Strategy Research Project

CYBERSPACE: DEVOLUTION AND RECOVERY

BY

MR. RODNEY EMERY
Department of Veterans Affairs Civilian

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State 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.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
23-03-2011	Strategy Research Project	

4. TITLE AND SUBTITLE

Cyberspace: Devolution and Recovery

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Mr. Rodney Emery

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

Professor Cynthia Ayers
Center for Strategic Leadership

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: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The following Strategic Research Paper (SRP) is a review of The National Strategy to Secure Cyberspace for the U.S. Army War College Master of Strategic Studies Degree. The purpose of this paper is to provide an objective review of the strategy, supporting initiatives, and other relevant material that will give the reader an introduction to this important segment of our infrastructure. Is the United States prepared to deal with a cyber attack on critical infrastructure and, more importantly, if and when an attack should occur, is there a reasonable expectation of a timely recovery? These are questions that must be addressed. To be thorough, this paper will provide an introduction to the notion of cyberspace, a mock scenario for an attack on cyber infrastructure, an analysis of the strategy and supporting initiatives, and present a conclusion.

15. SUBJECT TERMS

Cyber, telecommunications, EMP

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	26	

USAWC STRATEGY RESEARCH PROJECT

CYBERSPACE: DEVOLUTION AND RECOVERY

by

Mr. Rodney Emery
Department of Veterans Affairs Civilian

Professor Cynthia Ayers
Project Adviser

This SRP 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

AUTHOR: Mr. Rodney Emery

TITLE: Cyberspace: Devolution And Recovery

FORMAT: Strategy Research Project

DATE: 23 March 2010 WORD COUNT: 5,017 PAGES: 26

KEY TERMS: Cyber, telecommunications, EMP

CLASSIFICATION: Unclassified

The following Strategic Research Paper (SRP) is a review of The National Strategy to Secure Cyberspace for the U.S. Army War College Master of Strategic Studies Degree. The purpose of this paper is to provide an objective review of the strategy, supporting initiatives, and other relevant material that will give the reader an introduction to this important segment of our infrastructure. Is the United States prepared to deal with a cyber attack on critical infrastructure and, more importantly, if and when an attack should occur, is there a reasonable expectation of a timely recovery? These are questions that must be addressed. To be thorough, this paper will provide an introduction to the notion of cyberspace, a mock scenario for an attack on cyber infrastructure, an analysis of the strategy and supporting initiatives, and present a conclusion.

CYBERSPACE: DEVOLUTION AND RECOVERY

"This is the verdict: Light has come into the world, but people loved darkness instead of light because their deeds were evil."

- John 3:19 NIV

This paper is an objective review of the United States efforts to protect the critical infrastructure known as cyberspace, specifically *The National Strategy to Secure Cyberspace.*[1] The latest version of this strategy is dated February 2003, though there is continuous work ongoing in this area within the Department of Homeland Security, as well as other federal, state, and local government agencies and public and private civilian organizations. Before the discussion addresses cyberspace specifically, it must be understood that this strategy, and others like it, is brought about by the process of identifying critical infrastructure and key resources that are essential for the continued maintenance and operation of American society, its economy, and in fact it's very way of life.

The need to identify critical infrastructure and key resources was codified in Executive Order 13010, signed July 15, 1996, which established the President's Commission on Critical Infrastructure Protection (PCCIP).[2] In October 1997 the commission delivered the report entitled *Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection*[3], which originally identified the following critical infrastructures: telecommunications, electrical power systems, gas and oil storage, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

On May 22, 1998, in response to the commission's report, President William Jefferson "Bill" Clinton, the 42nd U.S. president, signed Presidential Decision Directive 63 (PDD-63) which set a goal to establish a national capability to protect the nation's critical infrastructures within 5 years. One important part of this directive was the use of the word "cyber" in the definition used for critical infrastructures, as follows: "those physical and cyber-based systems essential to the minimum operations of the economy and government."[4]

With cyberspace now defined as a critical infrastructure, it was time to develop a strategy and a policy to protect this important piece of American society and the American economy. Much time has passed and many things have changed, however, since the signing of PDD-63. Relevant to this discussion are the horrific events that the United States has suffered in the last 10 years, beginning with the terrorist attacks that became known as "9/11" having occurred on September 11, 2001. Following 9/11, 2 major hurricanes struck the southeast in 2005, Hurricanes Katrina and Rita.[5,6] Adding to these tragedies, beginning in October 2007 the Dow Jones Industrial average, a U.S. stock index, fell approximately 42% culminating in a new low by October 2008. This signaled a severe economic down turn for the U.S. economy.[7] Finally, in 2010 the Deepwater Horizon, an offshore semi-submersible oil-drilling unit exploded, ultimately causing an oil spill of "national significance."[8] It is events like these that over the last 10 years have given rise, to put it lightly, to a heightened awareness in the area of national infrastructure protection, many of which led to the creation of the *National Infrastructure Protection Plan (NIPP)* in 2006 (subsequently updated in 2009).[9]

The list of critical infrastructures and key resource sectors has since expanded. Table 1 shows the latest list, along with the agency lead for the sector as defined in the overall *National Infrastructure Protection Plan*.[10]

Sector Specific Agency	**Critical Infrastructure and Key Resources Sector**
Department of Agriculture and Department of Health and Human Services	Agriculture and Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Healthcare and Public Health
Department of Interior	National Monuments and Icons
Department of Treasury	Banking and Finance
Environmental Protection Agency	Water
Department of Homeland Security	Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, Nuclear Reactors, Materials, and Waste
Office of Cybersecurity and Communications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration	Transportation Systems
Immigration and Customs Enforcement	Government Facilities

Table 1. Sector Responsible Agencies and Sectors

Adding complexity to the security of the 'cyberspace' infrastructure, as well as most of the other components, is the fact that they are not wholly owned or maintained by the U.S. Government or any other single entity. This means that it will take public and private partnerships working in concert with the federal, state, local, tribal, and territorial governments; regional coalitions; the private sector; international entities; and nongovernmental organizations to adequately protect and provide for the recovery of these infrastructures.[11] Of all issues relating to the security of cyberspace, and likely all other infrastructure segments, this one simple fact may be the most difficult of all to deal

with due to human nature's innate need to build cultures and subcultures in organizations that allow them to operate independently, and to their mind most efficiently and effectively.

Background

Since the beginning of time, man has remained in a constant period of growth (from an intellectual perspective) yearning to "work smarter and not harder," finding ways to do things more effectively and efficiently. The Bible supports this idea in Proverbs 18:15, which states, "The heart of the discerning acquires knowledge, for the ears of the wise seek it out."[12] It could be argued that this is an inherent trait of man. The times of the 20th century were no different, having ushered in periods of leaping strides in technological advances beginning with the second industrial revolution and continuing through to today—the dawning of the twenty-first century. Many of these strides were made in response to the need of the United States to protect and defend its population, honor, and interests, and/or the people, honor, and interests of U.S. allies.

Speaking of technological advances, consider the Electronic Numerical Integrator and Computer (ENIAC), "the world's first electronic digital computer developed by U.S. Army Ordnance to compute World War II ballistic firing tables,"[13] which was first employed back in the late 1940's. Since that time, computer technology has advanced exponentially throughout the following decades: operating systems and minicomputers in the 60's, supercomputers and microprocessors in the 70's, Personal Computers (PC) in the 80's, the internet in the 90's, and smart phones beginning in the first years of the 21st century (and this is not an exhaustive list).[14]

Prior to the advent of the PC, the use of computer technology had penetrated, in some fashion, nearly every private business and government agency, to include the Department of Defense, and following its introduction computer technology was then introduced to more than half of all private homes in the country. The growing dependence on the use of computers in the United States puts this technology and supporting technologies on the list of infrastructures considered critical to American society and the American economy. Adding complexity to the matter, the U.S. Defense Advanced Research Projects Agency (DARPA), an agency within the Department of Defense, commissioned a wide-area computer network in the 1970's which became known as the ARPANET.[15] This project led to the creation of the Internet, which eventually made it possible to interconnect the world's computers.

