Cyber Exercises Today and Tomorrow

Charles Winstead, NSCI
Jim Ed Crouch, NSCI
November 19, 2010

National Security Cyberspace Institute, Inc. (NSCI)

Through the combination of research and education, NSCI supports public and private clients aiming to increase cyberspace awareness, interest, knowledge, and/or capabilities. NSCI is committed to helping increase security in cyberspace whenever and wherever possible. NSCI publishes a bi-weekly newsletter (*CyberPro*), has published numerous whitepapers on various cyberspace topics, maintains an online cyber reference library, and has established an email distribution list for sharing cyber-related resumes to interested parties. NSCI is a small, veteran-owned business headquartered in Virginia.

Introduction

Did you hear about the British scientist who infected himself with a computer virus earlier this year? It seems that Dr. Mark Gasson, a cybernetics researcher in the UK, had a radio frequency Identification (RFID) chip implanted in his wrist which allowed him to accomplish certain tasks--opening keycard locked doors and operating his cell phone. Of course, we have had that technology around for years for installing pace makers and cochlear implants. But as far as we could determine, no one has ever infected an RFID implant with a virus. The doctor was interested in testing the security of the system and passing along the results to others in the field so they could use what he had learned and adjust their activities if necessary.[1]

We know that learning from experiments and then exercising what you've learned is a great way to improve performance in a variety of circumstances. As an example, we found in the Vietnam War around 1972 that our exchange ratio (enemy losses vs. US losses) between USAF and enemy fighters was approximately one to one. Compared to our Korean Was performance (10:1), this ratio was devastating, so the Air Force did some studies and concluded that most of our losses occurred within the first ten encounters with the enemy. If a pilot could get beyond the first ten combat missions, the exchange ratio changed greatly in our favor. Hence, the Air Force created the two-week-long Red Flag Exercises. The idea was to give the young pilots their first ten combat engagements before they ever met the enemy. Red Flag Exercises today teach young pilots how to adapt quickly to combat and the consequences if they don't.[2] Today, we share what we have learned with young pilots from around the world at Red Flag, and most in the business would agree that they are among the best fighter pilots in the world.

This led us to wonder about cyber security exercises. Everyone knows what an enormous problem cyber security is worldwide, and how it touches virtually all facets of our society, from commerce and banking interests to our Governments and our education systems and others. Just who is conducting cyber security exercises today, what are they learning, and how are the lessons learned from these exercises being disseminated and to whom? Who is benefiting from all of the investments in cyber security exercises?

This paper will examine cyber security exercises from four communities: Academia, Industry, the Department of Defense, and other Government Agencies. We will conclude with some suggestions on how we can proceed more effectively and efficiently in the future.

Academia

Today many colleges and universities are on the cutting edge of cyber experimentation and provide their students with safe environments in which to test and perform repeatable exercises and experiments. Take the University of Utah, for example, and their public domain environment, Emulab, a network emulation testbed. Emulab is both a facility and a network software system, and it is used by many schools and universities today to evaluate, debug,

[1] http://www.digitaltrends.com/computing/man-infects-himself-with computer-virus/trackback/

[2] http://www.airforce-magazine.com/MagazineArchive/Pages/2000/November%202000/1100flag.aspx

Charles Winstead, NSCI
Jim Ed Crouch, NSCI
November 19, 2010

and appraise their network systems. Emulab is a public facility and is free of charge to most users.[3] Another example is the *cyber-**DE**fense **T**echnology **E**xperimental **R**esearch **lab**oratory Testbed* (DETERLab), operated through the University of Southern California and funded by the Department of Homeland Security. DETERLab is used as a testbed for future cyber security research and teaching, and it has over 300 nodes, or network processing locations, between the USC campus and UC Berkeley. This allows students to conduct, in a safe environment, reproducible experiments on system and network attacks and countermeasures.[4] The National Science Foundation funds GENI (Global Environment for Network Innovations), which provides a collaborative and exploratory environment for academia and the public for experimentation and innovation. "The GENI mission is to open the way for transformative research at the frontiers of network science and engineering, and inspire and accelerate the potential for groundbreaking innovations of significant socio-economic impact."[5] The University of Illinois at Urbana provides students with a Virtual Power System Testbed, while Dartmouth operates DIST, Dartmouth Internet Security Testbed.

This is not meant to be a comprehensive list of collegiate cyber testbeds and experimentation environments by any means, but it does provide one with the sense that academia is well aware of the necessity to experiment with cyber security, and has invested well in providing environments for their students to learn about the latest concepts in cyber security.

We find that the Government has contributed significantly to these capabilities. For instance, the National Security Agency has been sponsoring competitions in Network Defense called Cyber Defense Exercise (CDX) since 2001 at our service academies--this year's winner was the US Naval Academy, by the way, who edged out teams from the US Military Academy (West Point), the Air Force Academy, the Coast Guard Academy, the Merchant Marine Academy, the Naval Postgraduate School, and the Air Force Institute of Technology.[6] The focus of this exercise is to see who displays the best cyber defense skills. The idea behind CDX is to "build and defend computer networks against simulated intrusions by the National Security Agency/Central Security Services Red Team."[7] This is not the first exercise--this year's was CDX 10.[8] And, Industry is also involved in these collegiate level exercises. The Computer Science Corporation this year served as mentors for the 5th Mid-Atlantic Collegiate Cyber Defense Competition. This year's winner was Northeastern University. While the US Department of Homeland Security provides most of the financial backing; The Boeing Company, Deloitte, SAIC, Microsoft, and other industry leaders also provided funding.[9]

But not all Cyber Security exercises are executed at the collegiate level. Indeed, the Air Force Association (AFA), in partnership with Northrop Grumman and SAIC, sponsors an annual exercise called the CyberPatriot Competition. Beginning in 2009, the AFA sponsored teams of teenagers from Air Force Junior Reserve Officer Training Corps and the Civil Air Patrol units from eight high schools. The intent is to foster interest in Scientific, Technology, Engineering, and Math fields using a game-like format. CyberPatriot II built on the initial successes and brought together more than 200 teams from 44 states and Japan. The winning team's coach commented, "This was a great learning opportunity, and just a lot of fun for the teams. They are definitely more interested in the cyber security career field as a result." [10] The CyberPatriot exercise has been so successful that it has expanded this year to tens of thousands of high school students, regardless of whether they are affiliated with the military or not. AFA

[3] http://www.emulab.net/

[4] http://www.isi.edu/deter/

[5] http://www.geni.net/?page_id=2

[6] http://www.navy.mil/search/display.asp?story_id=52902

[7] Ibid

[8] http://news.cnet.com/8301-13772_3-20003203-52.html

[9] http://www.nationalccdc.org/

[10] http://www.airforce-magazine.com/MagazineArchive/Pages/2010/July%202010/0710cyberpatriot.aspx

Chairman of the Board Joseph Sutter states, "The Air Force certainly needs more cyber defenders, and it's important to the nation as a whole. CyberPatriot excites, it motivates, and it teaches."[11]

The point to be made here is that the academic community recognizes the importance of cyber security, exercises and experimentation, and is providing students many meaningful and significant opportunities to learn and practice cyber defense. Moreover, this community is getting considerable support, financial and otherwise, from both the US Government and commercial communities recognizing the value of cyber security.

Industry

Secretary of the Department of Homeland Security, Janet Napolitano, said earlier this year, "All Americans have an important role to play in securing our computer systems and cyber networks. We are challenging our nation's best and brightest to utilize their expertise and creativity to devise new ways to engage the public in the shared responsibility of safeguarding our cyber resources and information."[12] And commercial and industrial entities are on the front line of this war. Indeed, AT&T's Chief Security Officer Edward Amoroso told a Congressional Committee this year that "Evolving and more lethal types of cyber-attacks can devastate infrastructure. It has become so easy and rampant that the risk has grown exponentially." He added, "The result is a laser-like cyber-attack on an unsuspecting business or government system. Last year, the FBI announced that revenues from cyber-crime exceeded drug trafficking as the most lucrative illegal global business, estimated at reaping more than $1 trillion annually in illicit profits."[13] Putting its money where its mouth is, AT&T invested almost $18 billion this year to expand the capabilities of their network.

The partnership between the government and industry is absolutely essential, and the Government understands this fact of life. Founded in 1999, The Financial Services Information Sharing and Analysis Center (FS-ISAC) is a group formed in response to the Presidential Security Directive of 1998. This directive mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure. This year FS-ISAC hosted an exercise called Cyber Attack against Payment Processes (CAPP) for financial institutions, retailers, credit card processors, and other business ventures of all sizes. As Bill Nelson, FS-ISAC's President, explained about the exercise, "When cyber security threats occur, swift and well-planned reactions can mean the difference between business continuity and catastrophe. This is especially true with cyber attacks against payment processes. FS-ISAC is eager to provide payment systems participants with this unique opportunity to test their readiness to respond to major cyber attack incidents."[14] CAPP was a three day exercise and provided a different type of cyber attack each day. This exercise was open to all businesses of any size whether or not they were members of FS-ISAC and was free of charge. In addition, all participants and their company's information were kept anonymous and confidential. Participants were provided peer data to compare their results in an interactive after action report, which was not shared with the public at large.[15]

As Deputy Defense Secretary William Lynn pointed out recently, "Existing technologies can thwart a majority of cyber attacks, but defenses are expensive and burdensome. Although many industries have made a major investment in defensive capabilities, not everyone is able to make that kind of investment on their own." [16] We've highlighted some of the larger investments in the following paragraphs.

---

[11] Ibid

[12] http://www.enterprise-security-today.com/story.xhtml?story_id=72011

[13] http://www.outlookseries.com/N/Security/3230_AT&T_Chief_Security_Officer_Edward_Amoroso_Offers_Senate_Cyber-Security_Recommendations.htm

[14] http://www.informationweek.com/story/showArticle.jhtml?articleID=222200554

[15] Ibid

[16] http://www.govinfosecurity.com/articles.php?art_id=2201

Charles Winstead, NSCI
Jim Ed Crouch, NSCI
November 19, 2010

The Harris Corporation announced earlier this year their intention to build a Cyber Integration Center. The Harris Cyber Interrogation Center will be housed in a 14,000 square-foot facility located somewhere in the mid-Atlantic region. Expected to be opened in late 2010, the Center will offer a trusted technology infrastructure and will include a testbed and accredited environment. Retired Air Force Major General Dale Meyerrose, now Vice President and General Manager of Harris Cyber Integrated Solutions, reported in a press release that, "This first-of-its-kind center leverages Harris's extensive cyber capabilities to solve our customers' evolving cyber challenges while at the same time adding value through tailored applications and services."[17]

Science Applications International Corporation (SAIC) announced this year that they would open their Cyber Innovation Center (CIC) in Columbia, MD. "The CIC offers an environment where the comprehensive knowledge of SAIC's workforce is brought to bear upon the challenge at hand," said Larry Cox, Senior Vice President and business unit General Manager. The facility will feature a technical solutions laboratory and a secured infrastructure to assist in the testing and development of innovative cyber solutions. The CIC will be dedicated to fusing ideas, services and technologies for their company and their customers.[18]

Another major DoD contractor, Raytheon, is deploying the Raytheon Cyber Tactics Center (RCTC) this year. "The RCTC will provide a secure facility for hardware and software testing as well as a learning facility for Raytheon engineers, customers, and industrial and academic partners," reports Randall Fort, Director of Programs Security. The RCTC will provide an engineering environment to allow the evaluation of embedded cyber security and protection in cyberspace, Command, Control, Communications, and Intelligence (C3I), sensing, effects, and homeland security realms.[19]

In November, 2009, Lockheed Martin announced the grand opening of its NexGen Cyber Innovation and Technology Center, located in Gaithersburg MD, as a research and development center for customer and partner collaboration. NexGen will be housed in a 25,000 square foot facility and is outfitted with a global cyber innovation range used to solve technology problems in real time while simulating customer environments. "Our NexGen cyber center will foster innovation and collaboration to preserve our customers' missions and address the worldwide cyber security challenges," stated Linda Gooden, Executive Vice President, Lockheed Martin Information Systems and Global Services.[20] Together with participants from the NSA, DHS, National Institute for Standards and Technology, National Science Foundation, the University of Maryland, Johns Hopkins and others, Lockheed Martin and co-host Technology Council of Maryland have already hosted a Cyber Security Awareness Day at the NexGen facility for Science, Technology, Engineering, and Math high school students. Lt Gen (Ret) Charlie Croom, Lockheed Martin's Vice President of Cyber Solutions said, "This event will not only help students learn about what it takes to stay safe online, it will also help them chart their course for higher education and a career in the fast-growing field of cyber security."[21]

Finally, Northrop Grumman has also made significant corporate investments in their Cyber-space Solutions Center, which is used for both independent R&D on cyber projects and for conducting contract work for their customers. The Center has an internet research lab as well, which has been called "internet in a bottle." Northrop uses this lab for experimentation in a controlled, limited environment. Complementing the Cyber-space Solutions Center is their CSOC, or Cyber Security Operations Center, which is their threat detection and response center for protecting corporate assets and their customers as well. They rely on the CSOC to monitor their networks and assist in

[17] http://www.harris.com/view_pressrelease.asp?act=lookup&pr_id=2991

[18] http://investors.saic.com/phoenix.zhtml?c=193857&p=irol-newsArticle&ID=1474885

[19] http://www.raytheon.com/technology_today/2010_i1/meet_new_leader.html

[20] http://www.lockheedmartin.com/news/press_releases/2009/11.12.09ISGSOpensNexGenCyberCenter.html

[21] http://www.prnewswire.com/news-releases/lockheed-martin-hosts-students-for-cyber-security-awareness-day-with-tech-council-of-maryland-104851289.html

Charles Winstead, NSCI
Jim Ed Crouch, NSCI
November 19, 2010

mitigating advanced cyber threats.[22] Furthermore, Northrop Grumman has been called on by other nations to build cyber ranges in other countries. Earlier this year, Northrop announced the opening of the first commercially-available cyber test range in Fareham, United Kingdom. The Fareham facility was designed to be connected with other facilities worldwide to conduct large-scale experiments which are not possible from a single facility. "Cyber security is a fundamental necessity for protecting our critical national infrastructure and our new federated cyber range will be a major UK resource for building, testing, and validating technologies as rapidly and efficiently as possible," according to Sir Nigel Essenhigh, Chairman of Northrop Grumman UK.[23]

Department of Defense

With over 7 million users on more than 15,000 networks deployed in 88 countries, the DoD has significant interest in cyber security. Deputy Defense Secretary William J. Lynn recently reported that "All major weapons systems, the intelligence and logistics efforts and personnel programs rely on information technology.[24] Lynn went on to say that over "100 foreign intelligence services are trying to hack into U.S. Systems, and foreign militaries are developing offensive cyber capabilities."[25] And, the DoD has incisively invested in experiments and exercises to make sure that they stay on the cutting edge of cyber security.

The first DoD-led exercise was a certain clarion call for action in securing our networks. In 1997, the Joint Staff at the Pentagon conducted its first classified exercise on the vulnerabilities of their information infrastructure. "Eligible Receiver" was a Classified Secret, no-notice exercise sponsored by the Joint Chiefs of Staff and included participation from the National Security Agency, Defense Information Systems Agency (DISA), National Security Council (NSC), DIA, CIA, FBI, and the Departments of State, Justice, and Transportation.[26] The Red Team (attackers) was from the NSA, and they used only standard internet techniques and software they had obtained easily from hacker sites on the internet. This two-week long exercise uncovered some glaring deficiencies within the DoD's infrastructure. Essentially, the Red team could have shut down the entire power grid of the United States and crippled the Command and Control capability in the Pacific Theater and at the National Military Command Center in the Pentagon. As Pentagon spokesman Ken Bacon said at the time, "Eligible Receiver was an important and revealing exercise that taught us that we must be better organized to deal with potential attacks against our computer systems and information infrastructure."[27] And the DoD has continued to invest in exercises to help them continue to discover, learn, and practice.

