methods and Effectiveness*, (Argent Consulting, November 2, 2010), 7, http://www.infosecisland.com/documentview/12733-Cyber-Deterrence-Methods-and-Effectiveness.html (accessed January 13, 2013).

[7] Paul Cornish et al, *On Cyber Warfare*, (London: The Royal Institute of International Affairs, Chatham House, November 2010), 5, http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf (accessed January 13, 2013).

[8] Don Eijndhoven, *Cyber Deterrence – Methods and Effectiveness*, 7.

[9] Paul Cornish et al, *On Cyber Warfare*, 9.

[10] Keith B. Alexander, "Statement of General Keith B. Alexander, Commander, United States Cyber Command, Before the Senate Committee on Armed Services".

[11] Steven A. Hildreth, *Cyber Warfare* (Washington D.C.: U.S. Library of Congress, Congressional Research Service, June 19, 2001), 20.

[12] Ibid, 5.

[13] William C. Ashmore, *Impact of Alleged Russian Cyber Attacks*, School of Advanced Military Studies Monograph, (Fort Leavenworth, KS: United States Army Command and General Staff College, May 2009), 5, http://www.dtic.mil/dtic/tr/fulltext/u2/a504991.pdf (accessed January 3, 2013).

[14] Ibid.

[15] David J. Smith, "How Russia Harnesses Cyberwarfare," *Defense Dossier*, no 4, (August 2012): 9, http://www.afpc.org/files/august2012.pdf (accessed February 9, 2013).

[16] Ibid.

[17] Alexander Melikishvili, "Recent Events Suggest Cyber Warfare Can Become New Threat*," WMD Insights*, no 29 (December 2008/January 2009), 25, http://cns.miis.edu/wmd_insights/WMDInsights_2009_01.pdf (accessed January 13, 2013).

[18] William C. Ashmore, *Impact of Alleged Russian Cyber Attacks*, 5.

[19] David J. Smith, "How Russia Harnesses Cyberwarfare," 9.

[20] Alexander Melikishvili, "Recent Events Suggest Cyber Warfare Can Become New Threat*,"* 25.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] David J. Smith, "How Russia Harnesses Cyberwarfare," 9.

[25] Alexander Melikishvili, "Recent Events Suggest Cyber Warfare Can Become New Threat*,"* 25.

[26] Ibid.

[27] Timothy Thomas, "The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia," *Journal of Slavic Military Studies* 22, no 1 (2009): 55-59, http://fmso.leavenworth.army.mil/documents/thru-the-mountain.pdf (accessed January 19, 2013).

[28] David J. Smith, "How Russia Harnesses Cyberwarfare," 9.

[29] Alexander Melikishvili, “Recent Events Suggest Cyber Warfare Can Become New Threat*,”* 26.

[30] Ibid, 25.

[31] Richard Clarke, *Cyber War: The Next Threat to National Security and What to do About It* (New York: Harper Collins Publishers, 2010), 63.

[32] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), vii.

[33] Ibid, 66.

[34] Ibid, 84.

[35] Larry Wortzel, “The Chinese Way of (Cyber) War,” *Defense Dossier*, no 4, (August 2012): 2, http://www.afpc.org/files/august2012.pdf (accessed February 9, 2013).

[36] David Lague, “Chinese See Military Dependence on Computers as Weakness,” August 29, 2007, http://www.nytimes.com/2007/08/29/world/asia/29iht-cyber.1.7299952.html?pagewanted=all&_r=0 (accessed January 3, 2007).

[37] Richard Clarke, *Cyber War: The Next Threat to National Security and What to do About It,* 57.

[38] U.S.-China Economic and Security Review Commission, *2012 Report to Congress on the U.S.-China Economic and Security Review Commission* (November, 2012), 147, http://origin.www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress.pdf (accessed March 2, 2013).

[39] Ibid, 149-150.

[40] Ibid, 168.

[41] Steven A. Hildreth, *Cyber Warfare*, 12.

[42] Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Northrop Grumman Corp, March 7 2012), 9, http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf (accessed February 9, 2013).

[43] Ibid.

[44] Larry Wortzel, “The Chinese Way of (Cyber) War,” 1.

[45] Richard Stiennon, *Surviving Cyber War (Lanham, MD:* The Scarecrow Press, 2010), 1-10.

