THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

PROGRAM OF SCIENCE, TECHNOLOGY, AND SOCIETY

UNITED STATES CYBERSECURITY POLICY: AN ANALYSIS OF PROPOSED LEGISLATION OF THE 111TH CONGRESS AND A RECOMMENDATION FOR FURTHER LEGISLATIVE ACTION

JESSICA M. PELLICIOTTA
Spring 2011

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Political Science
with honors in Science, Technology, and Society

Reviewed and approved* by the following:

Darryl L. Farber
Assistant Professor of Science Technology and Society
Thesis Supervisor

Jesse F. Ballenger
Associate Professor of Science, Technology and Society
Honors Adviser

* Signatures are on file in the Schreyer Honors College

Abstract

The following thesis analyzes the current political environment and how it affects the opportunity to pass cybersecurity legislation. In order to do so, a brief timeline of cyber attacks is given to show that cybersecurity has come from a science fiction topic, to one of reality and great importance. Without the excuse of not understanding the threat, the study moves on to analyzing the cybersecurity bills proposed in the 111th Congress, the support, and the paths each bill took on the way to passage. Although not one piece of legislation was passed, this study can be used to learn lessons for the 112th Congress. This analysis leads to a set of recommendations. The first, that the Senate should pass a comprehensive bill. This bill should include general principles and goals that can guide future cybersecurity legislation. Further analysis supports the use of the membership in the Senate Homeland Security and Governmental Affairs Committee to power the legislation through the legislative process and garner support from both parties.

Identifying the mistakes or hurdles that the 111th Congress faced in legislating cybersecurity policy will validate the claim that cybersecurity is not unlike anything the United States has seen. It is to some degree more difficult to legislate because of the immense size and integration into everyday life; however, it is not changing the game itself. Cybersecurity is seeing the same struggles, to some degree, as other advances in technology and security threats they presented. This thesis will make comparisons to said advancements as it makes its analysis of cybersecurity legislation and recommendations to the 112th Congress.

Table of Contents

List of Figures

Acknowledgments

I would like to thank my thesis adviser, Dr. Darryl L. Farber; without his guidance I would not be in the Honors College, or writing this thesis.

I would like to also thank my mother and grandmother; without their love and support, I would not be at Pennsylvania State University. This thesis is dedicated to them, the people that believed in me before I did.

Introduction

Cybersecurity is far from being an unexplored, emerging threat. Thousands of articles have been written on the subject matter, while an equal amount of theories, policy suggestions, and assumptions float around the very same networks that people are trying to protect. In the Wild West that is the Internet, the United States shakily stands on rules and policies passed decades ago. While the international community moves ahead with agreements and objectives for securing safety from malicious activity online, the U.S. has failed to seen substantial action. President Clinton and President Bush began the cybersecurity conversation in the United States with different reports and executive directives ranging from defining critical infrastructure, to calling for different cyber positions. The Obama Administration has moved even further, appointing a head cyber position in the White House and defining the Internet as terrain the government must protect to ensure national security. This is juxtaposed with the inaction seen in the US Congress over the years.

The country still operates on laws passed in the 1980s.[1] While no one doubts that cyber threats challenge our national security (see countless examples of DDoS attacks on government websites, billions of dollars lost in cyber theft, cyber espionage, etc), no cybersecurity legislation has passed Congress. In 2009-2010, there were multiple drafts of bills sitting in committees, fewer passed committees, and zero managed to reach the President's desk. With individuals in the armed services, international community, private industry, and government are committed to solving the nation's cybersecurity issues, why did this happen? Possible explanations range from the political environment of the current Congress, to the complexity of the subject matter, to the

[1] *Reboot: Defining Paths to Cyber Policy, Law, and Technology Solutions*. San Francisco: U.S. Department of Energy by Lawrence Livermore National Laboratory and Georgetown University, March 25, 2010.

hesitation of regulating the Internet.

While all seem plausible explanations, and many jump to equate cybersecurity with other technological developments in history. Leading cybersecurity specialist, James A. Lewis, claims that individuals are hesitant to bring cybersecurity out of the control of the free market, and into the control of government, like many other technologies and innovations. He has used automobiles and airplanes as examples of the pattern of new technologies: technology is created→ problems rise from the technology→the free market is expected to encourage innovation and cure ills→government lags in policies and action to fix what the market cannot provide. Again, this seems a likely explanation, assuming Congress has not learned lessons from the past. It is important, however, to analyze the cybersecurity-related actions of Congress so far, and the qualities of the bills proposed to confirm Lewis' theory, as well as provide more specific recommendations for Congress.

The following study analyzes the cybersecurity policies proposed in the 111th Congress, the committees performing the work, the sponsors of the bills, political affiliation support and opposition, and the differences between the two houses. It then will provide a recommendation for the type of cybersecurity policy Congress needs to, and has the ability to, pass in the 112th Congress.

Brief History of Cyber Threats and Attacks

From individual perpetrators to organized foreign government attacks, cyber threats and attacks are by no means a new development. For each growth in networks and computers, there have been parties exploiting security weaknesses. This short timeline of selected events show cyber threats attacks on the U.S. Federal Government and international affairs over the years. This timeline's purpose is to discount the belief that Congress is waiting for a cyber attack to happen, before it has the ability to pass regulatory legislation.

1984: KGB Hires Hackers

It was known for several years that there were hackers present in international communication and US federal agency networks, however, in 1984 it was discovered that the KGB had hired young hackers for espionage purposes. According to an article in *The Computer Law and Security Report* (it was discovered that these hackers had been collecting passwords of high security networks, some belonging to The Pentagon and national labs. The article also reports, "The KGB asked the hackers for passwords to military and scientific computer systems, source-codes of named software products, information about chip construction, complier software, and data files about military and scientific project".[2]

1988: Robert Morris Worm

The first worm spread in 1988 with Robert Morris' self-replicating program that infected computers at, UC Berkley, UC San Diego, Lawrence Livermore, Stanford, and NASA Ames.[3]

---

[2] Wuermeling, U. "New Dimensions of Computer-Crime--Hacking for the KGB--A Report." *Computer Law & Security Report* 5.4 (1989): 20-21. *Google Scholar.* Web.

[3] Seeley, D. *A Tour of the Worm*. Department of Computer Science, University of Utah, 1988. *Google Scholar.* Web.

The same study summarizes the impact of the worm as,

> The Internet had never been attacked in this way before, although there had been plenty of speculation that an attack was in store. Most system administrators were unfamiliar with the concept of worms (as opposed to viruses, which are a major affliction of the PC world) and it took some time before they were able to establish what was going on and how to deal with it.

The case of the Morris Worm demonstrates one of the earliest examples of the lack of preparedness and emergency plan.

1998: Solar Sunrise

In the book, **Cyber Warfare and Cyber Terrorism** by Lech Janczewski, the author remarks on the surprising perpetrators of the major attack on government information system. "A group of teenage hackers, under the guidance of an eighteen-year-old mentor, gained access to numerous government computers including military bases. Solar Sunrise served as a warning that serious hacking capabilities were within the grasp of relative nonexperts"[4] After this incident, Congressional hearings and reports begin to comment on the unique nature of the security threats and the low-barrier to obtaining cyberattack capabilities. Demonstrates the difficulties of applying these new threats to standard US national security policy and foreign policy.

2000: DDOS Attacks on E-Commerce

In February of 2000, many e-commerce sites including Yahoo!, E*Trade, Amazon.com, and eBay are attacked by distributed denial of service attacks. Several federal responses ensued because of the scale of these attacks and high cost of the crime. One of these responses was Deputy Attorney General Eric Holder's statement to the Subcommittee on Crime of the House Committee on the Judiciary and the Subcommittee on Criminal Oversight of the Senate

[4] Janczewski, L, and A M Colarik. *Cyber Warfare and Cyber Terrorism*. N.p.: IGI Global, 2008. *Google Scholar.* Web.

Committee on the Judiciary. During the statement, he admitted to the scope of the situation. "Our vulnerability to this type of crime is astonishingly high - it was only this past December that a defendant admitted, when he pled guilty in federal and state court to creating and releasing the Melissa virus, that he caused over 80 million dollars in damage."[5] Holder also identifies the three difficulties to defending and prosecuting cybercrime. The categories of difficulties are identified as technical, legal, and resource challenges.

2007: Foreign Cyber Break-ins

As Laura L. Knapp, MAJ, USA summarized in her research report for Air Command and Staff College, Air University, "2007 witnessed a remarkable upswing in target sets, volume, and sophistication of Chinese cyber activity against military, economic, informational, and diplomatic targets." Government networks belonging to agencies like the Department of Defense and Department of State were hacked. Foreign hackers were able to gain access to classified information, as well as, administer DOS attacks, shutting down government websites. Some experts believe that terabytes of information were copied or stolen. These actions continued throughout 2007, and marked an increase in foreign attacks as well as a shift in public opinion. Suddenly, many more people were concerned with our nation's cybersecurity.

2007: Cyber Attacks on Estonia

When many hear the term cyberwar, they recall the Russia-Georgia conflict, however, that it not the first instance of cyberconflict. A year earlier, Russia used cyber attacks against Estonia. As *The Economist* depicted the event, "It was established in response to what has become known as "Web War 1", a concerted denial-of-service attack on Estonian government,

[5] "Internet Denial of Service Attacks and the Federal Response." Statement of Eric Holder Deputy Attorney General of The United States Before the Subcommittee on Crime of the House Committee on the Judiciary and the Subcommittee on Criminal Oversight of the Senate Committee on the Judiciary. February 29, 2000.

media and bank web servers that was precipitated by the decision to move a Soviet-era war memorial in central Tallinn in 2007."[6] This event, along with the conflict in Georgia that seemed more organized with military effort, sparked military and international affairs conversations. How would cybersecurity fit into the current constructs of international engagement, and how does a country deter cyberattacks?

2008: Poisoned Thumb Drive

Known by many as the most significant cyberattack on U.S. Military forces, a virus spread by an affected USB thumb drive was responsible for leaks in military intelligence in 2008 and prompted change in military policy. As the article, *Defending a New Domain*, in which *Foreign Policy* summarizes,

> It began when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control. It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary (Lynn 2010).[7]

The malicious code, known know as agent.btz, was addressed through Operation Buckshot Yankee. The weaknesses identified during the Operation encouraged the Air Force to develop Cyber Command. As stated in the *Department of Defense Fiscal Year (FY) 2011 IT President's Budget Request*,

> The [Air Force] Network Action Plan is designed to reinvigorate operational rigor and address lingering systemic issues in the AF Global Information Grid

---

[6] "Cyberwar: War in the Fifth Domain." *The Economist*. 1 July 2010. Web. 2 Nov. 2010.

[7] Lynn III., William J. "Defending a New Domain." Foreign Affairs (2010). Foreign Affairs. Sept.-Oct. 2010. Web. 05 Nov. 2010. <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>.

> highlighted by the Operation Buckshot Yankee. Our long-term goal is to enhance the Air Force portion of the Global Information Grid (GIG) to one that is global and integrated across all AF domains – air, space and cyberspace. Our continued priority is to modernize and develop the proper safeguards to secure our data, both in a joint and coalition environment.[8]

The Air Force Cyber Command was established to, "redefine Airpower…extend our global reach and power into cyberspace…Primary Mission is Warfighting: Integrate AF's global kinetic and nonkinetic strike capability…through the full range of military operations.[9] The 24th Air Force was activated as the cyber numbered air force (NAF) within Air Force Space Command (AFSPC). According to a publication by the RAND Corporation, "it consists of an operational center and three subordinate wings: the 67th Netword Wing, 688th Information Operations Wing; and 689th Combat Communications Wing".[10]

2010: Stuxnet

As one of the most recent cyberattacks, the Stuxnet worm brought what many politicians and technological experts alike had feared, attacks on critical infrastructure. The majority of the systems targeted by the malicious code were found in Iran. Among these Iranian facilities were different critical infrastructure systems, including the Bushehr light-water reactor controls.[11] Once infected, Stuxnet sabotaged the system controls of the facilities by reprogramming software. With the complexity of the worm, and targeted system, many believe that this attack

---

[8] Department of Defense Fiscal Year (FY) 2011 IT President's Budget Request**.** March, 2010.

[9] Robert Elder, "Air Force Cyberspace Command: Defense Technology Forum," briefing, 8th Air Force, June 14, 2007.

[10] Mesic, Richard, Myron Hura, Martin C. Libicki, Anthony M. Packard, and Lynn M. Scott. *Air Force Cyber Command (Provisional) Decision Support*. RAND Corporation, 2010.

[11] Maclean, William. "Cyber attack appears to target Iran-tech firms." *Reuters,* 24 September 2010.

was state backed. Regardless of the culprits, this attack has numerous consequences. Stuxnet demonstrated that critical infrastructures were in fact vulnerable to damage form cyber attacks, that privately owned weaknesses in national security present a challenge to countries like the United States, and that cyber attacks can affect multiple nations at once, requiring international cooperation.[12]

[12] Porteous, Holly. "The Stuxnet Worm: Just Another Computer Attack of a Game Changer?" *International Affairs, Trade and Finance Division, Parliamentary Information and Research Service*. 7 October 2010.

Cybersecurity Legislation of the 111th Congress

Over the past two years, there have been numerous bills proposed in the House and Senate. However, few make it beyond their committee assignments. The following is a brief summary of the proposed legislation that related to cybersecurity in the 111th Congress.

The House of Representatives

H.R. 266 Cybersecurity Education Enhancement Act of 2009 is sponsored by Democratic Representative Shelia Jackson-Lee (TX-18) and currently sits in the House Education and Labor Committee and was referred to the Subcommittee on Higher Education, Lifelong Learning, and Competitiveness. As the bill's introduction states, its purpose is, "To authorize the Secretary of Homeland Security to establish a program to award grants to institutions of higher education for the establishment or expansion of cybersecurity professional development programs, and for other purposes." This bill attempts to address the need for more cybersecurity professionals; however, similar program proposals are included in several other bills that are more comprehensive. H.R. 266 was referred to committee on March 16th, 2009, and will most likely see no further action because of the time spent inactive.

According to US-CERT, peer to peer (P2P) software allows for users to share files, but makes users vulnerable to computer attacks and loss of the confidentiality, authenticity, and controlled accessibility of personal information[13]. *H.R. 1319 Informed P2P User Act* aims to force P2P software makers to "provide clear and conspicuous notice that such program allows files on the protected computer to be made available for searching and copying by another

[13] McDowell, Mindi, Brent Wrisley, and Will Dormann. "US-CERT Cyber Security Tip ST05-007 -- Risks of File-Sharing Technology." *US-CERT: United States Computer Emergency Readiness Team*. 19 May 2010. Web. 08 Sept. 2010.

computer; and (B) obtaining by and copying to one or more other computers" and "provides clear and conspicuous notice of which files on the protected computer are to be made available for searching by and copying to another computer; and obtains the informed consent from an owner or authorized user of the protected computer for such files to be made available for searching and copying to another computer." This bill, as passed through the House and referred to the Senate Committee on Commerce, Science, and Transportation Committee in December 2009, addresses one small piece of the risk. Another drawback is that many P2P makers offer this disclosure already, calling into question the impact this bill would make.

H.R. 2020 Networking and Information Technology Research and Development Act of 2009 renames the National High-Performance Computing Program as the Networking and Information Technology Research and Development Program by amending the High-Performance Computing Act of 1991. Section 104 (a) reads, "Program shall encourage agencies identified in section 101(a)(3)(B) to support large-scale, long-term, interdisciplinary research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits." This bill aimed at strengthening the research and development of IT research includes interdisciplinary focus, which is a step in the right direction. H.R. 2020 was passed in the House, and on May 13th was referred to the Senate Committee on Commerce, Science, and Transportation. Research and development has been included in other cybersecurity pieces of legislation, without the specific recommendation of amending the High-Performance Computing Act of 1991.

The United States' power systems are probably subject to a majority of the security threat concerns. *H.R. 2165 Bulk Power System Protection Act of 2009* seeks to create a commission

that will be charged with creating a metric system for measuring cybersecurity risks. The Federal Energy Regulatory Commission would follow recommendations from the “vulnerabilities identified in the June 2007 communication to certain "Electricity Sector Owners and Operators" from the North American Electric Reliability Corporation” and gives FERC the power to, “issue orders for emergency protective measures if the President provides FERC with a determination that an imminent cybersecurity threat to the system exists”. This bill was introduced in April of 2009, and has been basically replaced by H.R. 5026 Grid Reliability and Infrastructure Defense Act.

H.R. 2195 To amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack, and for other purposes would amend the Federal Power Act to charge the Secretary of Homeland Security to evaluate the security of federally owned infrastructure affecting our electric infrastructure. This bill would also charge FERC to create mandatory measures until the Secretary makes his recommendations. This bill is also very similar to S. 946 Critical Electric Infrastructure Protection Act of 2009 and H.R. 5026, which has passed the House.

H.R. 4061 Cybersecurity Enhancement Act of 2010 passed the House in February of 2010 and was referred to the Committee on Commerce, Science, and Transportation in the Senate. Similar to *H.R. 2020 Networking and Information Technology Research and Development Act of 2009,* H.R. 4061 aims to direct research and development in cybersecurity. Going into more detail and delegation among federal agencies, H.R. 4061 charges the National High-Performance Computing Program with cybersecurity strategy research and the National Science Foundation to give grants in related areas. The Cybersecurity Enhancement Act also dictates the stipulations for the creation of Computer and Network Security Research Centers, charges the NSF Director to

create a Scholarship for service program in the federal, requires the President to conduct a report on the federal cybersecurity workforce, orders the Office of Science and Technology Policy Director to create a cybersecurity committee made up of university and industry personnel, and requires NIST, OSTP, and NSF leaders to conduct several targets and reports relating to improving cybersecurity personnel and research focus. Although there are more comprehensive bills, if the Senate cannot pass a compiled cybersecurity bill, this specialized bill could make it out of committee and through the Senate.

After being passed in the House on March 24th, 2010 *H.R. 4098 Secure Federal File Sharing Act* was referred to the Senate Committee on Homeland Security and Governmental Affairs. The main tenets of H.R. 4098 would prohibit federal employees and employees of contracting companies from downloading any peer-to-peer file sharing software on federal computers and home computers. The Director of the Office of Management and Budget would oversee this requirement. After over a year in committee, *Secure Federal File Sharing Act* waits along with many other bills in the Senate.

H.R. 4507 Cyber Security Domestic Preparedness Act is a brief piece of legislation currently referred to the House Homeland Security Committee that "Amends the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security (DHS) to establish the Cyber Security Domestic Preparedness Consortium". The role of the Consortium would be to train emergency personnel, create a training program for such people, and establish a Cyber Security Training Center for these educational purposes. Congressman Rodriguez (D-TX) introduced this bill in January of 2010.

H.R. 4900 Federal Information Security Amendments Act of 2010 aims to create a framework for information security. The overarching component of this act would create a

National Office of Cyberspace and a Federal Cybersecurity Board within the National Office of Cyberspace that is made up of at least one person from: the Office of Management and Budget, civilian agencies, the Department of Defense, law enforcement community, and such additional military and civilian agencies as the Director considers appropriate. This agency would be required to oversee all federal information security by setting policies establishing security requirements and monitoring information protection. The main tenets of this bill were included in *H.R. 5136 National Defense Authorization Act for Fiscal Year 2011* under Subchapter II of Title XVII—Federal Information Security. *H.R. 5136* passed the House and has been put on the Senate schedule.

H.R. 4962 International Cybercrime Reporting and Cooperation Act directs different federal agencies and the President tasks in order to promote international cooperation in cybercrime. The President would be required to give an annual report on the status of international cybercrime reporting, including but not limited to, summarizing the United States' and each member of the United Nations' efforts of international cooperation in cybercrime and its state of information and communications technology and security, identifying countries with a low level of information and communications technology in critical infrastructure, and assessing international efforts to combat cybercrime. Those countries identified as having low cybersecurity will each have an action plan developed for them, detailing how the United States is working with said government to improve the country's security and create measurable benchmarks. If said country does not meet benchmarks, the bill outlines several actions including, the suspension, restriction or prohibition of new financing and financial assistance in other trade programs. This bill also delegates the Secretary of State to select a high-level employee of the Department of State, "to coordinate the full range of activities, policies, and

opportunities associated with combating cybercrime and foreign policy." *H.S. 4962* was introduced to the House Financial Services, Ways and Means, and Foreign Affairs committee on March 25th.

Similar to *H.R. 2165 Bulk Power System Protection Act of 2009*, *H.R. 5026 Grid Reliability and Infrastructure Defense Act* uses the Federal Energy Regulatory Committee to protect our critical infrastructure. This bill however, does not have them make mandatory measures until the Secretary of Energy makes recommendations, but authorizes FERC the power to, "with or without notice, hearing, or report, to issue orders for emergency measures to protect the reliability of either the bulk-power system or the defense critical electric infrastructure whenever the President issues a written directive or determination identifying an imminent grid security threat." This bill, which would amend the Federal Power Act, was passed in the House on June 9th and was placed on the Senate Legislative Calendar on September 27th.

H.R. 5247 Executive Cyberspace Authorities Act of 2010 calls for the establishment of a National Cyberspace Office, whose director would serve on the National Security Council. This bill has also been included in *H.R. 5136 National Defense Authorization Act for Fiscal Year 2011* similar to *H.R. 4900 Federal Information Security Amendments Act of 2010.*

H.R. 5548 Protecting Cyberspace as a National Asset Act of 2010 proposes amendments to the Homeland Security Act of 2002. The first section of the bill establishes the Office of Cyberspace Policy, which would create goals, as well as, oversee and coordinate federal cybersecurity efforts in diplomatic, economic, military, intelligence, homeland security, and law enforcement policies and activities within and among Federal agencies. Secondly, it creates a National Center for Cybersecurity and Communications within the Department of Homeland Security. The NCCC would work with the private sector, Assistant Secretary for Infrastructure

Protection, and oversee the Office of Emergency Communications, the National Communications System, and the United State Emergency Readiness Team (US-CERT). The Director of NCCC would be required to create a program for information sharing between federal agencies, evaluate cyber vulnerabilities, establish a way to engage with the private sector, and research guidelines to ensure privacy and civil liberties. In June 2010 *H.R. 5548* was referred to the Committee on Oversight and Government Reform, Homeland Security, Armed Services, the Judiciary, and Education and Labor. *S.3480* is the corresponding bill in the Senate.

US Senate

S. 773 Cybersecurity Act of 2009 has received a good deal of media attention for its call to give the President power to declare a cyber emergency and shut down the Internet to federal networks and those relating to the critical infrastructure of the nation. However, there is much more specified in this comprehensive legislation referred to the Committee on Commerce, Science, and Technology as introduced by Senator Rockefeller. It would order the President to create a Cybersecurity Advisory Panel, the Department of Commerce to create a system to measure cybersecurity status, financial assistance given to Regional Cybersecurity Centers for small and medium sized businesses, and directs the President to create a national cybersecurity strategy and work with foreign nations on creating international organizations, joint acts, and standards for the improvement on cybersecurity.

S. 778 A bill to establish, within the Executive Office of the President, the Office of National Cybersecurity Advisor acts as a complementary piece of legislation to *S. 773*. If passed, the bill would crease the Office of National Cybersecurity Advisor, who would be the principle adviser to the President in all cybersecurity matters. He or she would also look over all budget

requests relating to cybersecurity to the Office of Management and Budget.

S. 921 United States Information and Communications Enhancement Act of 2009 if adopted, would create the National Office for Cyberspace to, "serve as the principal office for coordinating an assured, reliable, secure, and survivable global information and communications infrastructure and related capabilities." The office would be required to create and oversee information security policy and agencies' information security protections. Each federal agency would have to submit an evaluation of information security and work with US-CERT to achieve recommendations set by the Secretary of Commerce as approved by the President. S. 921 was referred to the Committee on Homeland Security and Governmental Affairs in April 2009. Its goal of regulating federal agencies' information security practices is similar to *H.R. 4900*.

S. 946 Critical Electric Infrastructure Protection Act of 2009 is the Senate version of *H.R. 2195* which charges the Department of Homeland Security with analyzing the security of electronic devices and communication networks essential to our critical electric infrastructure. It also directs the Federal Energy Regulatory Commission to create temporary mandatory measures to ensure the security of the United States' critical infrastructure. The bill has been referred to Senate Homeland Security and Governmental Affairs.

Senator Olympia Snowe introduced *S. 1070 A bill to establish the Small Business Information Security Task Force to address information security concerns relating to credit card data and other proprietary information* to the Senate Small Business and Entrepreneurship Committee in May 2009. This bill would charge the Small Business Administration Information Security Task Force with creating recommendations and a website to handle the information security of small businesses, with emphasis on the prevention of credit card data loss.

S. 1438 Fostering a Global Response to Cyber Attacks Act focuses on demonstrating the

United States' commitment to working with other nations to achieve cybersecurity. Charges the Secretary of State with working with other governments to develop common norms and terms, shared cybersecurity efforts, and creating "safeguards for the protection of privacy, freedom of speech, and commercial transactions for inclusion in cybersecurity agreements." Senator Gillibrand's bill was introduced to the Senate Committee on Foreign Relations on July 10th, 2009.

On March 23rd, 2010 Senator Gillibrand introduced another bill to the Committee on Foreign Relations**,** *S. 3155 International Cybercrime Reporting and Cooperation Act* that is the Senate version of *H.R. 4962.*

S. 3193 International Cyberspace and Cybersecurity Coordination Act of 2010 establishes a Coordinator for Cyberspace and Cybersecurity under the Secretary of State. This coordinator would be responsible for coordinating with other federal agencies to develop cybersecurity plans that span across departments, would be the senior position for cyberspace and cybersecurity issues, and would develop international policy stances and multilateral cooperation to ensure the security of cyberspace. The bill also includes the establishment of Country and regional cyberspace and cybersecurity policy coordinators. This would be accomplished by the Secretary of State appointing "an employee to have primary responsibility for matters relating to cyberspace and cybersecurity policy in each country or region that the Secretary considers significant with respect to efforts of the United States Government to combat cybersecurity globally." Senator Kerry introduced this bill to the Committee on Foreign Relations on May 25th, 2010.

S. 3480 Protecting Cyberspace as a National Asset Act of 2010 is arguably the most comprehensive cybersecurity bill in the Senate to accompany *H.R. 5548*, and is a competitor of

S. 3538, the other major comprehensive bill on cybersecurity. It currently sits in the Committee on Homeland Security and Governmental Affairs after its introduction in June 2010.

S. 3538 National Cyber Infrastructure Protection Act of 2010 aims to be the competitor of *S. 3480* while giving less power to the President, by creating a center which will be more responsible to the Congress. The bill does this by establishing The National Cyber Center, outside of the Executive Office of the President. The Director will have similar responsibilities to the Director of the Office of Cyberspace Policy as proposed in H.R. 5548/S.3480, without creating a body in DHS such as the proposed National Center for Cybersecurity and Communications within the Department of Homeland Security. Instead of the NCCC, *S.3538* would establish a Cyber Defense Alliance housed in a National Laboratory that would be "a public and private partnership for sharing cyber threat information and exchanging technical assistance, advice, and support". The Secretaries of Energy, Defense, Homeland Security, as well as the Directors of the National Cyber Center, National Intelligence, and the Federal Bureau of Investigation will collaborate to establish the Cyber Defense Alliance.

Update on Legislation Introduced in the 112th Congress

Since the first draft of this thesis the 111th Congress ended, and the 112th was underway. At the end of a session, all proposed bills that fail to pass Congress die, or fail at becoming law. As of the beginning of March, there have been five pieces of legislation introduced that deal with cybersecurity. The following bills were some of the first introduced, which leads one to believe each chamber has a renewed commitment to cybersecurity.

U.S. House

The first bill introduced in the House was *H.R. 76 Cybersecurity Education Enhancement Act of 2011.* Democratic Representative Shelia Jackson-Lee from Texas introduced this bill that focuses primarily on cybersecurity education on February 25th, 2011. The bill aims to improve education by authorizing the Secretary of Homeland security to establish a grant program in coordination with the National Science Foundation. The Secretary will create the goals of the grant program, work to expand associate degree programs in cybersecurity, and purchase equipment to supplement both degree and non-degree cybersecurity programs. *H.R. 76* also creates the "E-Security Fellow Program" which would bring together "State, local, tribal, and private sector officials to participate in the work of the National Cybersecurity Division in order to become familiar with the Department's state cybersecurity missions and capabilities."

On January 5th, 2011 *H.R. 174 Homeland Security Cyber and Physical Infrastructure Protection Act of 2011* was referred to the Committee on Homeland Security. Representative Thompson's bill is similar to *H.R. 5548* in that it would create a department within the Department of Homeland Security in charge of reviewing, coordinating, and implementing a common cybersecurity policy throughout the federal computer systems. The proposed Office of Cybersecurity and Communications would include United States Computer Emergency Readiness Team (US-Cert), and a Cybersecurity Compliance Division. Also included in the office would be relevant positions and programs under the Department of Homeland Security to enforce cybersecurity requirements to private industry. The Office would handle all reported cybersecurity incidents, conduct security reviews, and implement strategies for improving cybersecurity.

U.S. Senate

Typically, the first bills introduced at the beginning of a session are reserved for the majority leader and provide insight to his or her agenda for the upcoming session. The eighth bill introduced by Senator Reid in the 112th Congress was *S.8 Tough and Smart National Security Act.* This bill lays out five key priorities for the United States in order to improve national security. Among combating terrorism, to confronting nuclear threats from Iran and North Korea, one section is devoted to cybersecurity. The fifth goal of U.S. to improve national security is "reform cybersecurity policy to prevent cyber attacks on the United States Government and critical infrastructure, protect privacy and civil liberties, and implement mechanisms necessary to avert and respond to catastrophic cyber incidents." If passed, it will serve as a guiding policy for subsequently introduced national security bills, and show the United States' priorities to other nations.

Also introduced by Senate Majority Leader Reed is *S.21 Cyber Security and American Cyber Competitiveness Act of 2011*. This bill seeks to improve cybersecurity by: increasing jobs in the information technology industry; increasing research and investment into cybersecurity; providing incentives for the private sector to report cyber incidents and improve their safety; improving federal detection, reporting, and response to cybersecurity attacks against the government and military; preventing and prosecuting identity theft incidents; protecting critical infrastructure; improving the ability to prosecuting cyber crimes "in a manner that respects privacy rights and civil liberties"; and protecting the online privacy of American citizens. While ***S. 21*** clearly lays out the areas of cybersecurity that need improvement, it does not specify how these objectives will be achieved or who will be charged with completing these goals. Its main purpose seems to be soliciting further legislation that lines up with these cybersecurity priorities.

S. 372 Cybersecurity and Internet Safety Standards Act was introduced on February 16th, 2011 and focuses on securing computer networks and critical infrastructure in both the public and private sectors. This bill, introduced by Democratic Senator Cardin, currently sits in the Committee on Commerce, Science, and Transportation. If enacted, the Secretary of Homeland Security would be required to create a cost-benefit analysis of the federal government creating and enforcing cybersecurity standards on both public and private entities. Certain factors the Secretary must consider are effects on homeland security, global economy, individual liberty and privacy, and legal restrictions that would hinder cybersecurity standards. A report of the analysis would be due no later than one year after the Act was enacted.

Policy Proposal

Nature of the Situation

For years, cybersecurity has been studied, discussed, and promoted as a national security issue. Governmental officials and Congressmen finally understood the gravity of the threat and were starting to act. While those individuals interested in cybersecurity saw all the pieces come together for an opportunity to pass cybersecurity legislation, they were seriously disappointed to see none pass Congress. James A. Lewis articulated the feeling of frustration felt around the world.

