Cyberspace Security and Attribution

General (Ret) Ron Keys, RK Solutions;
Charles Winstead, NSCI;
Kendra Simmons, NSCI Intern (ECPI)

July 20, 2010

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated. . ." So says Article IV of the United States' Bill of Rights.[1] Many would argue that today the United States is the most powerful nation in the world. And with this power comes a great deal of responsibility. As Article IV states, the United States government is ultimately responsible for the security of its citizens. This responsibility extends far beyond the traditional arenas of land and sea that our forefathers knew in December of 1791 when the Bill of Rights was signed. In addition to the Air and Space domains which have since been added, today we have an entirely new dimension, Cyberspace, which literally touches all citizens every day--it underpins our Federal Government, including our Department of Defense and Department of Homeland Security protecting our security and our critical infrastructure such as banking systems, electrical power grids, transportation systems, and water plants. Today, technology is constantly evolving and touching more and more aspects of our daily lives, and those who would seek to violate our right to security in our houses and our effects are evolving as well. High-tech crimes involve the use of computers, the internet, and other electronic devices to violate our security. And these crimes not only affect us here in the United States, but also how we interact with others here and around the world. In order to combat high tech miscreants who would seek to violate our security, some groups argue that a universal strategy needs to be established. This strategy must involve the use of cyber attribution.

At the same time, others are concerned that their right to privacy and other civil liberties will be compromised because of the government's use of cyber attribution. All too often, some jump to the conclusion that attribution must necessarily involve the government, specifically the National Security Agency and now the newly established US Cyber Command as the attribution power. What is often overlooked is the 'attributing attributes' already in use today. We already have serial numbers on all types of products, as well as VINs on automobiles, and all the way to exploding dye packets in sacks of stolen money. All of these methods help in establishing ownership and by extension attribution when someone else takes the items. At that point the appropriate civil/criminal process kicks in to apprehend and treat the miscreant appropriately… without a lot of concern that the government is somehow on fishing or snooping expeditions.

Legal and policy issues must be addressed to enable domestic as well as international cyberspace attack attribution. This white paper will explore the responsibilities of our Government to provide its citizens security in Cyberspace and balance this responsibility against our basic right to privacy. These debates are happening on a daily basis. What are the rights versus responsibilities of the Transportation Security Agency to screen us before we fly, the Customs and Border Patrol agents that screen our passports and ask for information at borders, the information that we must now provide in order to get a driver's license… it goes on and on. But almost no where is there more concern and activism than surrounds the ubiquitous, friendly, innovative, but potentially dangerous Internet.

While not developed by us, we have provided some definitions of what Attribution means in cyberspace today in order to provide a framework for the discussion that follows:

[1] *United States Constitution*. Retrieved July 1,2010, from Cornell University Law School: http://law.cornell.edu/constitution/constitution.billofrights.html

Cyberspace Security and Attribution

General (Ret) Ron Keys, RK Solutions;
Charles Winstead, NSCI;
Kendra Simmons, NSCI Intern (ECPI)

July 20, 2010

Attribution means knowing who is attacking you, and being able to respond appropriately against the actual place that the attack is originating from.[2]

Attribution as it relates to cyber warfare is also defined as "determining the identity or location of an attacker or an attacker's intermediary."[3]

In the case of a cyber attack, an attacker's identity may be a name or an account number and a location may be a physical address or a virtual location such as an IP address.[4]

Successful cyber attacks have placed sensitive information into the hands of criminals and have compromised official websites as well as financial data. These attacks have caused concerns and fears that criminals or terrorists could use cyberspace to paralyze communications infrastructures, international financial systems, critical governmental services, or any number of other services we depend on in our everyday lives. In order to prevent cyber criminals, attribution has been identified as one of the most important tools of deterrence in cyberspace. Without attribution, both deterrence and retaliation are nearly impossible. Attribution is necessary before a group can take any action including offensive computer attacks, arrests, or lawsuits or kinetic attack.[5] And, attribution can be very difficult if you start from square one…knowing only that you have been penetrated, unsure of what was "taken", and having no pre-existing tracing modalities extant. Indeed," the unfortunate reality is that technical attribution of a cyber attack is very difficult to do (it is often said that electrons don't wear uniforms), and can be nearly impossible to do when an unwittingly compromised or duped user is involved."[6]

A high level of confidence is required in attribution to verify that the identified source of cyber attack is actually the responsible party. Because the Internet today offers almost complete anonymity for users, technical issues often make attribution more difficult. Cunning hackers can actually fake web addresses, use multiple servers and access the Internet from any number of physical locations. Because of these capabilities, a "traceback" approach to attribution, which begins with the victim computer and attempts to trace an attack backwards to its source, is often difficult to implement without foresight and preparation; which generally is lacking today, and in some instances might be questionably legal under today's unprepared policy regimes. [7]

Some argue that attribution techniques do not necessarily have to be hidden. Because attribution itself can serve as a deterrent if attackers know their anonymity is at risk, there are incidents where attribution should be exposed.

---

[2] Morrill, D. (2006, August 7). *Cyber Conflict Attribution and the Law*. Retrieved July 1, 2010, from Toolbox for IT: http://it.toolbox.com/blogs/managing-infosec/cyber-conflict-attribution-and-the-law-10949

[3] Wheeler, D. (2003, October). *Techniques for Cyber Attack Attribution*. Retrieved July 1, 2010, from Institute for Defense Analyses: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859&Location=U2&doc=GetTRDoc.pdf

[4] Wheeler, D. (2003, October). *Techniques for Cyber Attack Attribution*. Retrieved July 1, 2010, from Institute for Defense Analyses: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859&Location=U2&doc=GetTRDoc.pdf

[5] Wheeler, D. (2003, October). *Techniques for Cyber Attack Attribution*. Retrieved July 1, 2010, from Institute for Defense Analyses: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859&Location=U2&doc=GetTRDoc.pdf

[6] Owens, W., Kenneth W. Dam, and Herbert S. Lin. (2010). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use*. Retrieved July 1, 2010, from The National Academies Press: http://www.nap.edu/openbook.php?record_id=12651&page=R1

[7] Wheeler, D. (2003, October). *Techniques for Cyber Attack Attribution*. Retrieved July 1, 2010, from Institute for Defense Analyses: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859&Location=U2&doc=GetTRDoc.pdf

[General (Ret) Ron Keys](), RK Solutions;
[Charles Winstead](), NSCI;
[Kendra Simmons](), NSCI Intern (ECPI)

July 20, 2010

Laws and policies are often vague especially concerning Internet related crimes and may even be outdated due to rapid technological evolution. As a result, cyber attackers are able to perform unlawful acts that cannot be prosecuted under outmoded strictures of "physical law." Without physical borders, the Internet is a "system that is essentially lawless and lawful at the same time."[8]

The sheer volume of vulnerable electronic devices in the world makes attribution even more difficult. There are more than 1 billion PCs in the world, and there are 3.3 billion cell phone subscribers. These devices can have multiple operators as well. These numbers make attribution more difficult because if an attack could be traced back to a physical machine, it would still be extremely difficult to identify the user of the machine, or who controls the device. This makes punishing cyber criminals difficult because we must be able to prove who is carrying out the attack. We must also be able to prove that we have the ability to know who is attacking without giving your enemies the knowledge that will allow them to develop better ways to hide attacks.[9] Of course, it is impossible to investigate, or attribute every cyber attack. For this reason, cyberspace attacks should be categorized based on their potential effect. Currently, most cyber attacks must be large attacks directed at government or large commercial organizations, or have a large economic impact with enough media coverage to warrant the use of limited political, legal, law enforcement, military, etc. resources.[10]

Demand for more robust cyber attribution has a great number of supporters. Supporters believe it a necessary tool to counter cyber attacks along with identity theft, child pornography and enticement, and terrorism. Supporters also believe that without attribution, it is impossible to enforce policy, law, or treaties to support business and government objectives. While attribution is certainly a centerpiece to cyber security, another important component (that can be dealt with without solving attribution) is codifying and enforcing private/public/individual responsibility laws that mandate improved cyber hygiene, product liability, information sharing, and indemnification; which begins to build the solid framework to establish attribution processes.

In the private sector, companies are dealing with Cyberspace security in different ways. Microsoft devised a way to balance privacy with security needs within their business and their employees. They have launched new tools for its "U-Prove" I.D. Project. U-Prove allow employees to share select information about themselves to establish identity online. Employees are not required to unveil any more information.

"This concept is analogous to a bar patron who's asked by a bartender to produce his driver's license to prove he's of legal drinking age", states Robert Mullins, a freelance journalist. "The customer only has to prove he is 21, but the license reveals his name, address, height, weight, eye color and other information the bartender does not need. U-Prove in the computer world will only reveal the customer's age."[11]

Google and the National Security Agency have combined forces to crack down on cyber attacks. The former Director of National Intelligence, Dennis Blair, stated that "Cyberspace cannot be protected without a collaborative

---

[8]Morrill, D. (2006, August 7). *Cyber Conflict Attribution and the Law*. Retrieved July 1, 2010, from Toolbox for IT: http://it.toolbox.com/blogs/managing-infosec/cyber-conflict-attribution-and-the-law-10949

[9] Gourley, B. (2008. May 29). *Towards a Cyber Deterrent*. Retrieved July 1, 2010, from CTOvision.com: http://ctovision.com/references/towards-a-cyber-deterrent/

[10] Morrill, D. (2006, August 7). *Cyber Conflict Attribution and the Law*. Retrieved July 1 , 2010, from Toolbox for IT: http://it.toolbox.com/blogs/managing-infosec/cyber-conflict-attribution-and-the-law-10949

[11]Mullins, R. (2010, March 4). *Microsoft launches new tools for its "U-Prove" I.D. project.* Retrieved July 1, 2010, from Networkworld.com: http://www.networkworld.com/community/node/58181

General (Ret) Ron Keys, RK Solutions;
Charles Winstead, NSCI;
Kendra Simmons, NSCI Intern (ECPI)

July 20, 2010

effort that incorporates both the U.S. private sector and our international partners."[12] Privacy advocates dislike this approach and want information shared between the government and the private sector to be limited and closely monitored.

In order for partnership between private companies and the government to exist, trust must be established. Private companies do not necessarily trust the government to keep their secrets because they fear collaboration may lead to the government continuously monitoring their private communications and/or inadvertent disclosure of proprietary information. Sources with knowledge of the NSA and Google arrangement revealed that "the alliance is being designed to allow the two organizations to share critical information without violating Google's policies or laws that protect the privacy Americans' online communication."[13] This is similar to the intelligence communities practice of "collateralizing" or stripping sources and methods from intelligence so it can be disseminated in useful form at a lesser classification and protect collection capabilities. In the Private/Public partnership, a process has to be adopted that can strip out proprietary and competition sensitive information, while leaving in the details of the attack for other's defensive purposes.

A report prepared by James A. Lewis of the Center for Strategic and International Studies states that cyberspace enables anonymous attacks from sophisticated opponents. "The United States is far more dependent on digital networks than its opponents, and this asymmetric vulnerability means that the United States would come out worse in any cyber exchange**."** [14]

Speakers at the first World Wide Cyber Security Summit in May of this year acknowledged that lack of attribution is a weakness in cybersecurity. They called for a global electronic architecture that allows cyber attacks to be traced back to their original sources. Retired Lieutenant General Harry Raduege, Chairman of Deloitte Center for Cyber Innovation, stated that "You need to be able to define who you're declaring war on."[15]

A panel of experts at the summit suggested that a two-tiered structure would be able to balance the need for security in Cyberspace and the freedom or privacy necessary for innovation. The two tiers would consist of a lower tier in which individuals could interact anonymously and another tier that would require strict authentication. This structure is similar to online business transactions that require attribution. Raduege stated that "If you want to work in the 'Wild West', you can be anonymous. But if you want to interact and conduct business, you need authentication."[16] There was no discussion, however, of who would administer this two-tiered structure, or who would pay for it either. We posit that the cost of identification could be borne by those who need or desire it, namely businesses and the government. The Internet has a community forum that sets standards. Setting a standard on identification of users would allow businesses and the government to conduct vital transactions with

---

[12] Nakashima, E. (2010, February 4). *Google to enlist NSA to help it ward off cyberattacks*. Retrieved July 1, 2010, from The Washington Post: http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html?hpid=topnews&sid=ST2010020402509

[13]Nakashima, E. (2010, February 4). *Google to enlist NSA to help it ward off cyberattacks*. Retrieved July 1, 2010, from The Washington Post: http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html?hpid=topnews&sid=ST2010020402509

[14]Zorz, Z. (2009, October 27). *Serious cyber attacks on the horizon*. Retrieved July 1, 2010, from Help Net Security: http://www.net-security.org/secworld.php?id=8439

[15]Zorz, Z. (2009, October 27). *Serious cyber attacks on the horizon*. Retrieved July 1, 2010, from Help Net Security: http://www.net-security.org/secworld.php?id=8439

[16]Syed, S. (2010, May 4). *Two-Tiered Structure May Allow Both Security and Privacy Online, Say Experts*. Retrieved July 1, 2010, from EastWest Institute: http://www.ewi.info/two-tiered-structure-may-allow-both-security-and-privacy-online-say-experts

General (Ret) Ron Keys, RK Solutions;
Charles Winstead, NSCI;
Kendra Simmons, NSCI Intern (ECPI)

greater security. Just as one obtains verification for a driver's license or passport, a user would get verified to get an Internet ID. This may indeed also open up a new line of business creating these credentials. Estimates of losses due to identity theft range as high as millions of dollars daily. That amount could probably sustain an ID system.

> The FBI tallied $264 million in losses from Internet crime reported by individuals in the United States in 2008 compared to $18 million of losses from 2001.[17]
>
> In 2009, the Pentagon said it spent more than $100 million in a six month period responding to damage from cyber attacks and other computer network problems.[18]

Many times cyber attacks cross jurisdictional lines. In these cases attribution techniques require cooperation and active participation between jurisdictions that may not be able to trust one another. Cyber attackers are taking advantage of the fact that routing an attack through countries that are not on the best of terms with the target country will effectively conceal their identity and location.[19] This is why many are calling for cooperation both domestically and internationally. Indeed, Michael Chertoff, former U.S. Homeland Security Secretary, stated that "we cannot postpone the debate until we are in the midst of a catastrophic cyber attack. We must formulate an international strategy and response to cyber attacks that parallels the traditional laws governing the land, sea, and air."[20]

Dell Services President Peter Altabef said, “Cyber Crime is a very sophisticated crime with very sophisticated players, and it take a multinational effort to make sure we can enforce the law."[21] He also states that “Once you have identified who is at fault you really want to make sure, as a deterrent, that you can go to those jurisdictions and enforce the laws on the books."[22] Tracking down criminal across borders can also pose legal issues for those who draft multilateral regulations. Dell Services Chief Technology Officer, James Strikeleather, states that “the more companies added the technology needed to give investigators the ability to attribute a crime, the more users’ privacy anonymity would be reduced.”[23] And so we return to the age old debate of how much security versus how much liberty.

In poor nations, customers can purchase unregistered SIM cards with mobile Internet capability. This gives them the ability to commit online crimes against people in wealthy nations without being traced. Chairman of the U.N.-affiliated International Multilateral Partnership Against Cyber Threats, Datul Mohammed Noor Amin, said failure to

---

[17] Maclean, W. (2010, February 22). *Cyber Evil Will Thrive Without Global Rules- Good Luck With That.* Retrieved July 1, 2010, from WIRED: http://www.wired.com/epicenter/2010/02/cyber-evil-will-thrive/

[18] Cyber Commander's Handbook; p. 147; technolytics; Jan 2010

[19] Cyber Commander's Handbook: The Weaponry and Strategies of Digital Conflict; pp 10-13; technolytics; Jan 2010

[20] Dick, C. (2010, February). *Spies and hackers exploit world cyber rule void*. Retrieved July 1, 2010, from Reuters: http://www.reuters.com/article/idUSTRE61L37B20100222

[21] Dick, C. (2010, February). *Spies and hackers exploit world cyber rule void*. Retrieved July 1, 2010, from Reuters: http://www.reuters.com/article/idUSTRE61L37B20100222

[22] Dick, C. (2010, February). *Spies and hackers exploit world cyber rule void*. Retrieved July 1, 2010, from Reuters: http://www.reuters.com/article/idUSTRE61L37B20100222

[23] Dick, C. (2010, February). *Spies and hackers exploit world cyber rule void*. Retrieved July 1, 2010, from Reuters: http://www.reuters.com/article/idUSTRE61L37B20100222

General (Ret) Ron Keys, RK Solutions;
Charles Winstead, NSCI;
Kendra Simmons, NSCI Intern (ECPI)

July 20, 2010

regulate could perpetrate cyber "failed states." He believes that rich nations should help poorer countries develop capacity to crack down on Internet abuse because their own citizens are being targeted.[24] Kenneth Geers, a civilian with the U.S. Navy's Naval Criminal Investigative Services who is assigned to Cooperative Cyber Defense Center of Excellence in Tallinn (CCDCOE), states that it is "really easy to hide in cyberspace, you need much more than computer log files to know what happened." He also states that "You have to be able to get back at an aggressor, and in cyberspace, there's no guarantee of that." "You may not know who is attacking you, and to get back at them, you have to hack back or do a kinetic response." He goes on to say that "It is hard to deter an aggressor who can invest a small amount and cause the target 100-fold damage."[25]