[46] Richard Clarke, *Cyber War: The Next Threat to National Security and What to do About It,* 58.

[47] Ibid.

[48] U.S.-China Economic and Security Review Commission, *2012 Report to Congress on the U.S.-China Economic and Security Review Commission*, 168.

[49] Mandiant, *APT1: Exposing of China's Cyber Espionage Units (*February, 2013), 3, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (accessed February 22, 2013).

[50] Ibid, 4.

[51] Ibid.

[52] U.S.-China Economic and Security Review Commission, *2012 Report to Congress on the U.S.-China Economic and Security Review Commission*, 166.

[53] Ibid.

[54] Ibid.

[55] Statement of Frank J. Cilluffo, The U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence; and Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, *The Iranian Cyber Threat to the United States*, April 26, 2012, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Cilluffo.pdf (accessed January 21, 2013).

[56] Andrea Stone, "Iran Plot to Assassinate Saudi Ambassador Foiled by DOJ Sting," December 11, 2011, http://www.huffingtonpost.com/2011/10/11/iran-terrot-plot-saudi-arabia-ambassador-us-assassination_n_1005861.html.

[57] Statement of Frank J. Cilluffo, *The Iranian Cyber Threat to the United States*.

[58] Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxtnet Dossier*, Symantic Security Response, February, 2011, 2. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (accessed March 1, 2013).

[59] Ibid.

[60] Ibid, 7.

[61] Ilan Berman, “Cyberwar and Iranian Strategy,” *Defense Dossier*, no 4, (August 2012): 13, http://www.afpc.org/files/august2012.pdf (accessed February 9, 2013).

[62] Statement of Frank J. Cilluffo, *The Iranian Cyber Threat to the United States*.

[63] Ibid.

[64] David Goldman, “The Real Iranian Threat: Cyberattacks”, November 5, 2012, http://money.cnn.com/2012/11/05/technology/security/iran-cyberattack/index.html (accessed January 21, 2013).

[65] Statement of Chairman Lungren, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Joint Hearing, *Iranian Cyber Threat to the U.S. Homeland* (April 26, 2012)

[66] Statement of Frank J. Cilluffo, *The Iranian Cyber Threat to the United States*.

[67] Ilan Berman, “Cyberwar and Iranian Strategy,” 14.

[68] Statement of Frank J. Cilluffo, *The Iranian Cyber Threat to the United States.*

[69] Ibid.

[70] Barrack Obama, *National Security Strategy*, 27.

[71] Department of Defense, *Department of Defense Strategy for Operating in Cyber Space*, July 2011, http://www.defense.gov/news/d20110714cyber.pdf (accessed January 3, 2013), 1.

[72] Ibid, 5-10.

[73] Ibid, 9.

[74] JP 1-02, *Military and Associated Terms*, November 8, 2010, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed March 1, 2013), 85.

[75] Graham Allison and Philip Zelikow, *Essence of Decision, Explaining the Cuban Missile Crisis* (New York: Addison-Wesley Educational Publications, 1999), 14.

[76] Keith B. Alexander, “Statement of General Keith B. Alexander, Commander, United States Cyber Command, Before the Senate Committee on Armed Services”.

[77] House Rules Committee, *Text of HR 3523, The Cyber Intelligence and Protection Act*, April 19, 2011, 1-3, http://www.rules.house.gov/Media/file/PDF_112_2/LegislativeText/CPRT-112-HPRT-RU00-HR3523.pdf (accessed March 1, 2013).

[78] Barack Obama, *Executive Order 13636, Improving Critical Infrastructure Cyber Security* (Washington D.C.: February 12, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (accessed March 1, 2013).

[79] Barack Obama, *Presidential Policy Directive -- Critical Infrastructure Security and Resilience* (Washington D.C.: February 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed March 1, 2013)

[80] Barack Obama, *Executive Order 13636, Improving Critical Infrastructure Cyber Security.*

[81] Ibid.

[82] Ibid.

[83] Erick A. Fischer et al, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress* (Washington D.C.: Library of Congress, Congressional Research Service, March 1, 2013), https://www.fas.org/sgp/crs/misc/R42984.pdf (accessed March 10, 2013)

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu