American Security in a Networked World: Emerging Challenges in Cyberspace

Policy Paper and Directive

SCUSA 64 – Nov. 7-10, 2012

The American Security in Cyberspace Roundtable:

Megan E. Beyer, Smith College
Dustin Downing, Merchant Marine Academy
Charles Fiertz, St. Mary's College of Maryland
Gavin Moore, Texas A&M University
Mohamed Mouhktar, US Military Academy
Anthony Palmer, Gettysburg College
Graham Starr, Tufts University – *Lead Author*
Lina Tbatou, John Jay College

Robert W. Clark, Co-Chair
David Raymond, Co-Chair

Christopher M. Kelly, CPOC, US Military Academy
Andrew Thompson, Roundtable Scribe, US Military Academy

We are entering a changing venue of conflict. What used to be considered the five domains of warfare has added a sixth: cyberspace. As defined by the National Security Presidential Directive, cyberspace is an "interdependent network of information technology infrastructures, [including] the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries" (NSPD 54). Due to the disorganized and open nature of cyberspace, many positives arise in the realm of communication and in bridging the information gap. However, problems and detriments to security are ever present, as we find the world on the receiving end of attacks from state and non-state actors. Additionally, we find ourselves submerged in increasing security risks, from malware, advanced persistent threats, or simple human error in the field of technological responsibility. Among the problems and tumult we face, the most pressing issues are those of malicious actors and compromised human factor risk – specifically involving cyber warfare/espionage and individual vulnerability. Consequently, we are adjusting and adapting to the ever-persisting climate of International and Personal Security threats.

As a policy directive, we are proposing a greater future in American security in cyberspace through a joint approach in education and the strengthening of existing capabilities of full-spectrum cyberspace operations, while protecting personal privacy and civil liberty concerns. We hope to engage additionally in multilateral efforts, to promote legitimacy and improve security and responsibility in the field of cyberspace in the international order. We aim to accomplish this through a series of both short-term and long-term approaches: improving education, aiding in the development and strength of centers of critical infrastructure (CCIs), and decreasing the risk and jeopardy associated in the human element involved in many compromising circumstances, among others. This will create a more secure, sustainable, and flexible system moving forward, as cyberspace concerns become evermore present and relevant.

A focal tool in improving the security of the United States in the field of cyberspace results is an increase of education, and a more innovative approach to addressing education concerns. As technological advancement become more and more prescient, the discord between the younger and older generations in cyber literacy follows suit. Historically, the response has been to engage the youth in the issues with which those in policymaking position have problems; however, this leads to a perpetuating dilemma - a consistent schism between the older and younger generations on issues of current national security concerns. This, unfortunately, also leads to a limited population engaged in the technological workforce. Coupled with the current unemployment and economic crises, our directive in improving security must also take into account the measures inherent in an austere time and the possible improvements to both fields. The ways we offer to tackle these concerns are through increased education and training programs, both for those already in the workforce, and those about to enter it.

In order to better improve the future of the cyber security front, we aim to promote education in the technological fields starting with primary and secondary schools. We promote, working jointly with state governors and the department of education, the application and augmentation of computer science classes and recommended curricula starting as early as the 3rd grade. In combination with the already-promoted STEM coursework, this will create a larger workforce into the cyber security field, as well as a better educated and less vulnerable populous, something that will be specified and elaborated on later in this directive. There is no age too early to learn how to prepare oneself for the future of technology. As has been seen through development markers, most specifically the World Development and Technological Assessment Reports, an increased devotion and prioritization toward rising technologies results in increased stability, productivity, and economic performance.

But the encouragement does not stop at the elementary or primary schools. We hope to foster an even greater improvement and interest in the field of cyber security, and an accretion of the technological talent available at the university level. In the same line as other government scholarships and programs, we suggest a movement of funding toward student programs and scholarships directed at those interested in the cyber security or computer science fields, adding onto the already existing STEM-favored directive. Of course, this funding will be widely available on the condition that the recipient devotes 1.5 times the number of years that they benefitted to work in the cyber security field for the US Government. While we understand that this is an age of austerity, and increased funding is a mission not favored by many, the benefits to the US economy, workforce, and national security will be exemplary and beyond expectation.

Additionally, we propose a further movement toward partnerships with universities for the same objectives in improving our talent base and increasing technological literacy. By improving the already stellar *Centers of Academic Excellence* list of colleges and universities, more and more students interested in cyber security may engage in and take advantage of the many perks available in working for the public sector. By also offering up similar directives to those in the private sector, an example of which being “Hackathons,” we may more efficiently and creatively scout talent, recruit future employees, and receive greater insight into our operations from the younger and most promising generations.

But, of course, we must still take into consideration the climate in which we live – an economically tumultuous one filled with high unemployment and higher expectations for those out of the workforce. In order to solve both problems jointly, we propose a mid-career Information Technology elective training program, offered to both businesses and individuals, in order to improve skill sets in the job market. As a consequence of this economic downturn, many employed in production sectors are without a job or the skillset with which to get another. Through this initiative, we may improve not only our unemployment rate and economy, but also the general technological literacy of the mass populous, augmenting our nation’s citizens’ personal security.