Identity theft is becoming a growing epidemic in the United States and abroad. Identity theft is the crime of deliberately stealing someone's personal, identifying information for the purpose of using that information fraudulently.[26] Opponents of cyber attribution are also concerned with identity theft. They feel that allowing access to their personal information can open up a gateway for others to steal their personal information. Of course proponents of cyber attribution would only remark that identity theft is already a leading mode of cyber crime, and requiring strong authentication does not necessarily rely on in depth personal information.

In a recent debate concerning the use of the word "cyberwar," leading voices shared their concerns on anonymity in Cyberspace. "The threat of cyberwar is part of a long-running campaign to move control of the Internet from the current open model to one that would give the [National Security Agency] more authority to control users' activity," said Mark Rotenberg, executive director of the Electronic Privacy Information Center, arguing for the resolution that the threat has been exaggerated.[27]

And Bruce Schneier, BT's top security technologist and a well-known speaker and writer on the topic, offered a similar viewpoint arguing for the resolution. "Cyberwar is a rhetorical term that makes people feel good, like the war on drugs or the war on poverty," he said. "But it's a concept that has been grossly exaggerated by a government intent on grabbing the power and money that the threat can generate."[28]

Criminals steal social security numbers, credit card and bank account numbers, usernames, passwords, and patient records. They use this information to open new credit accounts, take out loans in the victim's name, and steal money from financial accounts. The stolen information can also be used to provide a thief with false credentials that they present to police at the time of an arrest. This creates a criminal record and leaves outstanding warrants for the person whose identity was stolen. It is important to note that none of this happens as a result of the government attempting to put into place a system of authentication.

---

[24]Dick, C. (2010, February). *Spies and hackers exploit world cyber rule void*. Retrieved July 1, 2010, from Reuters: http://www.reuters.com/article/idUSTRE61L37B20100222

[25]Dick, C. (2010, February). *Spies and hackers exploit world cyber rule void*. Retrieved July 1, 2010, from Reuters: http://www.reuters.com/article/idUSTRE61L37B20100222

[26] Knetzger, Michael, & Muraski, Jeremy. *Investigating High-Tech Crime.* Upper Saddle River: Prentice Hall ,2008. p.61

[27] Wilson, T. (2010, June 10). *In Debate, Audience Finds That the Cyberwar Threat is Not Exaggerated*. Retrieved July 1, 2010, from Dark Reading: http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=225600193

[28] Wilson, T. (2010, June 10). *In Debate, Audience Finds That the Cyberwar Threat is Not Exaggerated*. Retrieved July 1, 2010, from Dark Reading: http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=225600193

General (Ret) Ron Keys, RK Solutions;
Charles Winstead, NSCI;
Kendra Simmons, NSCI Intern (ECPI)

July 20, 2010

Every year, approximately 10 million Americans become the victim of identity theft.[29] Of these 10 million victims, an average of $800 to $14,000 is lost. Victims not only lose their hard earned money but they also spend approximately 840 to 1,300 hours trying to clear up credit report matters and other personal information.[30] Depending on the seriousness of the case, victims of ID theft can take about 5,840 hours trying to counter and correct damages. This is equal to working a full time job for two whole years.[31] We suggest that this is an example of where government standards are needed to push identification requirements. Today each business has its own standard; which no one really understands prior to using a web site to conduct a financial transaction.

The Internet makes it easier for terrorists to recruit by providing potential recruits with information that glorifies their causes. They use discussion forums and chat rooms to scope out those who may be interested in joining their cause. They use various techniques to "romance" followers to go along with their devious plans. Because money is the lifeline to a terrorist organization, terrorists use the Internet to finance or raise funds for their activities.