The National Defense University (NDU) this year held its second Cyber security Challenge where they experimented with how hackers try to penetrate systems to cause damage to networks. In the first Cyber Security Challenge, only teams from the DoD were invited to participate, but this year NDU has opened up participation to include technologists from civilian agencies. This year's players came from DISA, the FAA, the military academies, and others from across the military. Representatives from the Departments of State and Homeland Security served as observers.[28] In this scenario, each team is provided two computers, one for launching attacks against the opposing team, and another for defending their systems. Teams earn points by successfully infiltrating other team's systems, and they are docked points when they system is infiltrated. As Major Stephen Mancini explains, "There are security officers that only understand what an attack will look like after their systems get broken into,

[22] http://www.northropgrumman.com/presentations/2009/072909-linda-mills-cyber-security-media-briefing.html

[23] http://www.parkairsystems.com/index.php?option=com_content&task=view&id=151&Itemid=2

[24] http://www.af.mil/news/story.asp?id=123201999

[25] Ibid

[26] http://www.global security.org/military/ops/eligible-receiver.htm

[27] http://www.infosecnews.org/hypermail/9804/0217.html

[28] http://fcw.com/articles/2010/03/12/web-cyber-defense-competition-ndu.aspx?s=fcwdaily_150310

and often it's not until months later. Rarely do they get to see what's happening in real time. This provides them the opportunity to be the bad guy in a nice segmented network."[29]

And the Air Force is cascading the importance of exercises down to lower echelons as well. As an example, Buckley Air Force Base in Colorado Springs, CO, just completed its first Cyber Lightning Exercise. As Col Trent Pickering, the 460th Space Wing Vice Commander stated, "It gives us a peek under the tent on how we will command and control this base, and maintain our mission operations, in an environment where an adversary is attempting to deny us some of our key communications capabilities."[30] Cyber Lightning featured numerous challenges to the airmen at Buckley, from network degradations and partial outages to hacking and phishing and social engineering attempts to gain access to sensitive information networks. At various points during the exercise, e-mail, chat room, and base radios were disabled for the airmen. As a Buckley spokesman explained, "Overall, the exercise went very well and met the intention that the commander provided us as objectives. We forced the wing to develop and implement back-up communications and operational procedures, while under fire no less. It identified areas where we need to refine our processes and procedures, but that was exactly the point."[31]

Furthermore, as we observed in academia, the DoD is also investing in safe environments in which to test and perform repeatable information operation exercises and experiments. The U.S. Joint Forces Command (JFCOM) in Norfolk, VA, has invested in an Information Operations (IO) Range designed and built specifically to enable warfighters to experiment with military deception, psychological operations, electronic warfare, and computer network operations. [32] The idea behind this range is to allow warfighters to have a flexible, seamless, and persistent environment to test cyber operations in order to achieve certain non-kinetic effects much the same way that warfighters test the effects of kinetic weapons on a bombing range. The range has more than 60 nodes both in the States and the international community, and "supports the development, experimentation, testing, training, integration and synchronization of the core capabilities and supporting activities of persistent and emerging IO and cyber activities."[33] In the past, if a commander wanted to ensure freedom of maneuver in the airspace over a certain territory, he often opted to kinetically destroy assets used to defend that airspace. Today, with cyber operations, it may indeed be possible to restrain the air defense assets of the enemy without traditional electronic warfare jamming, firing a shot, or dropping a bomb.

Other Governmental Agencies

A recent survey found that the majority (61%) of the 200 IT professional security managers in both civilian and non-civilian governmental agencies assessed the possibility of being cyber attacked as "high." Fully one-third reported that their networks had indeed been attacked by international groups and terrorists within the past year. About 40% of the respondents assessed the government's ability to defend against these cyber attacks as "poor to fair at best."[34]

So, as one may surmise, there are a plethora of government agencies involved in experiments, evaluations, and exercises to get better prepared for the next attack. Indeed, the CIA reported in its newly-unveiled Five Year Strategy Plan that investing in technology to fight and prevent cyber threats is one of its three main tenets.[35]

---

[29] http://www.nextgov.com/nextgov/ng_20100218_2405.php

[30] http://www.af.mil/news/story.asp?id=123228646

[31] Ibid

[32] http://www.afcea.org/signal/articles/anmviewer.asp?a=1770&print=yes

[33] http://www.jfcom.mil/about/fact_iorange.html

[34] http://www.computerworld.com/s/article/9174906/Threat_of_cyberattacks_from_overseas

[35] http://www.informationweek.com/story/showArticle.jhtml?articleID=224600617

Charles Winstead, NSCI
Jim Ed Crouch, NSCI
November 19, 2010

Instead of expounding into each of these government agencies exercise programs, we have selected those we perceive as the largest of these exercises for discussion.