But as this is an austere time, we must require a more creative approach to funding. We have conducted cost-benefit analyses in order to best allocate and streamline the economic approach to these programs. As those involved in these programs will be brought into our national units combatting cyber security concerns, the benefits greatly outweigh the costs. Additionally, we will be working with private industry and individual electivity in order to best operate these programs. These initiatives will be funded in part through financial incentives directed at businesses that take part, as well as to those private industries partnering with the US Government in offering these training programs. We will thusly increase productivity while augmenting our workforce and the incentive of tech conglomerates to participate with greater involvement in United States affairs.

But how these affect the personal security and infrastructure of the United States as a whole, and fosters greater American Security in this networked age, comes through responses to what actually threatens our cyber structures and security institutions. A main trouble in the field of personal security comes in the field of human error. An email will be received. "Work Memo November 10th" it will say, so you open up the unencrypted document from someone whose name you may not recognize, but it *definitely sounds familiar*. You find yourself on the receiving end of a malware plot. You don't know how to accurately check for safe files, and the fact that you just opened that corrupt pdf file on a work computer just spread all that bad stuff throughout your company's or organization's databases and infrastructure, compromising private material and intellectual property, among other possibly more severe points of vulnerability.

So we have a couple issues: 1.) Why were you unable to see that email as a potential security risk, and 2.) Why was your business, company, or organization unable to deal with the issue accordingly and without compromise? A lot of it goes back to education. Through the programs and initiatives discussed earlier, the average individual will gain cyber literacy, and know how to avoid threats and security risks, and how to deal with them if they arise. But from the perspective of a secured system and network, more needs to be done; critical infrastructure needs to be improved and made more secure so that one does not compromise another's security through his or her own ignorance on the issue. Workshops, in the same realm as the education initiative listed above, will push toward more cyber literacy and a greater defensive capability of the private industry, but regulation standards must be created so as to ensure safety and security across the board for all American institutions. These regulations and reforms will also play into the personal security of the individual in the realm of privacy and communications. By fostering open-source and policy initiatives to more simplify and streamline User License Agreements (ULAs), the individual will not be as threatened from privacy concerns of programs of which terms they do not support. But the business must also be safe from unwanted expenditure in the scope of increased regulation and reform.

We cannot compromise the openness of the Internet; so, in order to keep systems safe, we must act more innovatively and creatively. One major problem in the field of cyber security is that of unapplied patches to software – when a software or program discovers a problem, the patch will fix it, and those who wish to act maliciously will then attack those with un-updated software. In order to improve the security of centers of critical infrastructure (CCIs), we propose to add a layer to all .gov, .mil, and other government websites in circumstances that may compromise our systems. This will be in the form of a government-administered scan. We, according to the Computer Fraud and Abuse Act, cannot administer any software or fix, including scan, without consent. Depending on the critical nature of the database accessed, a webpage will be available offering a free scan of malicious content and out-of-date major software, for one's computer. The scan, a short-term strategy and solution that can be very easily authored and distributed, and done so quickly, will then rate the security of the system scanned and offer ways in which to clean the system, with helpful walkthroughs provided by those directed under the Department of Defense human resources and technology departments. The rating system applied to the MAC address and other identification aspects of the system will then limit access to the database until whatever concern is mended. While this may pose problems to some who must access certain sectors of the Internet, we assure you that most of those databases will be structured internally in order to deter attack, but those involved in the technological world must rise to meet the challenges it poses. While this may not be an easy transition for all of us, it is a necessary one.

But while we strengthen ourselves at home, we must not forget the challenges we face from actors abroad, and malicious intent that may compromise or subvert our defensive capabilities. And thus we must address in this directive the most effective and efficient means in which to strengthen American security using a full-spectrum cyber operations approach. We propose, through this directive, a type of "Cyber Militia," as a response and readiness team, set to fix situations that arise. The US Government will work with the private sector technology firms in order to contract the best and brightest. These individuals will not, however, leave their day jobs, as the private industry will ensure the individual's salary, which the federal government cannot under these austere times, and because this leads to a consistent keep-up with issues in virtual and information technology. When a problem arises, let's say what appears to be a maliciously-intended piece of software propagating itself in order to shut down a power grid, those in the trade and "Cyber Militia," will be notified or will, without a needed directive, notice an inconsistency, and will aid the US Government in tracking down and stopping the threat. For this, the individual and his or her business, which allows us to contract their employee, will receive financial incentive.

There is an underlying theme here, and that is the one of vulnerability. Upper-level secure encryption is near impossible to crack, even by very powerful computers. But the human mind is notoriously easy. While I may not be able to break into your network by myself, if you give me an unencrypted door, I can wreak damage. So we must decrease our vulnerabilities in order to increase security. Our way in which to do that is by focusing on the major concerns of personal and international security, under which we have problems in number of computer scientists in the workforce and in the knowledge base of those that must protect our nation from vulnerabilities in promoting American security. In this networked age, our way of going about these improvements relies heavily on education improvement and on partnerships with industry. Through these directives, we may improve the general security and safety of the population, while also ensuring no breach of individual privacy or civil liberty. Once our general population is more educated, we will become less subject to threats and vulnerabilities, and malicious threats, in the form of cyber warfare, espionage, or exploitation, will cease to be as large an issue; after all, our population will be able to deal with anything thrown at them. On a similar line, we aim to act in multipolar forms, working with our allies in promoting similar programs.

We must protect our infrastructure; we must protect our freedoms; we must protect our people. By empowering the people through government- and policy-directed initiatives, our population will be built up stronger and more willing in this austere time, not only in improving our economy, but also in augmenting our cyber security capabilities, leading to a more full-spectrum and effective approach in dealing with challenges in cyberspace.