

**The Strategic Evaluation of  
The National Strategy to Secure Cyberspace**

**By: Peter H. Chen**

## Overview

Cyberspace is an essential critical infrastructure for many Americans today. It is the ability to communicate without boundaries that empowers us to perform many different tasks. Although cyber related threats existed prior to the September 11<sup>th</sup> attacks, it is often overlooked by the general public and politicians. As of today, many of our nation's critical infrastructures are all interconnected via cyberspace; it poses a serious vulnerability in the event of another terrorist related cyber attack (i.e. "Cyber Pearl Harbor"). The creation of the National Strategy of Secure Cyberspace is a U.S. government initiative to increase the awareness of cyber related threats to the American public. It provides a basic framework for protecting this nation's critical infrastructure that is essential to our economy, security, and way of life.<sup>1</sup> Although the proposed strategies encompass all sectors of the industry, including the American public, it lacks a clear decisive strategic approach in the realm of Information Warfare.

## Overall Strategies/Priorities

The National Strategy of Secure Cyberspace consists of five priorities. They are:

1. A National Cyberspace Security Response System
2. A National Cyberspace Security Threat and Vulnerability Program
3. A National Cyberspace Security Awareness and Training Program
4. Securing Government's Cyberspace
5. National Security and International Cyberspace Security Cooperation

The goals for the purposed National Strategy of Secure Cyberspace are the following:

- Promote the understanding/awareness of threats and vulnerabilities in Cyberspace to the general public, state governments/institutions, higher education (schools, universities, etc), public sectors, and private sectors.
- Propose both public sectors (government) and private sectors to allocate funds to develop and implement new protocols to guard against possible attacks. For example: the transition from IP version 4 to IP version 6.
- Implement a National Cyberspace Security Response Team to provide strategic and tactical analysis of cyber attacks and vulnerability assessments.<sup>2</sup> By implementing a security response system/institution, it will allow firms/industries to share information regarding security intrusions/attacks. The information will be shared among the American community in order to increase the defense of future attacks. The Cyberspace Security Response Team will also issue warnings regarding potential cyber threats/attacks similar to the Homeland Security Terrorists warning system.
- Seek for voluntary participation between the national government and private sectors to develop effective offensive and defensive strategies combating against cyber attacks. This includes research and development of new security protocols, mechanisms, etc.
- Promote the North America Safe Cyber Zone and the establishment of International Watch-and-Warning system to detect and prevent Cyber attacks.<sup>3</sup>
- Evaluate and assess the current Federal Cyber Systems and their critical infrastructures.

## Detail Summary of Priorities and Concerns

### Priority One: A National Cyberspace Security Response Team

The purpose for the development of a National Cyberspace Security Response Team is to provide a centralized reporting system for both the public and private sectors to submit their cyber intrusion and

---

<sup>1</sup> President's George Bush's Introduction to The National Strategy to Secure Cyberspace.

<sup>2</sup> Page X of The National Strategy to Secure Cyberspace.

<sup>3</sup> Page 51 of The National Strategy to Secure Cyberspace

vulnerability assessments. In addition, organizations can also share valuable information regarding their cyber defensive and offensive strategies (this includes corporate security policies, positioning of their critical systems, etc). Using this collected data, it will allow National Cyberspace Security Response Team (Operated by Department of Homeland Security) to provide the following:

1. Analysis: The development of tactical and strategic analysis and vulnerability assessments. This is done by the DHS Analysis Center under the proposed Security Response Team. The primary goal for this department is to analyze security incidents, malwares/toolkits, vulnerabilities, trends, and attacker's intentions. Through analysis and research the DHS Analysis center can provide tactical security strategies (offensive and defensive strategies) to degrade the enemy's ability to wage war/attacks.
2. Warning: The DHS Incident Operations Center issues warnings in regards to future or current cyber attacks. The objective of this warning system is to create a single point of contact between the federal government and private sector to exchange security incidences and issue cyber warnings. In the realm of Information Warfare, issuing warnings will allow our nation to have a better situational awareness and intelligence in regards to imminent cyber attacks.
3. Incident Management: Provide federal coordination between the federal, state, and local government on cyber related security incidences.
4. Response and Recovery: Provide contingency and recovery plans for both federal and private sectors. The National Security Response Team will assist public and private sectors to develop policies/strategies regarding crisis and cyber risk management and business continuity plans. In doing so, it will allow our nation to degrade the enemy's ability to wage cyber war and also provide operational control over our critical infrastructures/systems.

The development of the National Cyberspace Security Response Team is a good start for the federal government in securing cyber space. It provides a single point of contact for the public (including private and public sectors) to share intrusion information and to gain knowledge in offensive and defensive strategies against attacks. However, this strategy still needs some improvement. First of all, it encourages private sectors to share intrusion information which contains system vulnerabilities, threats, etc. Companies today are reluctant to release such information due to the fear of bad publicity and releasing their system vulnerability information to the public (the fear of additional attacks by cyber criminals, etc). As a result, few companies are willing to share their intrusion information. Because of this, it would be very difficult for the Cyberspace Security Response Team to develop effective offensive and defensive strategies against cyber attacks and also issue warnings to the general public.

Overall, I find the development of the National Cyber Security Response Team an effective strategy in the realm of Information Warfare. It promotes security awareness among the general public and the importance of evaluating/analyzing attack information; thus it will assist our nation to resist cyber attacks. However, the lack of detailed information in regards to how the team handles a crisis situation/attack makes it difficult to assess the effectiveness of this strategy/priority.

### **Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program.**

The purpose of this priority is to reduce the overall cyber threats and vulnerabilities in America's cyberspace. By adopting this priority, the public (both private and public sectors) will be able to help defend our critical infrastructures/cyberspace against cyber attacks/war. This priority includes the following strategies:

1. Reduce Threats and Deter Malicious Actors: Identify vulnerabilities and potential threats on systems, hardware, and applications; thus preventing cyber attacks. This strategy also entails the empowerment of law enforcement (FBI, US Secret Service, etc) to track down and prosecute cyber criminals. In the realm of Information Warfare, the best cyber defense is to identify and mitigate any system vulnerabilities and threats. This will degrade the enemy's ability to wage war

on our critical systems. As for the ability to track down and prosecute cyber criminals (overseas or domestic), it would assist many nations to bring these cyber-criminals to justice; thus preventing future cyber attacks.

2. Impact assessment on potential cyber attacks: The understanding of the potential impact on cyber attacks. This assessment helps to identify what systems can be compromised and what systems are critical for survival. By performing such assessments, it will help institutions mitigate any potential cyber-related catastrophes and develop effective defensive and offensive strategies. By performing impact assessments, it will allow our nation and businesses to have operational control of our critical systems.
3. Identify and Remediate Existing Vulnerabilities: The implementation of security mechanisms and Internet Protocols will remediate existing vulnerabilities. In this particular strategy, it proposes the following improvements:
  - a. Transition from IPv4 to IPv6: IPv6 offers more addresses and more attrition and native IP security (IPSEC).<sup>4</sup>
  - b. Secure Domain Name System (DNS): Implement a DNS system that avoids flooding attacks.
  - c. Border Gateway Protocol (BGP): Develop secure BGP to avoid false routing information and denial service attacks.
  - d. Address Verification: Implement an address verification mechanism to avoid denial of service attacks.
  - e. Improve Management: DHS will assist organizations that operate the Internet to develop and implement security mechanisms and protocols to prevent cyber attacks.
4. Securing DCS/SCADA systems: Allocate research funds to help protect DCS and SCADA systems that operate our nation's critical infrastructures. (Power, Water, etc) This includes the development of more secure software and hardware for the DCS/SCADA systems to prevent cyber attacks. The implementation of secure hardware/software will provide the overall defense against potential cyber attacks. Thus, the attacker in the realm of Information Warfare will not achieve his/her objective: to deny, exploit, or destroy systems to achieve advantages over military, nations, or business adversaries.<sup>5</sup>
5. Reduce and Remediate Software Vulnerabilities: Remediate software development flaws to avoid any security vulnerabilities. These include patching system/software vulnerabilities and promote good software development practices through training.
6. Understand Infrastructure Interdependency and Improve Physical Security of Cyber Systems and Telecommunications: The federal government/DHS and private sectors will evaluate the interdependencies among critical infrastructures. This includes implementing redundant systems and additional security mechanisms (backup power, physical security mechanisms, etc) to avoid a single point of failure on other dependent systems. This is crucial in the realm of Information Warfare because the enemy will look for targets that will generate a cascading destructive effect among connected systems. Using the above practices will degrade the effectiveness of the enemy's ability to wage cyber war on America.
7. Develop Systems with fewer Vulnerabilities and Assess Emerging Technologies for Vulnerabilities: The federal government will allocate its resources/funds to assist private sectors to develop secure systems. The goal is to develop highly secure, trustworthy, and resilient computing systems that will withstand any cyber attacks.<sup>6</sup> The federal government will also

---

<sup>4</sup> Page 30 of The Nation Strategy to Secure Cyberspace

<sup>5</sup> Slide 7 of Dr. Tim Shimeall's Information Warfare Presentation. (Quote from Dr. Ivan Goldberg)

<sup>6</sup> Page 35 of The National Strategy to Secure Cyberspace.

promote good software development coding practices/methodologies to boost the overall software integrity, reliability, and security.

The evaluation of risks and vulnerabilities on our critical infrastructures will promote the security awareness throughout all sectors of the industry. This priority makes a viable countermeasure to mitigate future cyber attacks. By implementing the above security practices/methodologies, it will assist firms and governments to develop “vulnerability-free” systems that will ensure safety and control of our critical infrastructures. In addition to the above stated practices, the federal government is taking the initiative to ask private sectors to transition from using insecure protocols/mechanisms (IPv4, insecure DNS and BGP, etc) to secure protocols/mechanisms (IPv6, secure DNS and BGP). The implementation and the development of these security systems, mechanisms, and protocols will help us/public to deceive, frustrate, and resist cyber criminals.

Overall, I find priority II of The National Strategy to Secure Cyberspace to be a good start to secure our nation’s critical infrastructures. It provided both defensive and offensive strategies to mitigate cyber attacks. The following are the defensive and the offensive strategies I compiled that can be utilized using the above proposed practices:

#### Defensive Strategies:

- **Deception**: The development of new security mechanisms will lure attackers away from critical systems. This includes research and development of security protocols, mechanisms, and systems. Example: The development of more secure Firewalls, IDS, protocols, and redundancy systems will lure attackers away from the real target (i.e. SCADA/DCS systems.)
- **Frustration/Resistance**: The implementation of IPv6, secure DNS, BGP, and security mechanisms on critical systems will frustrate the attacker. The federal government has taken the initiative to seek for the implementation of IPv6 in both public and private sectors. By using secure protocols such as IPv6, it will provide IP transmission security (IPSec). Thus, it will provide frustration and resistance against any IP related attacks. In addition to the above stated practices, the government is asking all software and hardware manufactures to utilize good coding practices and engineering in order to provide operational control of our systems in the event of cyber attack/war.
- **Recognize and Respond to the attacker**: Law enforcement agencies such as FBI, NSA, and CIA will have the power to track down and prosecute cyber criminals.

#### Offensive Strategies:

- **Positioning & Visibility**: The evaluation of critical infrastructure interdependencies will allow the government and private sectors to determine the high points and low points of our nation’s infrastructure. Using this evaluation, it can help security experts to determine what systems are the key for survival and what systems can be compromised due to an attack. The evaluation will also assist experts to determine what systems should be visible or not visible from external networks. Using these two strategies (positioning and visibility) will ensure the survival of our critical infrastructure systems against cyber attacks.
- **Nourishment**: Using good coding practices and engineering, it will allow developers/engineers to develop robust protocols, mechanisms, and systems in order to resist any cyber attacks. In addition to resistance, it will offer life/survivability of the critical systems.
- **Risk Avoidance**: By implementing secure protocols and mechanisms stated above, these will help private and public sectors to avoid any cyber related catastrophes.

### **Priority III: A National Cyberspace Security Awareness and Training Program**

The purpose of the National Cyberspace Security Awareness and Training program is to promote security awareness to the American public. (This includes the general public, private and public sectors) This can be achieved by training and offering security certification programs to the general public. Since the September 11<sup>th</sup> terrorist attack, the federal government is taking serious measures to train security experts through corporate and international partnerships. Using this tactic, it will allow the government to “maintain an adequate pool of well trained and certified IT security specialists” to assist in securing our nation’s critical infrastructures and the ability to wage cyber war on nation states.<sup>7</sup> The following are the key audiences that the federal government proposed to increase awareness through education:

- **Home Users and Small Business:** Increase security awareness among home and small business users. Although these systems are not critical to our nation’s infrastructure, securing home users and small businesses’ systems will assist in securing America’s cyberspace.<sup>8</sup> The proposed strategy suggests that home users should install personal firewalls and virus scanners on to their systems. In addition, users should also update their operating systems, anti-virus, and firewalls to avoid threats and vulnerabilities.
- **Large Enterprises/Private Sectors:** Increase security awareness among employees with in an organization, especially top management. Educating top management is a key priority because they are the decision makers for allocating funds for purchasing and implementing security mechanisms (firewalls, IDS, Proxies, Honey Pots). Using these security mechanisms, it will prevent and resist cyber attacks that may affect other interconnected critical systems (i.e. critical infrastructure systems). The federal government also suggested strategies to detect and prevent insider threats/attacks. This include the implementation of access controls (ACL, physical security-bio metrics, etc), segregation of duties (no employee can have complete control of the entire system), and corporate security policies.
- **Institutions of Higher Education:** The federal government is asking institutions to collaborate with private sectors to develop new security mechanisms and protocols. It also wants higher educational institutions to make IT security as a priority in their curriculum. Using education, it will generate a pool of IT security specialists to assist in protecting America’s cyberspace.
- **State and Local Government:** Educating key government officials on the threats/dangers of cyber attacks/war. Using education, government officials will be willing to allocate state/local funds to adopt security mechanisms and policies in order protect its critical systems from cyber attacks.
- **Certification:** The federal government is partnering with private sectors to develop a “national recognized” security certification program to identify experts in the field of IT security.

Using education and training, it will promote the security awareness of our nation. Through awareness, the American people will be proactive in securing their systems; thus protecting our nation’s critical infrastructure. I am in favor of this practice because the government is recognizing training/educating of the American people is crucial to secure our cyberspace. By utilizing good security practices (i.e. install personal firewalls, antivirus scanners, etc) among the general public, system intrusions/exploits can be avoided. (i.e. prevent systems to become zombies agents that can launch attacks like DDoS, etc against our nation’s critical infrastructures.) Overall, I find the above practices are crucial to assist our nation to resist, to avoid, and to defend against any cyber attacks.

#### **Priority IV: Securing Government’s Cyberspace**

The purpose of Securing Government’s Cyberspace is to identify threats and vulnerabilities of the federal cyber systems. This includes documenting all government’s systems architecture, reporting structures, and security policies. Using this method, it will allow security experts to perform improvements to vulnerable

---

<sup>7</sup> Page 36 of The National Strategy to Secure Cyberspace.