Homes in the U.S. used various methods to connect to the Internet including modulation/demodulation devices, known as MODEMs, using the Plain Old Telephone Service (POTS), cable television MODEMs, Digital Subscriber Line (DSL) MODEMs, and in some cases fiber optic technology just to name a few. Other's types of connections are now available that provide for higher bandwidth capabilities and are typically used by businesses, government agencies, and educational institutions as examples. The 2009 U.S. Census Bureau cites that over 60% of U.S. homes have a computer and that over 68% have Internet access in the home.[16] To build upon this, consider the latest data from the *Internet World* Stats website which states that the current number of Internet users in 2010 was just shy of two billion users, or 29% of the world population.[17]

To digress, albeit briefly (while continuing to build upon the idea that is the Internet and cyberspace), one of the latest fads on the Internet is related to social media; and it will be useful to understand its role in the world today. Social media according to Anthony Bradley of Gartner, a technology research firm, "is a set of technologies and channels targeted at forming and enabling a potentially massive community of participants to productively collaborate."[18] This topic is broached because of what is happening in the Middle East as this paper is written. Riots and protest in Tunisia beginning in December 2010, eventually led to the downfall of the Mubarak regime in Egypt in February 2011. This began a domino effect in about eleven other Middle Eastern countries.[19] The spurring of these protests and riots, possibly resulting in failed state status for some, has been attributed to the mass usage of social media to rally millions of supporters.[20]

All of these together with a whole host of other technologies, from simple physically wired infrastructures to advanced computing capabilities and satellites, create the critical information infrastructure that is now referred to as "cyberspace." Cyber components are so pervasive that they touch, if not manage, virtually all other critical infrastructure elements, making computerized, networked components so vital that cyber disruption could be catastrophic. For instance, these cyberspace (networked) systems are used to provide Supervisory Control and Data Acquisition (SCADA) access to the U.S. power grids, water treatment facilities, and rail lines, as well as facilitate finance, healthcare, and all practical communication capabilities on cyberspace. SCADA systems are widely used in the management and control of systems for distribution and transmission of electricity, waste and water management, oil and gas

pipeline management, rail and air transportation, and long-haul telecommunications maintenance and management.[21]

With regard to the protection of these infrastructure components, there have thus far been multiple programs, policies, directives, and actions taken in an attempt to secure portions of cyberspace at costs estimated to be in the billions of dollars across the federal, state, and local governments as well as in the public and private sectors. Two such federal government-led efforts aimed at improving the security posture of cyberspace(or components thereof), have been the Common Criteria Evaluation and Validation Scheme (CCEVS), which was originally known as Common Criteria and the National Information Assurance Partnership (NIAP) ,[22] precursors to the Federal Information Security Management Act (FISMA).[23] Briefly, the CCEVS developed criteria that vendors of information technologies could be tested against to ensure certain levels of information assurance. The National Institute of Science and Technology (NIST) and National Security Agency (NSA) have the following objectives in developing, operating, and maintaining an evaluation and validation scheme:

- to meet the needs of government and industry for cost-effective evaluation of IT products,
- to encourage the formation of commercial security testing laboratories and the development of a private sector security testing industry,
- to ensure that security evaluations of IT products are performed to consistent standards,
- to improve the availability of evaluated IT products.[24]

The NIAP developed as an outcropping of the NSA and NIST efforts and has attempted to form strategic partnerships in and amongst all stakeholders, while also getting buy-in from across all sections of society to ensure more secure information technology systems.

In summary, FISMA, in its original form, is the federal regulation that demands compliance from federal government departments and agencies on information security and assurance objectives, though its approach is more from a policy and oversight perspective. According to the law, FISMA is supposed to at least ensure effectiveness of information security controls over information resources that support federal operations and assets; provide effective management and oversight of information security risks, and coordinate like efforts with civilian, national security, and law enforcement communities; provide for development and maintenance of minimum controls required to protect federal information and information systems; and provide oversight of federal agency information security programs.[25] Today, FISMA does not provide or require the use of practical toolsets, methods, real-time monitoring, or secure configuration requirements. Thus far, the FISMA efforts do not reflect well on the U.S. government according to the annual FISMA scorecard, which currently shows an overall grade of "C" or less.[26] Given this score for the protection of federal information assets the question then becomes, "if we cannot adequately secure these cyberspace systems, can the country ever expect a timely and adequate recovery from a massive and concerted strike against these cyberspace systems that is sure to come?" In an attempt to answer this question, the following scenario will describe a possible series of attacks on critical infrastructure. An attempt will then be made to analyze the U.S. planning established to protect, respond, and recover the cyberspace infrastructure in the event of an attack.