> 2010 should have been the year of cybersecurity. It began with a major penetration of Google and other Fortune 500 companies, saw the Department of Defense describe how its classified networks had been compromised, watched the Stuxnet worm cut through industrial control systems, and ended with annoying denial of service attacks over Wikileaks. These public incidents were accompanied by many other exploits against government agencies, companies, and consumers. They show how the United States is reliant on, but cannot secure, the networks of digital devices that make up cyberspace.[14]

There are several theories to explain the difficulty in passing legislation, but an important question exists throughout all discussions: what makes cybersecurity different as a policy topic. The sheer size of the issue is unprecedented. The Internet has becomes ingrained in everyday life, critical infrastructure, government workings, the global economy. Not only does the issue affect almost all aspects of government, business, and security, but it also brings up issues of individual privacy and civil liberties. Another characteristic that makes it difficult to pass related legislation is that cybersecurity's nature leads to confusion over who is responsible for it. Beyond the question of federal involvement in general, the current situation presents an

entanglement of Department of Defense, Department of Homeland Security, Department of State, and other department oversight. This confusion is mirrored in the multiple committees in Congress that are assigned cybersecurity bills.

This confusion in responsibility and the magnitude of the issue's size contributed to the 111th Congress not passing a single piece of cybersecurity legislation. Five bills have already been introduced in the 112th Congress; the commitment to the problem is there. Analysis must be done on the subject, as well as the actions of the 111th Congress, in order to make recommendations to see cybersecurity policy be passed this Congress.

---

[14] Lewis, James A. *Cybersecurity Two Years Later*. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. January, 2011. Web.

Policy Options

One of the first decisions made of the policy proposal is to issue an overall recommendation for both the House and the Senate, or to focus on a specific chamber. The second set of characteristics to consider is recommending a general method for passing legislation, suggest specific policies to introduce or a group of policies for one comprehensive bill, or a combination. If a method for passage is recommended, one must consider what committees should be assigned the legislation. Another important thing to consider is if it is more beneficial to select one committee or assign multiple simultaneously. Party affiliation adds yet another dynamic to the policy options. Party support and opposition to certain subtopics of cybersecurity, bipartisan efforts, and political environment must be taken into account. A recommendation, depending if it is focused on the House, Senate, or both, can suggest a certain party carry the bill, or focus on legislation that can gather bipartisan support. Certain Congressman of importance can also be approached to take on the issue instead of affiliating it with a particular party. The final consideration when deciding the policy options is whether cybersecurity policy should be presented as a unique issue, or argued as subtopic for economic or national security policy.

Policy Analysis

In order to make a sound proposal for the 112th Congress, an analysis of the cybersecurity legislation that was introduced in the 111th is vital. The following analysis and figures were collected by analyzing the 23 bills introduced in the House and Senate in the 111th Congress. The first analysis is to address the policy options of providing a recommendation for one or both chambers of Congress. The question to answer is whether they preformed differently in regards to cybersecurity policy.

The first clue to answering this is simple; the House was able to introduce thirteen bills, pass six out of committee, and pass five to the Senate. In comparison, the Senate introduced ten bills, passed two out of committee, and zero to the House.

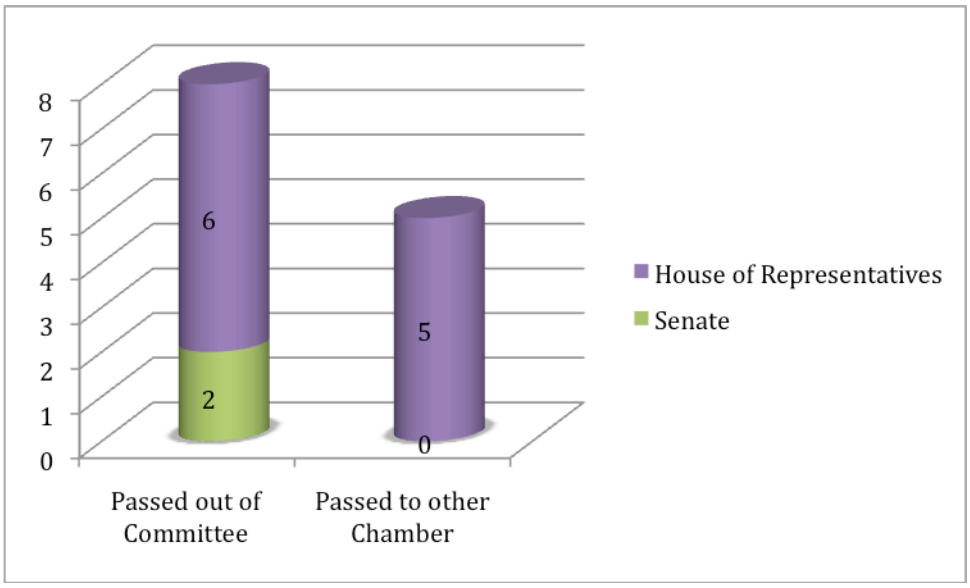

Figure 1 Cybersecurity Policy Passage Breakdown between House of Representatives and Senate in the 111th Congress

The first quality of the proposed legislation to look at is whether the bills were comprehensive, or addressing more than two different subtopics of cybersecurity, or non-comprehensive, focusing on one or two cybersecurity issues.

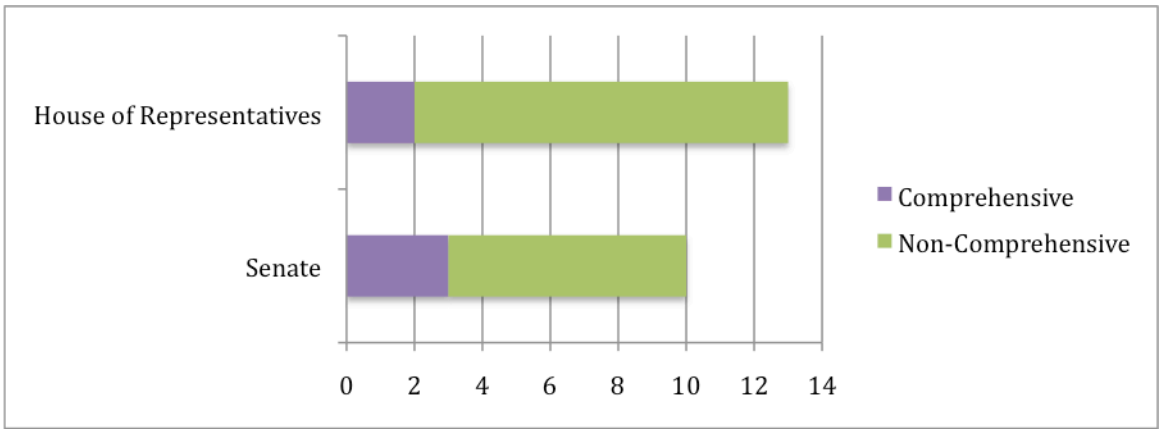

Figure 2 Comprehensive and Non-comprehensive breakdowns in Cybersecurity Legislation in the 111th Congress

As seen in Figure 2, a majority of the legislation introduced was not comprehensive, in neither the House nor Senate. It is important to further break this down and look into the makeup of the bills that advanced.

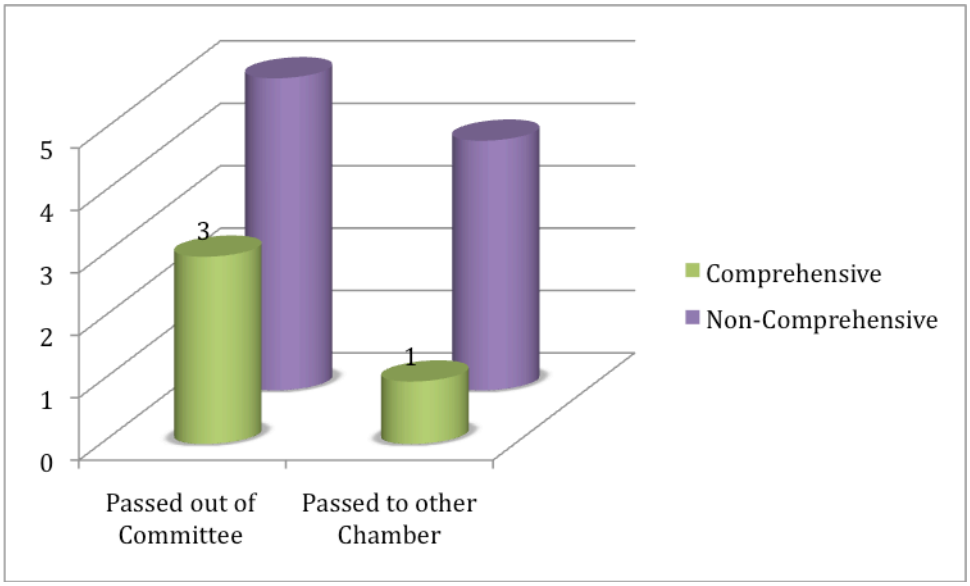

Figure 3 Cybersecurity Policy Passage breakdown between Comprehensive and Non-Comprehensive

This further supports that non-comprehensive bills have a higher success rate of both passing out of committee and then to the other chamber. The next step of analysis is to determine if there are any other correlations in topics between legislation that were introduced. The first characteristic

to test is the specific topics of all the legislation introduced.

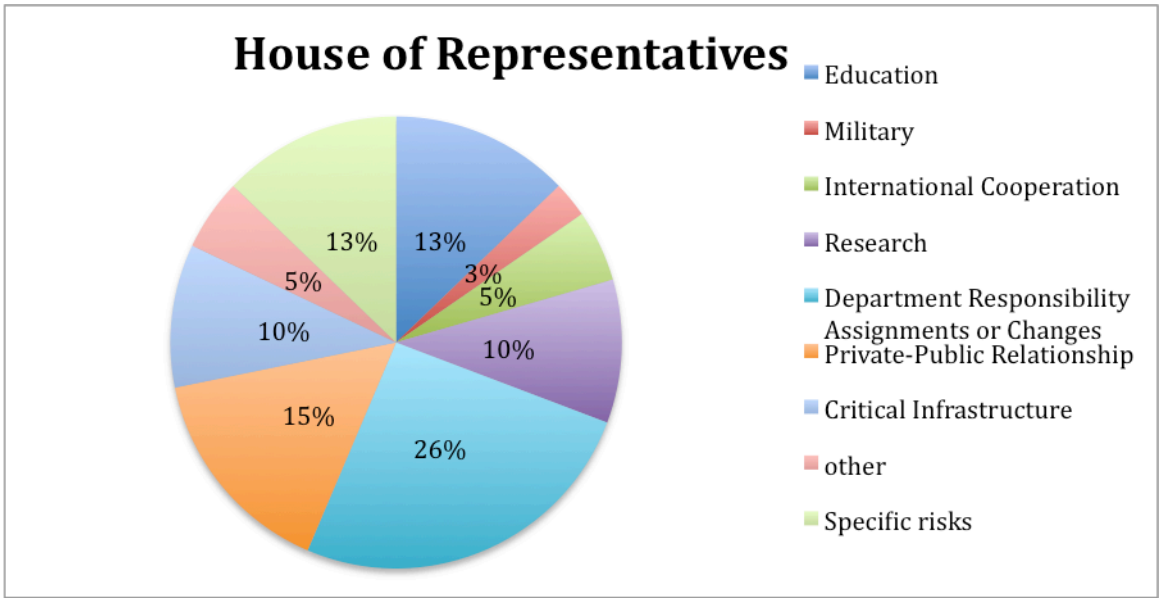

Figure 4 Proposed Legislation Topics: United States House of Representatives

The most common subtopic in all legislation introduced in the House (both comprehensive and non-comprehensive, as well as successful and unsuccessful) is department responsibility assignments and changes, followed by public-private relationship. Of those that passed in the House, the topics were department responsibility changes and assignments, followed by specific risks. These included regulation on peer-to-peer software and file sharing.