Many terrorist openly request funds from Web surfers who visit their sites, while others use illegal means such as credit card fraud and email scams. They also exploit and infiltrate legitimate charities to raise money for their causes. The internet also allows terrorist to plan and coordinate attacks. It connects members of a terrorist group and allows them to communicate through secure chat rooms. The Internet also gives terrorists the ability to connect globally and puts distance between those planning the attacks and the potential targets without compromising their identities. To stop terrorists from using the internet for propaganda and recruiting purposes, it may seem reasonable to monitor their chat rooms or completely shut down their sites.[32]

Panelists from The International Summit on Democracy, Terrorism, and Security held in Madrid, agreed that strict regulation of the Internet could have an adverse effect on the lives of individuals. They also agreed that interfering with the democratic freedoms offered by the internet would probably damage democracy more than it would harm terrorists. The Internet's positive effects in connecting people outweigh the possibility of abuse.[33]

One of the panelists, Dan Gilmore stated "We believe that an attempt to end anonymity would be highly unlikely to stop a determined terrorist or criminal of any kind, but it would certainly have a deeply chilling effect on political activity in places where speaking one's mind is dangerous and where certain kinds of unpopular speech could jeopardize someone's livelihood or perhaps life."[34] Notice that Mr. Gilmore's opinion seems to be that identification/authentication would be universal on all parts of the web and would track all data, all the time. To be effective, the identification/authentication needs only to apply to certain parts of the web, and only to certain bits of data.

---

[29] Moto, H. (2010). *Identity Theft Statistics- Reasons For Concern*. Retrieved July 1, 2010, from Articlesbase: http://www.articlesbase.com/finance-articles/identity-theft-statistics-reasons-for-concern-1915866.html

[30] Moto, H. (2010). *Identity Theft Statistics- Reasons For Concern*. Retrieved July 1, 2010, from Articlesbase: http://www.articlesbase.com/finance-articles/identity-theft-statistics-reasons-for-concern-1915866.html

[31] Moto, H. (2010). *Identity Theft Statistics- Reasons For Concern*. Retrieved July 1, 2010, from Articlesbase http://www.articlesbase.com/finance-articles/identity-theft-statistics-reasons-for-concern-1915866.html

[32] *DEMOCRACY, TERRORISM, AND THE INTERNET*. (2005, March 10). Retrieved July 1, 2010, from Safe-Democracy.org: http://english.safe-democracy.org/keynotes/democracy-terrorism-and-the-internet.html

[33] *DEMOCRACY, TERRORISM, AND THE INTERNET*. (2005, March 10). Retrieved July 1, 2010, from Safe-Democracy.org: http://english.safe-democracy.org/keynotes/democracy-terrorism-and-the-internet.html

[34] *DEMOCRACY, TERRORISM, AND THE INTERNET*. (2005, March 10). Retrieved July 1, 2010, from Safe-Democracy.org: http://english.safe-democracy.org/keynotes/democracy-terrorism-and-the-internet.html

Cyberspace Security and Attribution

General (Ret) Ron Keys, RK Solutions;
Charles Winstead, NSCI;
Kendra Simmons, NSCI Intern (ECPI)

July 20, 2010

Senators John Rockefeller (D-W.Va) and Olympia Snowe (R-Maine) introduced the Cybersecurity Act of 2009. This act gives the president the ability to "declare a cybersecurity emergency" and shut down or limit Internet traffic in any "critical" information network "in the interest of national security." The bill does not specifically define exactly what cybersecurity consists of nor does it define a critical information network. The president would have complete authority to determine these definitions. Nor does the pending Cybersecurity Act explicitly explain how the President might shut down or limit Internet traffic by fiat during an emergency.

The bill also gives the Secretary of Commerce access to all relevant data concerning critical networks without regard to any provisions of the law. In other words, the Secretary of Commerce can monitor or access any data on private or public networks without regard to privacy laws. Rockefeller states that "We must protect our critical infrastructure at all costs-from our water to our electricity, to banking, traffic lights and electronic health records." Snowe also agrees with Rockefeller and made a statement saying "if we fail to take swift action, we regrettably risk a cyber Katrina.[35]

Leslie Harris, head of the Center for Democracy and Technology (CDT) was an opponent of the bill. Harris believed that "such a drastic federal intervention in private communications technology and networks could harm both security and privacy." CDT senior counsel Greg Nojeim believes the bill will undermine the Electronic Communications Privacy Act (ECPA). The ECPA protects electronic communications in transit, sets requirements for search warrants, and protects messages stores on computers.[36]

Another opponent of the Cybersecurity Act of 2009, Jennifer Granick, Civil Liberties Director at the Electronic Frontier Foundation, says that allowing the Commerce secretary such power could potentially cause networks to be less safe. Granick believes that when one person can access all information on a network, it makes it more vulnerable to intruders. "You've basically established a path for the bad guy to skip down."[37] However, just as DoD has numerous programs that are "compartmented", if shown to be warranted, detailed information could be sequestered in several "cantonments", but the aggregated flow, and network up and down information could be centralized without much threat to individual liberties.