Scenario

Imagine for a moment that the year is 2011, the month is September, and the day is Sunday the 11th, a mere 10 years since the horrific events that would come to be known as 9/11. The fateful day now known as 9/11 has been forever etched on the minds of every American as an ordinary day of the week--a Tuesday when not many people knew the term al-Qaeda nor did many know the goals and objectives of Islamic extremists. On the Tuesday morning of September 11, 2001, at approximately 8:46 AM until approximately 10:28 AM Eastern Time (ET) as the result of a carefully planned, coordinated, and executed terrorist attack by 19 al-Qaeda members, over 2,750 human lives ceased to exist when these 19 terrorists hijacked 4 loaded, civilian airplanes and used them as ballistic missiles crashing them into 3 iconic buildings and nose-diving one into a cornfield in Pennsylvania.[27] Now a mere 10 years later, as many are preparing to commemorate the events of 9/11, plans are again laid out for devastation. This time, however, it would not be a direct attack on human life--rather an indirect attack on nearly every form of infrastructure that supports human life--a carefully planned, coordinated, and executed attack on cyberspace and several other critical nodes.

The attack actually begins on the Friday evening prior to Sunday, September 11, 2011. An initial mass distribution of an email message with the title “The 9/11 Declaration” is noted—an email which is really a carefully disguised computer worm; although instead of carrying a payload that opens a backdoor into the infected computer system, the payload for this worm quickly and efficiently collects vital Privately Identifiable Information (PII), password files, and financial information and passes the

information quietly to a predetermined location. As the information is collected, it is parsed and stored for use by another program, which uses it to target financial institutions with directed attacks against associated accounts. As the attackers gain access, they begin draining bank accounts, and manage to continue their activities covertly for the next 24 hours. On Saturday evening, at about 8:00 PM a massively, well planned, coordinated, and executed Distributed Denial of Service (DDoS) attack begins which methodically cripples carrier networks, essentially rendering the Internet useless. Keeping in mind that this overall plan has been well thought out and planned for years prior, it is no surprise that the next set of attacks begin to target both analog systems of this infrastructure as well as other infrastructures. The attacks continue, using Information collected from war-dialing programs that methodically identified Supervisory Control and Data Acquisition (SCADA) systems using dial-up modulation/demodulation (MODEMS) devices for out-of-band maintenance of the following systems; telephone Private Branch Exchange (PBX) switching systems, power plant control, transmission, and distribution systems, sewage and water treatment control systems, oil and gas pipeline management systems, power generating and Uninterruptable Power Systems (UPS) at critical facilities such as banks, hospitals, and other critical operations. As these systems are accessed, administrative passwords are changed, viruses are implanted and executed, source code programs are modified, or systems are shut down completely, essentially rendering them all unusable. As if the preceding attacks were not enough, the morning of Sunday, September 11, 2011 brings with it the *coup de grace*--3 nuclear explosions at an altitude of 200 kilometers above the earth, each causing the generation of an Electromagnetic Pulse (EMP). The

strategic placement of these aerial explosions, one over the east coast, one over the mid-west, and one over the west coast, provide for maximum effect and geographic exposure, which could be devastating to unprotected electronics across the United States. As quoted from Halffast in the free online book entitled *Lights Out,* the following may be heard on the emergency alert systems immediately after the attacks—if the emergency alert system was still operational:

> My fellow Americans, as you know, 27 minutes ago the power went out. Also affected were most of the communication and transportation systems in the continental United States, most of Canada, and parts of Mexico. This seems to the effect of a large EMP burst. We are not sure at this time of the source of the burst and we do not know if it was accidental, an act of God, or a malicious attack. [28]

The remainder of a speech like this could detail information about available services that could help those in need, if the community was prepared. It might also relay pre-established governmental priorities for the recovery of services. Unfortunately, given the current state of preparedness, even a simple declaration of what may have happened would probably be more than current capabilities would allow after such an event.[29] Suffice it to say, as a result of such attacks, the U.S. could return to the pre-industrialized state, the economy would be in a state of collapse, and there would ultimately be a huge loss of life, with an expected loss of over 2/3rds of the population in the affected areas within the first 365 days.[30] The United States would be forever changed. That is, if the appropriate measures have not been taken in advance.