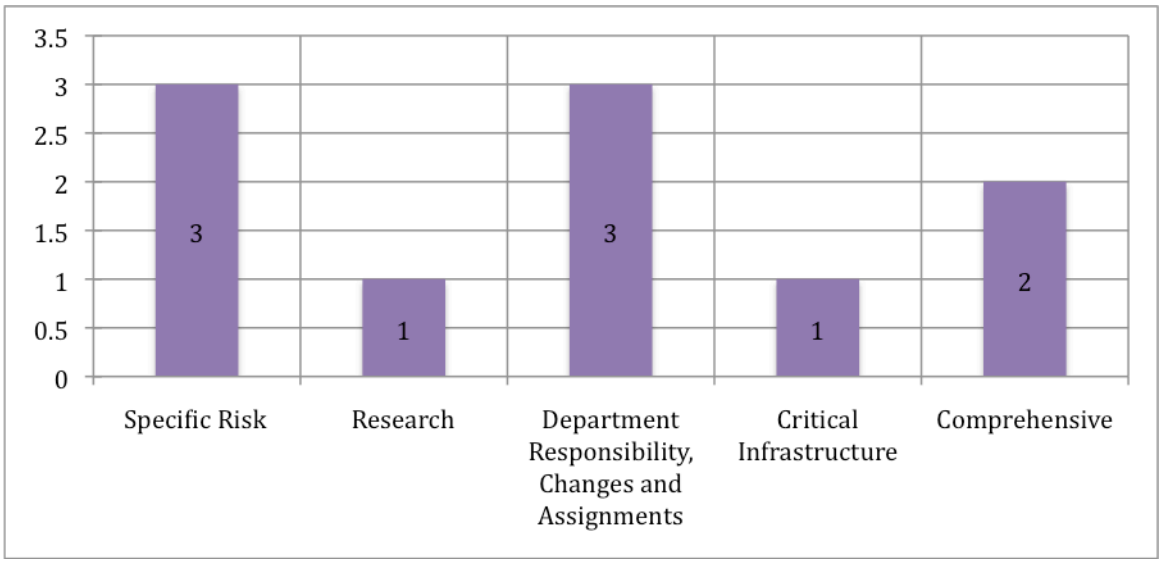

Figure 5 Passed Legislation Topics: House of Representatives

In the Senate, the most prominent type of topic is the same, but differ beyond that. The most common topic is department responsibility changes and assignments. This does not necessarily mean that the House and Senate introduced similar legislation. Because of the lack of department responsibility assignment that exists currently, almost every piece of legislation needs to include the topic of assigning or changing responsibility. It is important to note that public-private relationship, international cooperation, and research were also common topics in cybersecurity legislation. The biggest change evident by this breakdown is that international cooperation seems to be a priority for the Senate, but not the House.

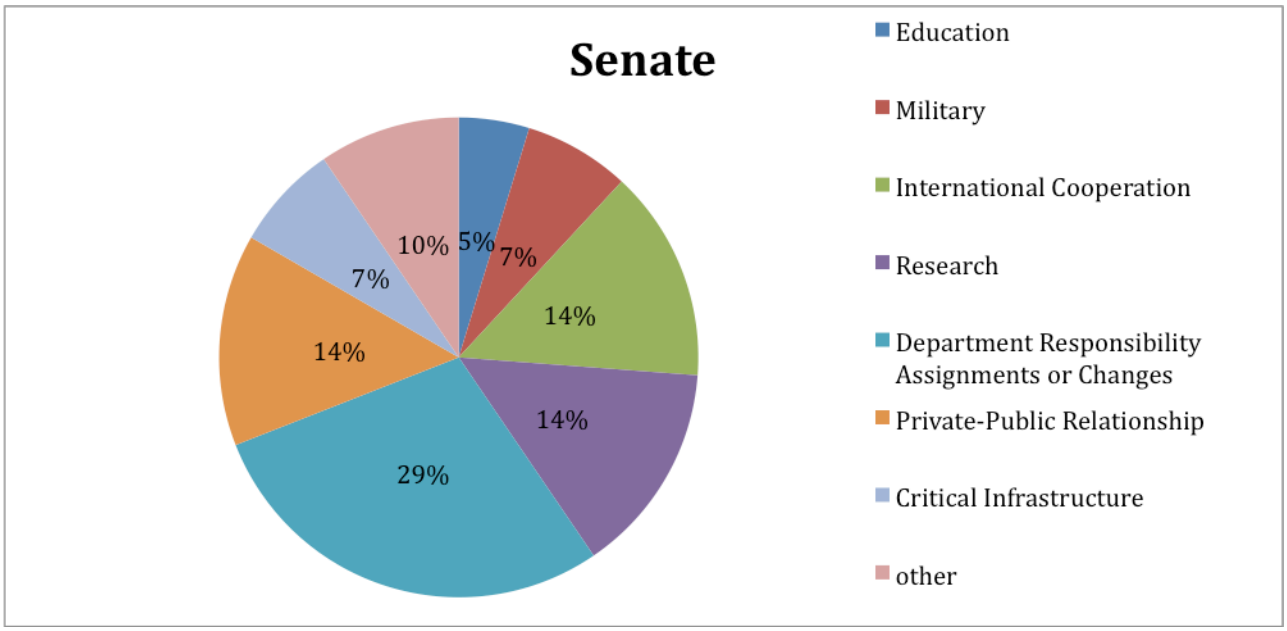

Figure 6 Proposed Legislation Topics: Senate

The next topic of analysis is committee origin. This could show if a particular committee is more able than others to pass cybersecurity legislation, and if it is more strategic to place bills in multiple committees or just one. For the House, there were eleven committees that were assigned cybersecurity legislation. Of those, only four passed legislation out of committee: Committee on Oversight and Government Reform, Science and Technology, Homeland Security and Governmental Affairs, and Energy and Commerce. It is important to note that many bills were assigned to more than one committee, and just because the bill "died" in one committee, it does not mean it died all together.

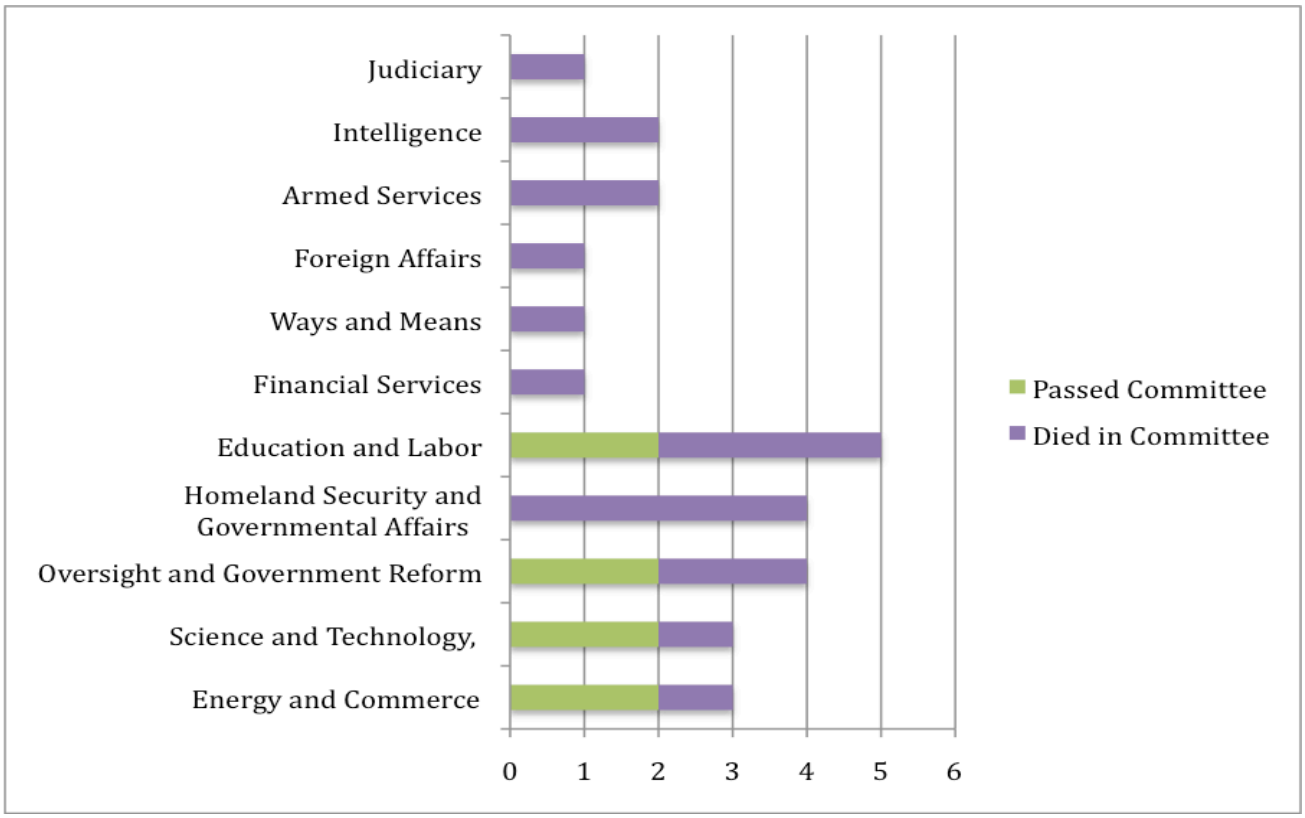

Figure 7 House of Representatives Committee Passage Successes

Of the five pieces of legislation that passed the House and was given to the Senate, two were committed in the Science and Technology Committee, two in the Energy and Commerce Committee, and two in the Oversight and Government Reform Committee. The Energy and Commerce Committee reported out *H.R. 1319* and *H.R. 5026*, the Science and Technology reported out *H.R. 2020* and *H.R. 4061*, the Oversight and Government Reform Committee reported out *H.R. 4098*.

The Senate only had two committees pass any legislation to the Senate floor. The Committee on Homeland Security and Government Affairs passed *S. 3480* and the Committee on Commerce, Science, and Transportation passed *S.773*.