As we found when looking at major investments in both the academic and military communities, cyber security professionals in other government agencies have also invested a significant amount of their research funds in providing a cyber range to conduct testing and experimentation of both offensive and defensive cyber operations. The National Cyber Range is a component of the Comprehensive National Cybersecurity Initiative (CNCI), even though its lead agency for implementation is the Defense Advanced Research Projects Agency (DARPA). DARPA's role in the DoD is to bring high-risk, high-return programs on line quickly and efficiently, so this agency appears to be a logical pick to serve as the lead for bringing on the NCR in a timely manner. Started during President Bush's administration, CNCI is a $40 billion major government-wide program whose purpose is to increase the nation's defenses against electronic attack. As the need to create a test bed for experimentation of both offensive and defensive cyber operations became pressing, the CNCI team looked across the cyber professional spectrum and decided a consortium of government, industry and academia was needed to ensure the most comprehensive outcome. [36] During Phase one of the NCR Program, a number of industries, Johns Hopkins Applied Physics Lab, and DARPA created the initial designs, concepts of operation, and detailed engineering plans. In the Phase 2 down-select, Lockheed Martin was awarded a $31 million contract to build and evaluate the prototype ranges, while Johns Hopkins was awarded a $24.7 million contract as a partner. As Michael VanPutte, the DARPA Program Manager states, "We're looking at revolutionizing the state of the art of cyber testing itself. We want to create a test range that is fully automatic and rapidly configured so that we can get the results back out to the community." VanPutte continued, "We don't want to take six months to do the test and another three months to do the analysis. We want to do a large number of tests rapidly and really push the comprehensive national cyber initiative to get technologies deployed."[37] While VanPutte affirms that the NCR will be capable of both offensive and defensive cyber operations, he speculates that most of the tests and exercises will be on the defensive side. DARPA is scheduled to transition the NCR to some as-yet-unidentified operational partner when the range has been fully tested and accepted.[38]

Established in the aftermath of the 9-11 attack on the US, the Department of Homeland Security's job is to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. This, of course, includes preparing for cyber attacks, so it is no wonder that DHS has developed the Cyber Storm (CS) set of exercises, which are the largest and most comprehensive in the US. The DHS's National Cyber Security Division (NCSD) successfully performed the first Cyber Storm exercise from Feb 6 - 10, 2006. The first Cyber Storm exercise was designed to test communications, tactics, techniques, and procedures in response to various cyber attacks against the US. DHS was interested in exercising interagency coordination, inter-governmental and intra-governmental coordination, public and private information sharing mechanisms and identifying the interdependence of cyber and physical infrastructures. "Exercises like Cyber Storm are essential to our continued efforts to secure cyberspace and America's cyber assets," said George Foresman, DHS Under Secretary for Preparedness. "We are committed to working with our public, private, and international partners to turn the lessons learned from Cyber Storm into solutions for enhancing our nations' cyber preparedness and response capabilities."[39] There were more than 110 public, private, and international agencies, organizations, and companies involved in the planning and implementation of Cyber Storm I. Experts from the public and private agencies and companies helped ensure that the exercise realistically simulated a series of coordinated attacks on critical US infrastructure in the information technology, communications, energy, and

[36] http://fcw.com/Articles/2010/05/26/Defense-IT-1-Cyber-Range.aspx?p=1

[37] Ibid

[38] http://www.bizmonthly.com/3_2010/2.shtml

[39] http://www.dhs.gov/xnews/releases/pr_1158341221370.shtm

Charles Winstead, NSCI
Jim Ed Crouch, NSCI
November 19, 2010

transportation (air) sectors. The major adversarial objectives were to" (1) disrupt specifically targeted critical infrastructure through cyber attacks; (2) to hinder the governments' ability to respond to cyber attacks; and (3) to undermine the public confidence in the governments' ability to provide and protect services."[40]