Analysis

With the introduction and background providing context, it is obvious how important the cyberspace infrastructure is to the American way of life and easy to see why the United States would need a nationally coordinated strategy to begin to outline

the measures and efforts that must be undertaken, as well as provide a baseline to understanding the resources that will be required to adequately protect this infrastructure. The scenario provided then opens the topic of vulnerabilities associated with operating and depending upon cyberspace, as well as other such infrastructures. It is also easy to see that this will not be a small effort. It will require many resources and much time. At the end of the day, resources and time equate to U.S. dollars; thus begging the question, "Can the United States afford it"? As is typical, the country will first need an overarching strategy and policy to point out the direction in this area.

The U.S. strategy and policy on this matter is contained within *The National Strategy to Secure Cyberspace* and its *National Policy and Guiding Principles*. This strategy and policy identify the way business is transacted, the way the government operates, and the way national defense is conducted as 3 functions that depend on an interdependent network of information infrastructures that define cyberspace. *The National Strategy to Secure Cyberspace* states: "It is the policy of the United States to prevent or minimize disruptions to critical information infrastructures and thereby protect the people, the economy, the essential human and government services, and the national security of the United States."[31] It goes on to identify the following guiding principles: it must be a national effort, must protect privacy and civil liberties, consider regulation and market forces, maintain accountability and responsibility, ensure flexibility, and provide for multi-year planning.[32] The recognition that a national effort is needed takes into account a previous point that the systems that make up cyberspace are widely distributed and require the efforts of many segments of society. With regard to the protection of privacy and civil liberties, abuses of cyberspace infringe upon

American rights and the strategy must aid in avoiding any such infringements. The reference to regulation and market forces again points out that this cannot be done by the federal government alone; yet the Department of Homeland Security is appointed as the accountable and responsible office for many initiatives in this realm. The changing environment of cyberspace is recognized along with the importance of remaining flexible. Finally, there must be provision for a multi-year planning effort, as technology advances and new threats come to the forefront.

The objectives for the National Strategy to Secure Cyberspace follow: prevent cyber attacks against our critical infrastructures, reduce our national vulnerabilities to cyber attack, and minimize the damage and recovery time from cyber attacks that do occur.[33] The overarching strategic plan goes on to layout 5 priorities that are aimed at making these objectives obtainable; a national cyberspace security response system, a national cyberspace security threat and vulnerability reduction program, a national cyberspace security awareness and training program, securing governments' cyberspace, and national security and cyberspace security cooperation.[34]

These priorities are largely addressed by the establishment of the Department of Homeland Security (DHS) National Cyber Security Division. The DHS National Cyber Security Division is a coordination and collaboration entity that partners with public, private, and international groups to build a capable cyberspace response system and risk management program.[35] This is accomplished through its 3 organizations; National Cyberspace Response System, Federal Network Security (FNS), and Cyber-Risk Management Programs. The National Cyberspace Response System is largely made up of the U.S. Computer Emergency Response Team (US-CERT).

The mission of the US-CERT is multifaceted, though for the purposes established here, there are 2 specific US-CERT efforts that are important: the Government Collaboration Groups and Efforts and the Analytical Tools and Programs. The Government Collaboration Groups and Efforts coordinate the following: Government Forum of Incident Response and Security Teams (GFIRST), Multi-State Information Sharing Analysis Center (MS-ISAC), National Cyber Response Coordination Group (NCRCG), and the Software Assurance (SwA) group.[36]

The GFIRST is made up of practitioners, both technical and tactical, whose principle purpose is to aid in the security of government systems. The GFIRST folks work as a team to deal with information security threats and incidents while also sharing knowledge and best practices. All of these efforts fully support the "new C^2" which is cooperation and collaboration among the government agencies represented and civilian organizations as well. The MS-ISAC is focused on threat prevention, threat protection, as well as response and recovery and works with state and local governments to facilitate this capability.