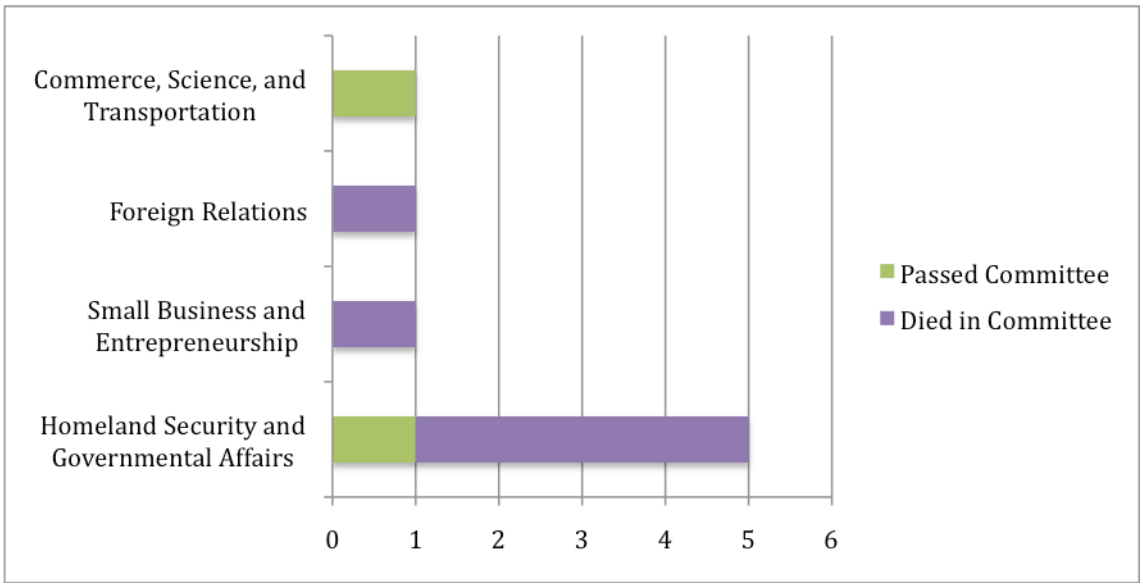

Figure 8 Senate Committee Passage Successes

The next type of analysis relates to party affiliation of sponsors, and cosponsors. In the House, Democrats sponsored a large majority of bills, while a Republican sponsored only one piece of legislation. That piece, a specific issue bill, was eventually passed by the House, in addition to four Democrat-sponsored bills

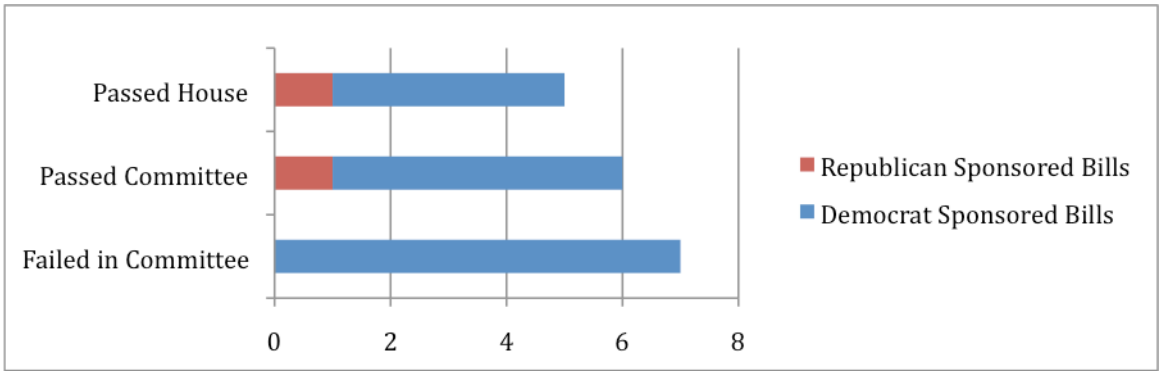

Figure 9 Sponsor Affiliations and Legislation Passage: House of Representatives

In the Senate, Republicans sponsored two bills and Democrats sponsored six. Independent Senator Joseph Lieberman sponsored one as well. Of the two bills that passed committee, one was sponsored by a Democrat and one was sponsored by an Independent.

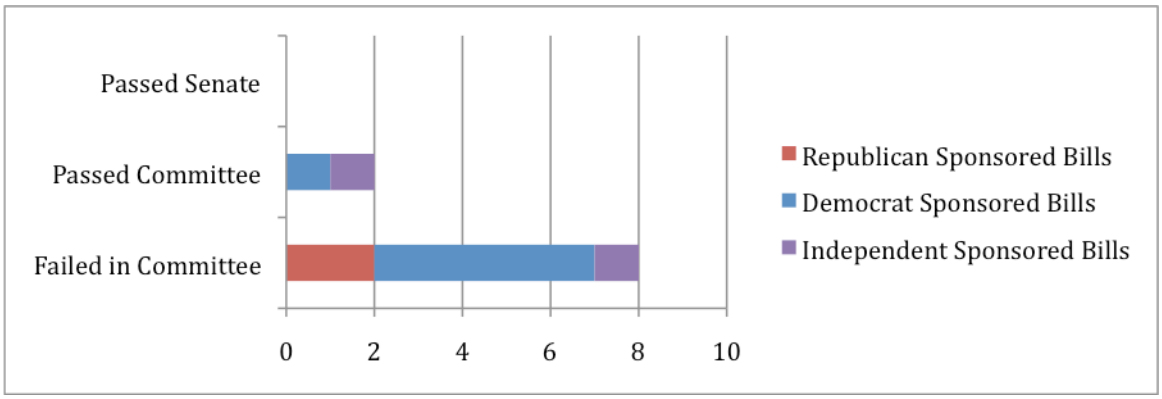

Figure 10 Sponsor Affiliation and Legislation Passage: Senate

To look at the parties' support and chances of bipartisanship, looking at the party breakdowns of each bill can be of assistance. It is important to note that these are only breakdowns of cosponsors; a bill could still have been bipartisan if the sponsor was a Democrat and the cosponsor was a Republican, or vice versa.

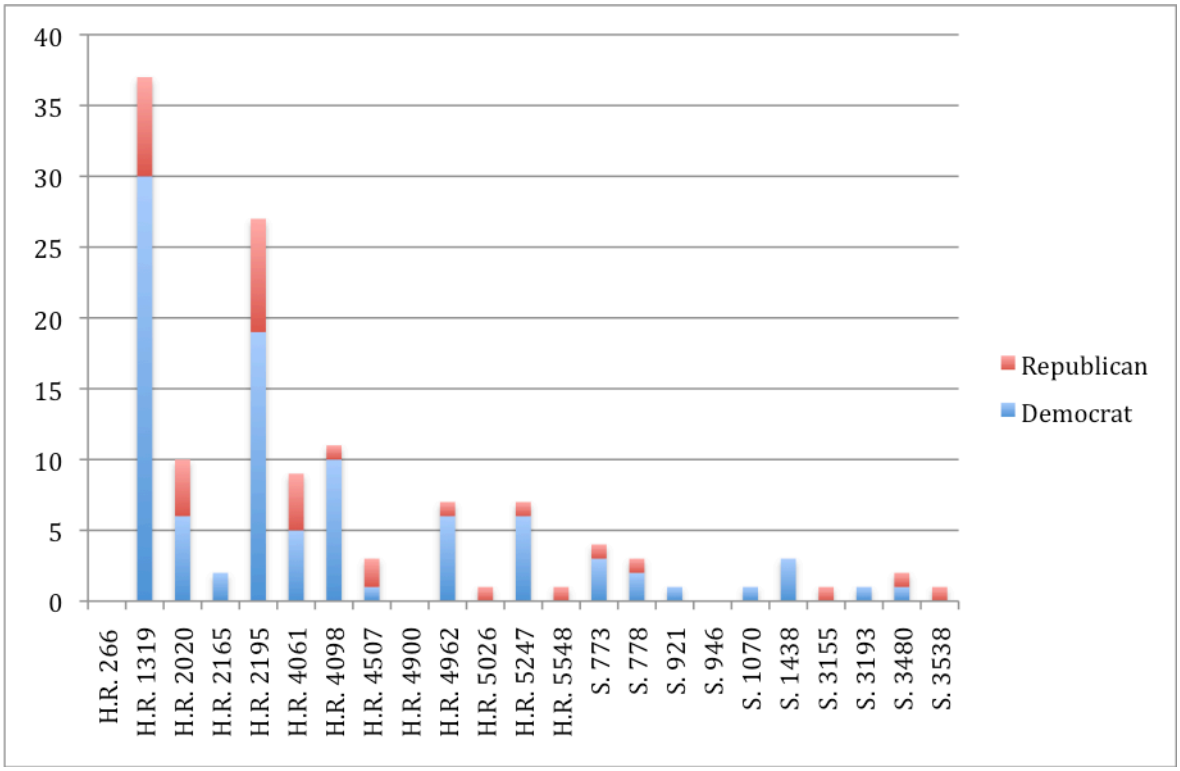

Figure 11 Cosponsor Party Affiliations by Bill

Possibly more beneficial, one must analyze the subtopics' party support. This can give a better insight of what kind of cybersecurity legislation can be passed. In the House, Republicans supported the Republican sponsored bill of regulating peer to peer software between government officials, but other than that, did not overwhelmingly support government regulation. Democrats also overwhelmingly supported the Republican sponsored P2P bill, but also supported file sharing regulation, international cooperation, and public-private partnerships. While this is not guaranteed to translate to party stances in general, it does provide some insight.