<sup>8</sup> Page 37 of The National Strategy to Secure Cyberspace.

systems and maintain their understanding of government systems. In addition to these practices, the federal government is seeking improvements in the areas of user authentication and federal outsourcing. In regards to user authentication, the government will continue to improve its multi-layered authentication systems. This includes the appropriate use of bio-metric smartcards for accessing systems, strong passwords, ACL, and smart tokens to eliminate many significant security problems that exist today.<sup>9</sup> As for security concerns regarding federal outsourcing, the priority/strategy suggests that the government identify ways to improve security in agency contracts and evaluate the overall federal procurement process.<sup>10</sup> This includes the use of commercial software/products that may generate vulnerabilities/weaknesses in our existing government systems. As a result, the proposed strategy suggests that outsourcing government systems and operations may lead to serious security vulnerabilities to our government's systems.

By evaluating government's systems/cyberspace, it will allow the federal government to develop an effective offensive and defensive strategy. The following are the offensive strategies that can be incorporated in government systems:

#### Offensive Strategies:

- **Positioning and Visibility:** Identifying threats and vulnerabilities of the federal systems will allow security experts to position government systems in high or low points in the network. Through system and network identification, security experts can determine what systems are critical or non-critical to its operations. In addition to system positioning, system visibility will also be evaluated to determine what government systems should be visible or not visible to external networks.
- **Nourishment, Occupation, and Risk Avoidance:** The evaluation of government's cyberspace will allow security experts to provide "life/survivability" by incorporating security mechanisms such as biometrics, ACL, air-gapping, encryption, etc. By eliminating vulnerabilities on our government's systems/cyberspace, it will degrade the enemy's ability to wage cyber war.

The idea of evaluating our government's cyberspace is the key for survival to avoid future cyber attacks (i.e. "cyber-pearl harbor"). By implementing these strategies that I compiled, it will provide operational control of our government systems in case of cyber attacks/war.

#### **Priority V: National Security and International Cyberspace Security Cooperation**

The purpose of the National Security and International Cyberspace Security Cooperation is strengthening the coordination between nations on cyber security awareness. Since Cyberspace has no boundaries, cyber-criminals/terrorists can launch a cyber attack virtually anywhere. As of right now, there is no definitive international cooperation regarding sharing valuable information on cyber attacks and strategies. (Information such as strategies, technologies, attack information/analysis, etc) In addition, the federal government is strengthening the intelligence gathering on all government agencies. (FBI, DoD, DHS, etc) By improving cyber intelligence gathering, it will improve our "cyber attack attribution and prevention capabilities."<sup>11</sup> The following are the objectives for this priority:

1. **Strengthen Counterintelligence Efforts in Cyberspace/Improve Attack Attribution and Prevention Capabilities:** Improve cyber intelligence gathering among government agencies. Using intelligence gathering, our agencies can have a deeper understanding of our enemies/adversaries in the realm of Information Warfare and be able to defend our nation's cyberspace/critical infrastructure in a timely manner. (Gather intelligence on what technologies, attack strategies, etc may be utilized by an enemy)

---

<sup>9</sup> Page 46 of The National Strategy to Secure Cyberspace.

<sup>10</sup> Page 47 of The National Strategy to Secure Cyberspace

<sup>11</sup> Page 50 of The National Strategy to Secure Cyberspace

2. Promote North American Cyberspace: The United States will work with Canada and Mexico on identifying and securing North America's critical infrastructures. Through cooperation among these nations, it will safe guard all North America's cyberspace and its critical infrastructures.
3. International Involvement:
  - a. Promote international security awareness: This includes sharing information on security policies, standards, technologies, attack/incidence analysis, etc between nations. Sharing information among the international community will help our nation to obtain superior intelligence on the enemy's movements/strategies.
  - b. Develop international cooperation on prosecuting cyber-criminals: Currently, many nations including United States have limitations on prosecuting international cyber-criminals. The U.S. government is seeking other nations to adopt/follow the Council of Europe Convention on cyber-crime. By adopting international regulations, it will assist nations to prosecute cyber-criminals across international borders.
  - c. Develop international standards, protocols, etc to secure cyberspace: The federal government is seeking international cooperation in research and development on security protocols (IPv6, Secure DNS, BGP), effective corporate security policies, strategies to help nations defend against cyber attacks.
  - d. Develop International Watch and Warning Networks: Establish a point of contact in case of potential cyber attacks/threats among nations. For example: Implement security coordination centers like U.S. CERT in order for countries to share information, attack patterns, imminent threats, etc. Through international cooperation, this will greatly reduce the enemy's ability to wage cyber war/attacks.