The NCRCG is likely one of the primary (if not the primary) offices that would address issues related to the scenario laid out earlier in this paper. The NCRCG is a partnership between the US-CERT, DoD, and the Department of Justice (DoJ). The NCRCG "serves as the federal government's principal interagency mechanism for coordinating efforts to respond to and recover from cyber incidents of national significance."[37]

The SwA team helps to ensure the software is vulnerability free and operates as advertised. The Analytical Tools and Programs efforts are as follows: "Federal Security

Mailing List, Federal Vulnerability Knowledgebase (VKB), US-CERT Portal, US-CERT Einstein Program, Internet Health and Status Service, Security Configuration Benchmarks and Scoring Tools, and Build Security In."[38] The Federal Security Mailing List is an e-mail application that allows one to self-subscribe in order to receive US-CERT notices or other information related to information security. The VKB is a database of information regarding information security vulnerabilities that allows federal civilian employees to self-subscribe and login to obtain relevant information.

The US-CERT portal is a website dedicated to sharing relevant information with participants. The Einstein Program is a program that allows for the aggregation, comparison, evaluation, and distribution of information regarding information security issues across the federal government. The Internet Health and Status Service collects and can distribute Internet related statistics. The Security Configuration Benchmarks and Scoring Tools are a host of guides and tools that are assembled and provided by experts in the information security and information assurance arenas through the Center for Internet Security website. The Build Security In is a website that makes pertinent information available to software and hardware developers and engineers to ensure that information security is "baked in" as opposed to added on.

The Federal Network Security (FNS) organization maintains 4 programs: Security Management (SM), Requirements and Acquisition Support (RAS), Network and Infrastructure Security (N&IS), and the Compliance & Assurance Program (CAP). The Security Management function provides for the aggregation and evaluation of information related to risk management for civilian government agencies and departments. The Requirements and Acquisition Support program maintains efforts for

the Information Security Systems Line of Business (ISSLOB), which is aimed at eliminating duplication of effort across federal government organizations this one specifically related to information security. The Network and Infrastructure Security (N&IS) maintains the Comprehensive National Cybersecurity Initiative (CNCI), specifically the Trusted Internet Connections (TIC) Initiative which is aimed at reducing external Internet connections to all government agencies and departments. The Compliance and Assurance Program (CAP), as the name implies, is an assessment capability that measures and monitors risk and provides appropriate policy. Finally within the National Cyber Security Division is the Cyber-Risk Management Program, which provides for exercises and awareness programs, related to information security and assurance.

It is all of these programs that together make up the U.S. capability to measure risk associated with operating information technology systems across the federal government and to coordinate and collaborate with the state and local governments, the public, private and international organizations and ultimately to respond to an event or events as described in the scenario above. It should be mentioned at this point that this capability discussed thus far has only addressed the civilian side of the U.S. federal government's capability and has not addressed similar, and in some cases more advanced, U.S. Department of Defense capabilities which opens many other avenues for discussion regarding the responsibilities of operating cyberspace (touching on issues of privacy, aggression, and defense to name a few). Considering the DHS capability explained here, if the FISMA information security efforts across the federal government thus far have produced an average grade of a "C", will the efforts described in this

section of this paper be able to adequately provide for the protection against or recovery from an event such as suggested in the scenario above?

At first glance and considering the estimated cost of the DHS National Cyber Security Division described above, which cursory research places to be just shy of one billion U.S. dollars per year, one may think that the DHS could adequately respond to, minimize damage, and recover from the scenario described above. Unfortunately, according to *Government Informationweek,* an online magazine, in its review of the Government Accountability Office (GAO) report entitled *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened*, "DHS is struggling with how to share its recommendations on resiliency with network owners and operators because of the voluntary nature of the work, according to the report."[39] A separate online magazine article by *HSToday.US* states "The White House cybersecurity coordinator and the Department of Homeland Security (DHS) should do more to share information on cybersecurity threats, congressional investigators warned Monday" [40] citing yet another GAO report. Both of these assessments appear to point directly at the issue that makes this problem so difficult to deal with--sharing and coordination with not only other federal government organizations, which can be difficult enough on their own, but also with State, local, tribal, and territorial governments; regional coalitions; the private sector; international entities; and nongovernmental organizations.