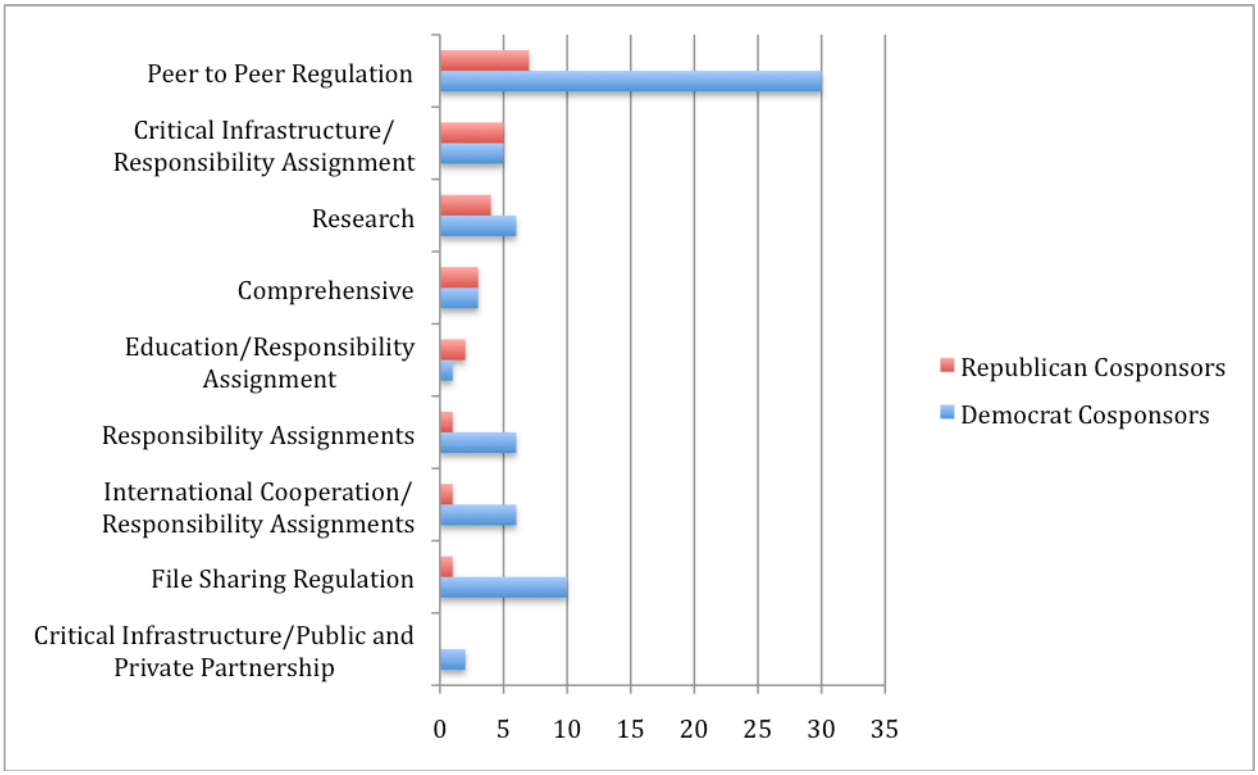

Figure 12 Average Breakdown of Cosponsor Affiliation by Main Issue: House of Representatives

In the Senate, the parties seem to be in more agreement. Moderate Republican Senators have signed onto Comprehensive, department responsibility assignment and changes, and international cooperation bills. These also happen to be the top three topics among Democrat cosponsors.

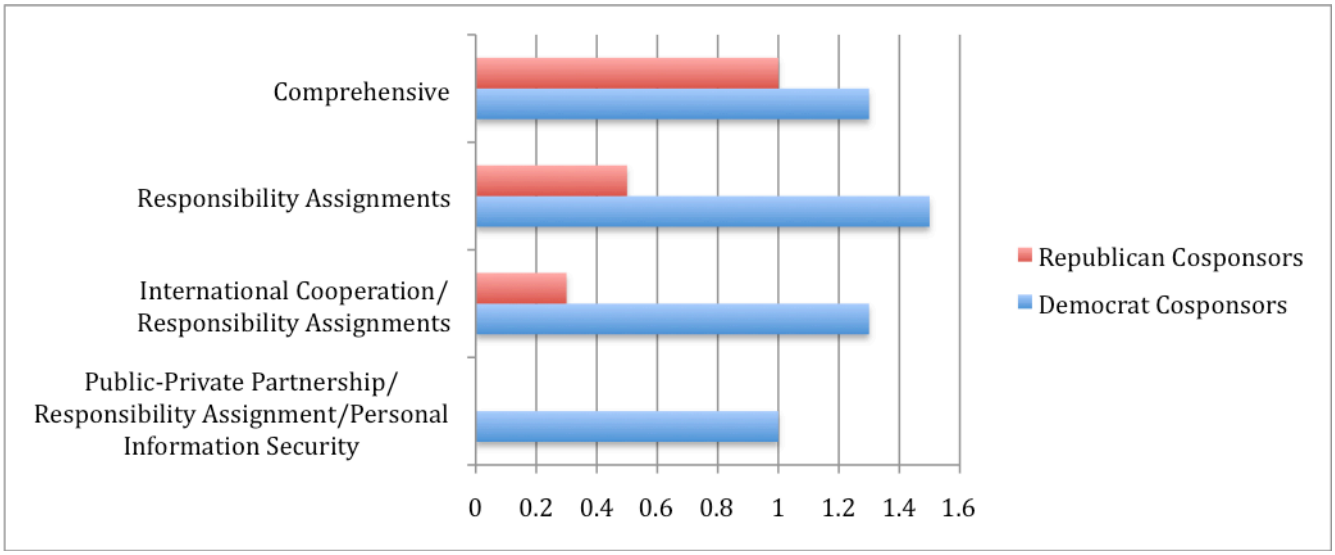

Figure 13 Average Breakdown of Cosponsor Affiliation by Main Issue: Senate

Further research into the cybersecurity stances of individual Congressmen and women would provide more insight into party support; however, this analysis allows for a glimpse into the behavior of the Senate and House in general.

Policy Recommendation

Cybersecurity legislation, comprehensive and specific, failed to pass in the 111th Congress. As the analysis and vote breakdowns show, this is not a Democrat versus Republican issue, nor is it as simple to have one cause of failure. The nature of the Senate, which has changed less than the House since the last election, has caused it to stall the process of legislating cybersecurity policies. This is why the recommendation focuses on the Senate. More specifically, further research would need to be conducted to make recommendations for the House with the party control changes. Senate Majority Leader Henry Reid has set the tone in the 112th Senate to make cybersecurity a priority in national security, and the environment is prime for pushing through cybersecurity legislation. This is why the recommendation focuses on the Senate.

As far as what type of legislation should be introduced, the answer comes in two phases. The first step is to pass a comprehensive bill that includes general principles. This is necessary to have guiding principles for future legislation that focuses on specific subtopics, and to define a long-term goal for United States' cybersecurity efforts. Senate bill *S.21 Cyber Security and American Cyber Competitiveness Act of 2011* is a perfect example of this. This will show to the world where the United States stands, and will help make government officials make decisions. One thing that is missing from *S.21* that would make subsequent legislation easier to develop is designation of who is in charge of what. Study of the 111th Congress show support of responsibility assignment from both parties. Until this is established, every proposed bill with specific subtopics of cybersecurity will be stalled. After the first step of passing comprehensive, yet non-specific legislation, the Senate can and should pass legislation on specific subtopics of cybersecurity. As James A. Lewis connected, the United States must realize the market cannot

always solve issues involving national security and technology. This leads one to conclude there is an immediate need to pass legislation that addresses public-private relationships and offer concrete steps and programs to foster a better relationship. The government can either move to regulate or offer incentives to achieve this. Although this should be one of the first specific pieces of legislation that Congress should pass, this can only come after a more comprehensive overview is passed.

S.21 is currently sitting in the Senate Homeland Security and Government Affairs Committee. This is exactly where a bill has the greatest chance of passage according to the study of the 111th Congress. It passed more bills than any other committee. Another reason of choosing this committee for current legislation and future proposals is because of the membership. The Chairman of the committee, Senator Lieberman, has been a leader in cybersecurity policy, and has sponsored two previous bills. The ranking member, Senator Collins, is a moderate Republican that has also been tied to cybersecurity. Although Democrats have sponsored and cosponsored more cybersecurity than republicans, by Senator Lieberman, an Independent, and Senator Collins, a Republican, leading cybersecurity and the Homeland Security Committee, legislation is likely to pick up speed and bipartisan support. She has previously supported comprehensive cybersecurity bills, so her support of *S.21* is obtainable and beneficial for passage.

Conclusion

In 2010 everyone appeared to recognize the serious problem of the United States' cybersecurity and the risk is caused national security, global economy, and personal information security. The attacks seen since the 1980s are evolving over time in severity and reaffirm the gravity of the current situation. It was disappointing and surprising that although countless congressmen spoke of the seriousness of cyber threats, the United States did not see any cybersecurity legislation. It is important to study the nature of the topic itself and the current legislative environment, in order to ensure the passage of cybersecurity legislation in the 112th Congress. By analyzing the failed bills of the last two years, it is recommended that the Senate pass a comprehensive cybersecurity bill immediately that provides a general set of goals and priorities in cybersecurity. That will allow for an easier path to approval for further cybersecurity legislation. The Senate Committee on Homeland Security and Governmental Affairs should continue to see a majority of cybersecurity legislation because of its membership. These recommendations are vital to ensuring the passage of cybersecurity legislation before a major cyber incident. Not only will legislation prevent cyber attacks, but also reactionary cybersecurity policy that may call for too much government regulation.[15]

[15] Lewis, James A. *Cybersecurity Two Years Later*. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. January, 2011. Web.

Bibliography

"Cyberwar: War in the Fifth Domain." The Economist. 1 July 2010. Web. 2 Nov. 2010.

Department of Defense Fiscal Year (FY) 2011 IT President's Budget Request. March, 2010. Janczewski, L, and A M Colarik. Cyber Warfare and Cyber Terrorism. N.p.: IGI Global, 2008. Google Scholar. Web.

"Internet Denial of Service Attacks and the Federal Response." Statement of Eric Holder Deputy Attorney General of The United States Before the Subcommittee on Crime of the House Committee on the Judiciary and the Subcommittee on Criminal Oversight of the Senate Committee on the Judiciary. February 29, 2000.

Lewis, James A. Cybersecurity Two Years Later. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. January, 2011. Web.

Lynn III., William J. "Defending a New Domain." Foreign Affairs (2010). Foreign Affairs. Sept.-Oct. 2010. Web. 05 Nov. 2010.

Maclean, William. “Cyber attack appears to target Iran-tech firms.” Reuters, 24 September 2010.

McDowell, Mindi, Brent Wrisley, and Will Dormann. "US-CERT Cyber Security Tip ST05-007 -- Risks of File-Sharing Technology." US-CERT: United States Computer Emergency Readiness Team. 19 May 2010. Web. 08 Sept. 2010.

Mesic, Richard, Myron Hura, Martin C. Libicki, Anthony M. Packard, and Lynn M. Scott. Air Force Cyber Command (Provisional) Decision Support. RAND Corporation, 2010.

Porteous, Holly. “The Stuxnet Worm: Just Another Computer Attack of a Game Changer?” International Affairs, Trade and Finance Division, Parliamentary Information and Research Service. 7 October 2010.

Reboot: Defining Paths to Cyber Policy, Law, and Technology Solutions. San Francisco: U.S. Department of Energy by Lawrence Livermore National Laboratory and Georgetown University, March 25, 2010.

Robert Elder, “Air Force Cyberspace Command: Defense Technology Forum,” Briefing, 8th Air Force, June 14, 2007.

Seeley, D. A Tour of the Worm. Department of Computer Science, University of Utah, 1988. Google Scholar. Web.

United States. Cong. House. *Bulk Power System Protection Act of 2009* . 111th Cong., 1st sess. H.R. 2165.

United States. Cong. House. *Cyber Security Domestic Preparedness Act* . 111th Cong., 2nd sess. H.R. 4507.

United States. Cong. House. *Cybersecurity Education Enhancement Act of 2009*. 111th Cong., 1st sess. H.R. 266.