In May of 2010 Sen. Sheldon Whitehouse (D-RI) was interviewed by the Center for Strategic & International Studies (CSIS). In his interview he stated the intelligence community has to make sure that it is defending the U.S. against cyber attack the same way it would against any other type of attack. They must also use covert tools at its disposal.

He strongly believes that we should not compromise the technological capabilities and advantages that the NSA provides for our country, while at the same time we must make sure that "safeguards for privacy and civil liberties are not only adhered to but that there is a mechanism in place for making sure that they are adhered to." He also believes that "identification of problem areas that lead to civil liberties and privacy concerns are the key areas where we need to be focusing our time."[38]

---

[35] Aquino, S. (2009, April 2). *Should Obama Control the Internet?.* Retrieved July 1, 2010, from Mother Jones: http://motherjones.com/politics/2009/04/should-obama-control-internet

[36] Aquino, S. (2009, April 2). *Should Obama Control the Internet?.* Retrieved July 1, 2010, from Mother Jones: http://motherjones.com/politics/2009/04/should-obama-control-internet

[37] Aquino, S. (2009, April 2). *Should Obama Control the Internet?.* Retrieved July 1, 2010, from Mother Jones: http://motherjones.com/politics/2009/04/should-obama-control-internet

[38] Schwartz, H. (2010, May 3). *CSIS Interview: Cybersecurity with Sen. Whitehouse (D-RI).* Retrieved July 2, 2010, from CSIS: http://csis.org/press/press-release/csis-interview-cybersecurity-sen-whitehouse

Cyberspace Security and Attribution

General (Ret) Ron Keys, RK Solutions;
Charles Winstead, NSCI;
Kendra Simmons, NSCI Intern (ECPI)

July 20, 2010

In summary, any individual or group with access to the Internet can engage in cyber attacks and crimes. It can be hard to determine the good guys from the bad. Cyber attribution levels the playing field making everyone play by the same rules. Finding a balance between cyber attribution and protecting individuals' right to privacy can seem a daunting task. If it is the government's job to protect the security of citizens, should they compromise the safety of the nation in order to satisfy those who feel they are being violated? At the same time, should citizens compromise their privacy and individual rights in order to play fair on the internet? Also, how much privacy should they give up without feeling that the government is being too invasive?

How private is our private information? When applying for something as simple as a library card, you must show identification to verify your name and address. Without this verification, you may not be allowed to check out library books. Most people are willing to show their driver's license, social security card, military ID, and even automobile registration in order to check out items from the library. These documents contain sensitive information about an individual. In addition, millions of Americans shop online. Upon checking out, they are asked to disclose private information such as their billing address and credit card number. Few object to providing this information in order to receive their items.

Advocates of attribution make an argument that many people who are concerned about their privacy online willingly divulge sensitive information on a regular basis. In other words, what is the point of going through the trouble of putting up a privacy fence when you leave your mini blinds wide open? Are we really giving up our right to privacy or are we allowing the government to do their job of protecting our safety? Balancing cyber attribution and privacy concerns is one tough battle.

Ultimately, we reason that the government should protect citizens in cyberspace if citizens want this protection. In order to provide this security, the government will need those citizens to cooperate with their attribution techniques. The US Military provides this security to their members already. The DOD already operates a global long-haul IP based network to support unclassified IP data communication services. Created by Defense Information Systems Agency (DISA), this network is used to exchange sensitive information between "internal" users, who are either military personnel, civilian government employers, or military contractors. Access is provided by suitable logins to gateways from the public internet.[39] It would be plausible to offer a similar service to other citizens who are willing to provide some modicum of personal information required for attribution. We recommend a crawl, walk, run approach, starting with small numbers in some states or regions before offering this security nationwide. Some bi-lateral agreements with trusted nations can be a possibility in the future, but we believe it is a time tested, small scale approach that is the best starting point. Perhaps the Department of Homeland Security with expert help from US Cyber Command on technical issues could be tasked to take this on and begin to bring order to the panoply of emerging laws and technology. We think this would be a great starting place.

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.

[39] *NIPRNET*. (2010). Retrieved July 1, 2010, from Citizendium: http://en.citizendium.org/wiki/NIPRNET