The good news, if there is any, to come out of a scenario as described above, is that the *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures* states "that EMP

presents a less significant direct threat to telecommunications."[41] Unfortunately, in the same sentence, the commission goes on to say the vulnerable electrical grid may add another complexity dependent upon the time involved in recovery--though this is outside of the scope of this analysis,[42]--which seems to say that while cyber technology may survive the EMP blast it would require stand-alone power generating equipment to operate it.

Conclusion

This strategic research paper has provided the reader with an introduction into the *U.S. National Strategy to Secure Cyberspace* as well as components of and information related to the *National Infrastructure Protection Plan*. This information was followed by background information related to the components and makeup of cyberspace and some of the early U.S. efforts aimed at dealing with the notion of security of the systems that make up cyberspace--remember NIAP and FISMA, as if the U.S. government lacks acronyms. The background was followed by a fictional scenario presenting a mock attack on critical infrastructure. The focus then turned to the latest U.S. efforts since 2003, specifically DHS, which have been designed to mitigate the risks associated with operating this infrastructure and providing a response and recovery capability. Finally, a subjective review of this capability weighed against the proposed scenario was provided concluding that there is plenty of opportunity to do a better job in order to mitigate risk and adequately prepare response to an incident such as the scenario proposed in this paper.

In a world that is vulnerable, uncertain, complex, and ambiguous, this problem--that of securing the cyberspace infrastructure and preparing the country to adequately

recover from the inevitable attack that is likely to come--continues to allude the United States, her coalition partners, and many others, and therefore qualifies as a "wicked problem" that may only be resolved in a way similar to that of the "Gordian Knot"--that is with a bold stroke. The final question that may remain then is, can the U.S. afford the costs associated with the ultimate solution or can the U.S. afford to not seek the ultimate solution? The rule of "opportunity cost" would suggest that in dealing with such a problem as described here will require that something else is foregone. Remember after all, without aiming it at an individual, group, organization, or agency, "it's the economy stupid."[43]

Endnotes

[1] *The National Strategy to Secure Cyberspace*, February 2003.

[2] *Executive Order 13010 Critical Infrastructure Protection*, July 15, 1996, http://www.fas.org/irp/offdocs/eo13010.htm. (accessed on January 15, 2011).

[3] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection*, http://www.fas.org/sgp/library/pccip.pdf (accessed on February 3, 2011).

[4] John Moteff and Paul Parfomak, *Critical Infrastructure and Key Assets: Definition and Identification*, http://www.fas.org/sgp/crs/RL32631.pdf, (accessed on November 13, 2010).

[5] National Oceanic and Atmospheric Administration, http://www.ncdc.noaa.gov/special-reports/katrina.html, (accessed on February 3, 2011).

[6] National Oceanic and Atmospheric Administration, http://www.ncdc.noaa.gov/special-reports/rita.html, (accessed on February 3, 2011).

[7] Wagonner, John. November 2008. *Is today's economic crisis another Great Depression?.* USA Today. http://www.usatoday.com/money/economy/2008-11-03-economy-depression-recession_N.htm. (accessed on February 3, 2011).

[8] British Petroleum (BP). 2010. *Deepwater Horizon Accident Investigation Report, Executive Summary*. http://www.bp.com/liveassets/bp_internet/globalbp/globalbp_uk_english/incident_response/STAGING/local_assets/downloads_pdfs/Deepwater_Horizon_Accident_Investigation_Report_Executive_summary.pdf (accessed on February 3, 2011).

[9] Department of Homeland Security. 2009. *National Infrastructure Protection Plan, Partnering to enhance protection and resiliency*, Department of Homeland Security.

[10] Ibid.,

[11] Ibid., p. 2.

[12] Proverbs 18:15 (New International Version, 2010).

[13] Martin Weik, *The ENIAC Story*, Ordnance Ballistic Research Laboratories, Aberdeen Proving Ground, MD, 1961, http://ftp.arl.mil/~mike/comphist/eniac-story.html (accessed on November 15, 2010).

[14] Extrapolated from www.computerhistory.org (accessed on February 3, 2011).