Cyber Storm II (CS-II) was conducted for five full days in March 2010 and included participants from nine states, four foreign governments, 18 federal agencies and over 40 private companies--about 2,500 people from the US, UK, Canada, Australia, and New Zealand. CS-II focused on responding to critical cyber attacks on information technology, communications, chemical and transportation infrastructure. DHS, the FBI, and the DoD were among the major federal agencies that participated. The scenario for CS-II was much more sophisticated and complex than the scenario in CS-I, and it took a full 18 months just to plan this exercise. Simulated elements from organized crime, political activists, hackers, and international terrorists were all represented in this CS exercise.[41] As Gregory Garcia, DHS Assistant Secretary for Cyber Security and Communications explains "You have a simulated incident that comes in over the e-mail and it may have only to do with the chemical sector at this point. There's an employee in the chemical sector who's arrested. He was fired the day before and did something to sabotage the network...so somebody in the chemical sector gets that "OK, what do I do with that?"[42] The exercise is designed to overwhelm participants and allow emergency responders to find out if their plans work out as expected and experience if people react to situations as the response planners thought they would. Garcia went on to offer a lesson learned, "It's better to exchange business cards now rather than during a crisis. If the exercise never even took place, I think people would have come away with a much better appreciation of what their vulnerabilities are, what could potentially happen to them, and how they need to connect with in this vast network. "[43]

Cyber Storm III occurred in September 2010 and included a scenario that was even more comprehensive and complex than the first two exercises. Exercise participants included professionals from 11 states, 12 countries, and 60 private sector organizations. Participants were warned that they could expect as many as 1500 "injects" or separate events which could be injected into the scenario. The primary goal of this exercise was to test the National Cyber Incident Response Plan which was released in late 2009. Phil Reitinger, Deputy Under Secretary of the DHS National Protection and Programs Directorate, explained, "One of the things I think it's critical to recognize about cyberspace is it's beyond the capability of any one government agency to respond, or even one government or one private sector entity. This really requires a joint response."[44] Reitinger continues, "Right now it is indisputable that our risk as a community and a community of nations is growing. People recognize that we have a problem and we are working as a global economy, a set of nations to address it."[45]

In early 2010, the Bipartisan Policy Center hosted a cyber exercise called Cyber Shockwave, which set out to explore the policy issues involved in Federal Government reacting to a massive cyber attack on the US. In the scenario, an unknown group or nation state sent a virus via smart phones which eventually resulted in phone service being shut down, the internet slowed to unmanageable speeds, and portions of the nation's electric power grid were disrupted. The attack also affected the networks of the transportation systems, the stock exchange, and the financial institutions. In essence, the US was disconnected from the worldwide web. Former government officials from both the Bush and Clinton administrations took the roles of the President, Secretaries of Homeland Security, State, DoD, Transportation, and other high ranking Government officials. Various industry representatives were also participants. "A lot of our attention ought to be focused on the ability to quarantine this problem before it spreads," said Stephen Friedman, the former Director of the National Economic Council who

[40] http://www.dhs.gov/xnews/releases/pr_1158340980371.shtm

[41] http://fcw.com/articles/2008/02/29/cyber-storm-ii-stirring.aspx

[42] http://www.pcworld.com/article/144374/us_cyber_storm_exercise_complete.html

[43] Ibid

[44] http://*www. pcworld.com/businesscenter/article/206554/cyber_storm_iii_simulates_largescale_attack.html*

[45] http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1514918,00.html

Charles Winstead, NSCI
Jim Ed Crouch, NSCI
November 19, 2010

was role playing as the Secretary of Treasury.[46] However, this requires the regulation of the private sector because about 85% of computer networks are owned and operated by the private sector. Other issues probed were whether the President had the authority to declare a devastating cyber attack as an act of war, thus giving the President more powers to react to attacks, especially if there was no sure attribution as to who was initiating this action? As Clinton's former Deputy Attorney General, acting as the exercise Attorney General, said, "The President has no statutory authority in any of these situations, and would have to assert authority and make orders and ask retroactively for those authorities to be ratified. But we just don't abandon the Constitution."[47]

Summary and Conclusions

We believe most cyber professionals agree that experiments and exercises should help us discover, learn, and practice cyber security more efficiently and safely, and we have seen significant progress in the communities documented in this paper.