United States. Cong. House. *Cybersecurity Education Enhancement Act of 2011.* 112th Cong., 1st sess. H.R. 76.

United States. Cong. House. *Cybersecurity Enhancement Act of 2010.* 111th Cong., 2nd sess. H.R. 4061.

United States. Cong. House. *Executive Cyberspace Authorities Act of 2010.* 111th Cong., 2nd sess. H.R. 5247.

United States. Cong. House. *Federal Information Security Amendments Act of 2010.* 111th Cong., 2nd sess. H.R. 4900.

United States. Cong. House. *Grid Reliability and Infrastructure Defense Act.* 111th Cong., 2nd sess. H.R. 5026.

United States. Cong. House. *Homeland Security Cyber and Physical Infrastructure Protection Act of 2011.* 112th Cong., 1st sess. H.R. 174.

United States. Cong. House. *Informed P2P User Act*. 111th Cong., 1st sess. H.R. 1319.

United States. Cong. House. *International Cybercrime Reporting and Cooperation Act.* 111th Cong., 2nd sess. H.R. 4962.

United States. Cong. House. *Networking and Information Technology Research and Development Act of 2009*. 111th Cong., 1st sess. H.R. 2020.

United States. Cong. House. *Protecting Cyberspace as a National Asset Act of 2010.* 111th Cong., 2nd sess. H.R. 5548.

United States. Cong. House. *Secure Federal File Sharing Act.* 111th Cong., 1st sess. H.R. 4098.

United States. Cong. House. *To amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack, and for other purposes*. 111th Cong., 1st sess. H.R. 2195.

United States. Cong. Senate. *A bill to establish the Small Business Information Security Task Force.* 111th Cong., 1st sess. S. 1070.

United States. Cong. Senate. *A bill to establish, within the Executive Office of the President, the Office of National Cybersecurity Advisor.* 111th Cong., 1st sess. S. 778.

United States. Cong. Senate. *Critical Electric Infrastructure Protection Act of 2009.* 111th Cong., 1st sess. S. 946.

United States. Cong. Senate. *Cyber Security and American Cyber Competitiveness Act of 2011.* 112th Cong., 1st sess. S. 21.

United States. Cong. Senate. *Cybersecurity Act of 2009.* 111th Cong., 1st sess. S. 773.

United States. Cong. Senate. *Cybersecurity and Internet Safety Standards Act.* 112th Cong., 1st sess. S. 372.

United States. Cong. Senate. *Fostering a Global Response to Cyber Attacks Act* . 111th Cong., 1st sess. S. 1438.

United States. Cong. Senate. *International Cybercrime Reporting and Cooperation Act.* 111th Cong., 2nd sess. S. 3155.

United States. Cong. Senate. *International Cyberspace and Cybersecurity Coordination Act of 2010.* 111th Cong., 2nd sess. S. 3193.

United States. Cong. Senate. *National Cyber Infrastructure Protection Act of 2010.* 111th Cong., 2nd sess. S. 3538.

United States. Cong. Senate. *Protecting Cyberspace as a National Asset Act of 2010.* 111th Cong., 2nd sess. S. 3480.

United States. Cong. Senate. *Tough and Smart National Security Act.* 112th Cong., 1st sess. S. 8.

United States. Cong. Senate. *United States Information and Communications Enhancement Act of 2009.* 111th Cong., 1st sess. S. 921.

Wuermeling, U. "New Dimensions of Computer-Crime--Hacking for the KGB--A Report." Computer Law & Security Report 5.4 (1989): 20-21. Google Scholar. Web.

Appendix

Methodology of Collecting, Categorizing, and Graphing Data of Legislation

The following is an example of graphing two figures, Figure 4 Proposed Legislation Topics: House and Figure 6 Proposed Legislation Topics: Senate. The same method of summarizing the bills proposed in the 111th Congress, categorizing, and graphing were used for all data collected and summarized in the figures included in the paper.

Collecting and Categorizing Data

A summary was written for each bill proposed in the 111th Congress. For identifying subtopic breakdown of the 111th Congress, "tags" were given to each bill, identifying what subtopic of cybersecurity policy they addressed (Education, Military, International Cooperation, Research, Department Responsibility Assignments or Changes, Private-Public Relationship, Critical Infrastructure, Other, or Specific risks). If there were more than two issues addressed, the bill was considered comprehensive.

TOPICS	NUMBER	BILLS
House		
Education	5	H.R. 266, H.R. 4098, H.R. 5548, H.R.76, H.R. 4061
Military	1	H.R. 5548
International Cooperation	2	H.R. 4962, H.R. 5548
Research	4	H.R. 2020, H.R. 4061, H.R. 5548, H.R.76,
Department Responsibility Assignments or Changes	10	H.R. 2195, H.R. 4061, H.R. 4098, H.R. 4507, H.R. 4900, H.R. 4962, H.R. 5026, H.R. 5247, H.R. 5548, H.R.76, H.R.174
Private-Public Relationship	6	H.R. 2165, H.R. 4061, H.R. 4900, H.R. 5548, H.R.76, H.R.174
Critical Infrastructure	4	H.R. 2165, H.R. 2195, H.R. 5026 , H.R.174
Other	2	*H.R. 5548 (civil liberties) H.R. 4061 (diversity)*
Specific risks	5	H.R. 1319, H.R. 2165, H.R. 2195, H.R. 4098, H.R. 5026
Senate		
Education	2	S. 773, S. 3480
Military	3	S. 3480, S. 3538, S.21
International Cooperation	6	S. 773, S. 1438, S. 3155, S. 3193, S. 3480, S. 3538, S.21
Research	6	S. 773, S. 3480, S. 3538, S. 3538, S.21, S.372
Department Responsibility Assignments or Changes	12	S. 773, S. 778, S. 921, S. 946, S. 1070, S. 1438, S. 3155, S. 3193, S. 3480, S. 3538, S.21, S.372
Private-Public Relationship	6	S. 773, S. 946, S. 1070, S. 3480, S. 3538, S.372
Critical Infrastructure	3	S. 773, S.8, S.21
Other	4	S. 1070 (personal information security), S. 3480 (civil liberties), S.8 (civil liberties), S.21
Specific risks		

Graphing Data

Once each bill was entered into the categories corresponding to each subtopic it addresses, the total "Number" was identified, and the information was presented in a graph.

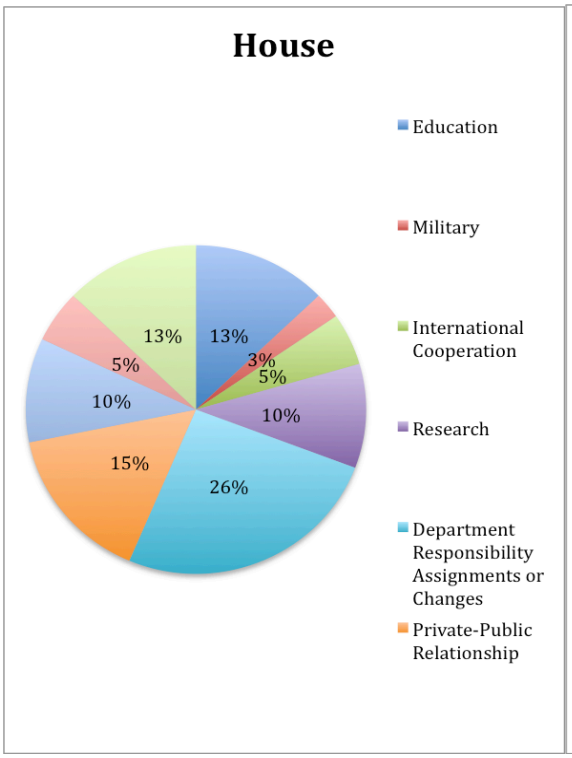

Figure 4 Proposed Legislation Topics: House

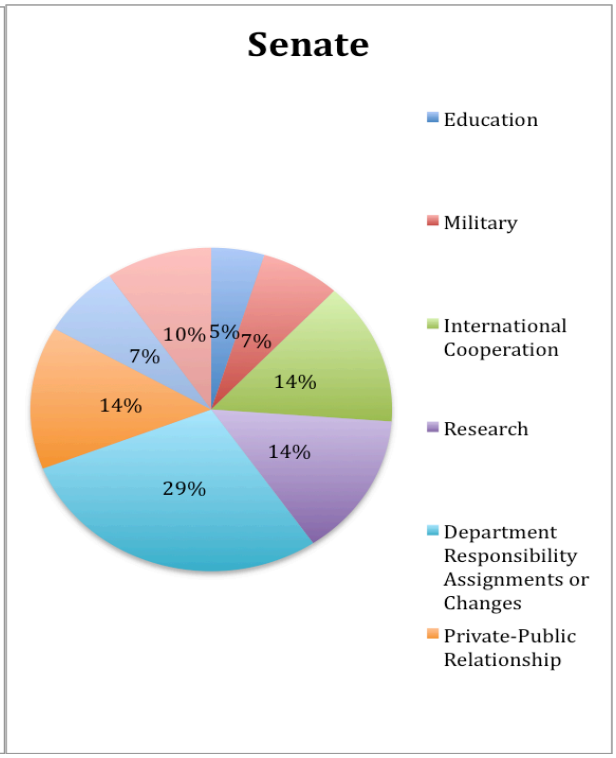

Figure 6 Proposed Legislation Topics: Senate

ACADEMIC VITA of Jessica M. Pelliciotta

Jessica Morgan Pelliciotta
436 South 19th Street
Easton, PA 18042
JPellici@gmail.com

Education: Bachelor of Arts Degree in Political Science, Pennsylvania State University, Spring 2011
Minor in Science, Technology, and Society
Honors in Science, Technology, and Society
Thesis Title: Cybersecurity Policy Analysis and Proposal
Thesis Supervisor: Darryl Farber

Related Experience:

Fellow at Roosevelt Institution Academy
Summer 2009, Washington, D.C.

Fellow at Young People For
2009,Washington, D.C.

Awards: American Association of University Women's Scholarship
Craig Millar Award
Dean's List
Phi Beta Kappa
Penn State Endowed Scholarship Recipient
Penn State Leadership Scholarship

Activities: Homecoming
Fall 2008, Spring 2010-Fall 2010
Corporate Relations Captain (Spring 2010-Fall 2010)

Lion's Paw Senior Honor Society
Spring 2010-Spring 2011
Member

Penn State College Democrats
Fall 2007-Spring 2011
President (Fall 2009-Spring 2010)

Penn State Student Handbook
Spring 2010-Spring 2011
Co-editor, Spring 2010
Editor in Chief, Spring 2011

Skull and Bones Society

Spring 2010-Spring
President (Spring 2010-Spring 2011)

UPUA (Penn State Student Government)
Spring 2009-Spring 2011
Chair of the Assembly (Spring 2010-Spring 2011)