[15] Robert E. Kahn and Vinton G. Cerf, *The Internet: What Is The Internet (And What Makes It Work)*, *http://dr-net-cyber.blogspot.com/2007/03/internet.html* (accessed on November 15, 2010).

[16] U.S. Census Bureau. 2009. http://www.census.gov/population/www/socdemo/computer/2009.html (accessed on February 3, 2011).

[17] Miniwatts Marketing Group, Internet Usage Statistics: The Internet Big Picture, World Internet Users and Population Stats, http://www.internetworldstats.com/stats.htm (accessed on February 21, 2011).

[18] Anthony J. Bradley, Gartner, *A New Definition of Social Media*, http://blogs.gartner.com/anthony_bradley/2010/01/07/a-new-definition-of-social-media/ (accessed on February 21, 2011).

[19] North Africa and Middle East Protests Timeline – UPDATED, http://www.recreatingtampa.com/2011/01/28/north-africa-middle-east-protests-timeline/ (accessed on February 21, 2011).

[20] Hilary Bassett, Iowa State Daily.COM, *Social media used to motivate protests in the Middle East*. http://www.iowastatedaily.com/news/article_d7b5fd58-401d-11e0-ba52-001cc4c03286.html (accessed on February 21, 2011).

[21] *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Critical National Infrastructures,* April 2008, p. 2.

[22] Extrapolated from data available on http://www.niap-ccevs.org/ (accessed on February 3, 2011).

[23] Federal Information Security Management Act, 2002, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf (accessed on February 3, 2011).

[24] Common Criteria Evaluation and Validation Scheme, http://www.niap-ccevs.org/ccevs/objectives/ (accessed on February 3, 2011).

[25] Federal Information Security Management Act (FISMA), 2002, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf (accessed on February 3, 2011).

[26] Prepared by Ranking Member Tom Davis, House Oversight and Government Reform Committee, based on reports required by the Federal Information Security Management Act of 2002. http://www.coact.com/FISMA/FISMA_FY2007_ReportCard.pdf (accessed on February 3, 2011).

[27] Extrapolated from *The 9/11 Commission Report*, 2002, http://www.9-11commission.gov/report/911Report.pdf (accessed on February 3 , 2011).

[28] *Lights Out, Halffast,* January 2003*,* http://www.frugalsquirrels.com/fiction/ (accessed on January 15, 2011).

[29] *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Critical National Infrastructures,* April 2008.

[30] Ibid.

[31] *The National Strategy to Secure Cyberspace*, February 2003, p. 13.

[32] Ibid., 14-15.

[33] Ibid., viii.

[34] Ibid., x.

[35] Department of Homeland Security, National Cyber Security Division, http://www.dhs.gov/xabout/structure/editorial_0839.shtm , (accessed on February 3, 2011).

[36] Department of Homeland Security, U.S. Computer Emergency Response Team, http://www.us-cert.gov/federal/, (accessed on February 3, 2011).

[37] Department of Homeland Security, U.S. Computer Emergency Response Team, National Cyber Response Coordination Group, http://www.us-cert.gov/federal/collaboration.html (accessed on February 3, 2011).

[38] Department of Homeland Security, U.S. Computer Emergency Response Team, http://www.us-cert.gov/federal/, (accessed on February 3, 2011).

[39] Elizabeth Montalbano, October 2010, InformationWeek, *DHS Urged To Bolster Cyber Infrastructure Security*, http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=228000168 (accessed on February 3, 2011).

[40] Mickey McCarter, August 2010, HSToday.US, *Weak Info Sharing Risks Cyber Attacks, GAO Says:Public and private sector must do more to communicate threat info,* http://www.hstoday.us/briefings/today-s-news-analysis/single-article/weak-info-sharing-risks-cyber-attacks-gao-says/77c62232a0f7c18db1fb149e91d488c2.html (accessed on February 3, 2011).

[41] *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Critical National Infrastructures,* April 2008, p. 69.

[42] Ibid., 69.

[43] Bill Schneider, CNN, *Analysis: Could it be 'the economy, stupid' again?,* http://articles.cnn.com/2007-11-07/politics/schneider.economy.poll_1_top-five-issues-elections-job-growth?_s=PM:POLITICS (accessed on February 21, 2011).