In Academia, we see good progress and cooperation with the Government and Industry partners in educating, experimenting, and collaborating at the collegiate levels and even in some progress in the secondary education levels. However, we agree with Dr. David A. Honey, Chief Technology Officer for the DoD, that we must reach out to students as early as primary education to excite them on focusing on scientific, technology, engineering, and math (STEM) curricula. Dr Honey is responsible for policy and oversight of the DoD Science and Technology programs from basic research through Advanced Technology Development, and he asserted at a recent InfoTech 2010 Conference that if we waited until the fifth grade to excite our youth about how exciting STEM subjects are, we have missed important milestones in students development.[48] We believe that this initiative is largely a local community responsibility, with the assistance of the Government and industry partners. There is a lot of work needed in this area.

We understand that due to the competitive nature of businesses, sharing lessons learned with competitors is a difficult bridge to cross, but we urge the Government to increase its efforts in sharing these lessons with national and international stakeholders, in confidentiality when available. We are very supportive of the work being accomplished by The Financial Services Information Sharing and Analysis Center, and recommend even further commitment from this group to help businesses understand and appreciate the cyber vulnerabilities and risks they have and share lessons learned with other businesses. There is plenty of room for growth here.

We are optimistic about the future of the National Cyber Range now under construction. If this initiative delivers even half of what it promises, it will be a great environment to advance cooperation across the Government agencies and industry to share cyber lessons learned. Additional range-like capabilities are needed to allow government, industry, and academia to collaboratively tackle non-kinetic effects.

At the Department of Defense, we see good progress in the growth of cyber exercises. We applaud the recent standup of US Cyber Command as a sub-unified command under United States Strategic Command, but we also agree with the caution many have expressed regarding the command and control structure and relationship with the National Security Agency. We anticipate this command will exert its leadership and influence to provide a DoD-wide cyber exercise program which can reap enormous benefits. Today, each of the services has a training infrastructure with its own requirements, tactics, techniques, and procedures. We see this approach as wasteful and ineffective and are eager to see how USCYBERCOM tackles the challenge of integrating a cyber exercise program for all DoD. While the DoD appears strong in cyber exercises, we were unable to find any significant results regarding cyber experimentation. Given the opportunity for discovery and learning via experimentation,

[46] http://www.nextgov.com/nextgov/ng_20100216_5378.php?oref=search

[47] Ibid

[48] http://hosted.mediasite.com/mediasite/Catalog/pages/catalog.aspx?catalogId=50916593-99d3-4651-8016-535c838d3f73

and the relative newness of cyber as a domain, we believe a focused cyberspace experimentation program would enhance the exercise efforts. Especially important is experimentation and exercises related to the integration of cyber with air, land, space, and maritime planning and operations.

Additionally, there seems to be significant opportunity for increased cyber experimentation and exercise at the state and local levels. Establishing an exercise program at the city and/or state levels would not have to be cost prohibitive. It does not have to be as grandiose as DHS's Cyber Storm, but could be as simple as local communities doing tabletop discussions to talk through a cyber scenario. Local communities could conduct tabletop exercises to talk through the various policy issues, processes, authorities, and roles and responsibilities. Conducting these exercises is key to establishing relationships and trust prior to a crisis. On this point, we agree with Gregory Garcia, DHS Assistant Secretary for Cyber Security and Communications, that the time for exchanging business cards is prior to – not during – a crisis. As an example, we believe it is not a matter of *if,* but rather *when* our Supervisory Control and Data Acquisition (SCADA) infrastructure will suffer a cyber attack. SCADA controls our power grids, our transportation systems, our sewer and water generation plants--the very infrastructure of our towns, cities, and states. This type of threat could be "played out" via a tabletop discussion at the local level.

From an educational perspective, it would be beneficial if more cyber users could be involved in cyber experimentation and exercises; or at least made aware of the lessons learned and best practices. Thus exercises and experiments should be designed that help not only major organizations, but also the everyday user - where many cyber threats begin and multiply.

As a whole, we applaud the commitment and progress of government, academia, and industry as it relates to cyber experimentation and exercise. While more is needed, we believe this is one of the few cyber-related areas with activities *and results* showing public-private collaboration and improvement towards a safer and more secure cyberspace.