Promoting international cooperation, research, and security awareness is an effective strategy to defend the global cyberspace. Through cooperation, nations can safeguard their critical infrastructures and their way of life against any possible cyber-terrorism/attacks. As for adopting global regulations, nations are able to track down and prosecute cyber-criminals/terrorists. Personally, I am in favor of adopting international prosecution regulations because in the past, many nations including United States have had difficulties in prosecuting cyber-criminals across international borders.

There are also flaws in regards to this strategy. First of all, promoting North America "Safe Cyber Zone" is nearly impossible. Since there are no boundaries in regards to Cyberspace, how can one continent be able to filter its inbound and outbound network traffic to prevent imminent cyber attacks? This could pose a serious problem for private and public sectors if their entire operations rely on IP transmission. For example: If CERT or other coordination centers issue a potential cyber-attack in North America, assuming that the "Safe Cyber Zone" is in place, will it block all traffic outside of North America? This can be considered a "self-inflicting" denial of service attack because some organizations may rely on Cyberspace to communicate with its business partners in other continents. (If implemented, this can pose serious economic losses in our nation) The second concern I have for the proposed strategy is will nations be willing to allocate their funds for research, development, and implementation of security mechanisms/protocols? Are countries willing to share security information and to adopt international cyber-crime regulations? International cooperation may be difficult to achieve in this scenario.

### **Thoughts and Conclusion**

The National Strategy to Secure Cyberspace is a good initial framework for protecting America's critical infrastructures and cyberspace. Its overall objective is to raise security awareness among the American people and also promote cooperation among the federal government and private sectors on the subject of

information security. As for Information Warfare, these strategies/priorities may be useful in the following:<sup>12</sup>

- Degrades the enemy's ability to wage cyber war: The implementation of security response team, threats and awareness programs/training, development of secure protocols/mechanisms, and international cooperation will greatly degrade the enemy's ability to wage war.
- Enhance the ability for America to wage cyber war: If the stated practices/strategies are in place (identify and resolve system/hardware vulnerabilities, implementation of secure protocols and mechanisms, etc), America can easily launch cyber attacks on nation states.
- Operational control: This can be achieved by using secure protocols, mechanisms, etc. By using these practices, we will have control of our critical infrastructures/systems in the event of a cyber attack.
- Superior intelligence gathering and situational awareness: In this proposal, the federal agencies such as CIA, FBI, and NSA will be gathering intelligence on potential threats and enemies. (including nations that may wage war against U.S., etc) As for situational awareness, the government is raising security awareness among the American public through education and training.

The concern that I have regarding the National Strategy to Secure Cyberspace is the lack of substance in defensive and offensive strategies. Most of the stated strategies in this paper are implied by my understanding of its priorities. I find some of the stated strategies are open for debate due to its lack of technical details and its implementation. As for "voluntary" involvement between the government, nations, and private sectors, there will be serious challenges to carry out this initiative. Not all organizations or countries are willing to allocate funds and manpower to protect their cyberspace and critical systems. In my opinion, the federal government must take a proactive stance by giving economic incentives to industries and local/state governments that utilize good security practices. Using this approach, it will assist our nation to secure its cyberspace.

---

<sup>12</sup> Slide 12 of Dr. Tim Shimeall's Information Warfare Presentation.

**References:**

The National Strategy to Secure Cyberspace, February 2003.  
[http://www.whitehouse.gov/pcipb/cyberspace\\_strategy.pdf](http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf)

Shimeall, Timothy. Strategy and Models of Information Warfare PowerPoint Presentation.