Political Strategy for Cyber Security

Hilary Stone
Stanford University

Due to growing resentment from GOP Senators, the Cyber Security Act of 2012(S.2105), a bill that Senator Reid adamantly supports, is at risk. However, this bill is essential for the security of our nation's economy and citizens. In addition, by passing a measure on cyber security before the House of Representatives does, the Senate can frame the discussion in such a way that promotes the Democratic party's policy goals. In order to rescue this bill, the Democratic Party in the Senate needs to effectively build a coalition with children, senior citizens, and religious advocacy groups in addition to social media users and civil liberty groups. In addition, the Democrats need to respond swiftly to Republican claims that the Cyber Security Act of 2012 will hurt American companies.

There are currently two bills in the Senate that focus specifically on cyber security: the Cyber Security Act of 2012 and the McCain-sponsored Secure IT Act. The Cyber Security Act was introduced on February 14, 2012 to the Senate. On February 15, 2012, the bill was placed on the legislative calendar and on February 16, 2012, the Committee on Homeland Security and Governmental Affairs held hearings for the bill. Senator Reid has stated that he wants to put the bill to a vote before Congress's April recess.

In this paper, I will provide the legislative background to the bill and explain the Cyber Security Act of 2012 as well as the Republican response in detail. However, I will also provide the means for Reid and the Democratic Party to build a coalition and respond to Republican comments.

Background

Cyber security involves the protection of cyber networks from attack by foreign countries and hackers. These attacks could result in the loss of company trade secrets, classified government information, and personal identification information like Social Security numbers, credit card information, and home addresses. While this may seem like a drastic occurrence, cyber attacks do happen and can have costly results. Cyber attack victims include Google Inc, NASDAQ, and both McCain and Obama's presidential campaigns. According to Senator Susan Collins (R-Maine), cyber attacks cost Americans and American companies $114

billion a year. Experts from the Center for Strategic and International Studies predict that these cyber attacks will affect critical networks in America within the next two to three years.

One particularly dangerous aspect of cyber security is that many companies do not even know they are under attack. The Chamber of Commerce and its member organizations were the victims of an attack by Chinese hackers and did not know for several months. In fact, for many months after the Chamber of Commerce knew about the attack, Chinese hackers were still able to access secure information. Scott Aken, a former FBI agent that specialized in cyber security, noted that many companies do not realize their trade secrets have been stolen until many years later when a foreign company is able to produce the same good at a much cheaper price.

In addition, many companies do not disclose cyber attack information to either the government or their clients. Many companies fear that their customer base or stock price will drop as a result if they release that information. However, this only means that while some companies are aware of a threat, other companies are left in the dark and leave their customers unprotected.

In 2009, President Obama pledged support to cyber security legislation as long as doing so did not comprise personal privacy. However, Obama has not addressed what specific agency should be in charge of cyber security. There is a "turf war" in the cyber security field between the Department of Homeland Security, the National Security Administration, and the Pentagon. President Obama has appointed Howard Schmidt as a "Cyber security Coordinator" whose job is to help coordinate planning amongst all federal entities, and he reports directly to the President. In addition, the director of the National Security Administration, Gen. Keith B. Alexander, also serves as Chief of the Pentagon's Cyber Command. Cyber Command's mission is to protect military networks at home and abroad without sacrificing individual privacy.

In August 2009, Senators Rockefeller, Snowe, and the White House proposed bills that would allow the government to take control of vital Internet networks during times of "national emergencies". The government would then have power to order the disconnection of certain networks. Many critics have called this a "kill-switch" bill.

Below is a brief summary of a few previous cyber security bills, and their status in the Senate.

Cyber Security Enhancement Act of 2011-June 7, 2011-Robert Menendez (D-NJ)-Proposed requiring agencies to coordinate research and related activities in order to address cyber threats. It also required the creation of cyber security technical standards. Was referred to the Committee on Commerce, Science, and Transportation.

Public Awareness Act- April 13, 2011-Sheldon Whitehouse (D-RI) and Jon Kyl (R-AZ)- Required federal agencies to increase reporting of cyber

threats. By increasing reporting, agencies could determine what information should be made available to the public concerning cyber threats. The bill was referred to the Committee on Homeland Security and Governmental Affairs.

Cyber Security and Internet Freedom Act of 2011-February 17, 2011-Joe Lieberman (ID-CT), Susan Collins (R-ME), and Thomas Carpenter (D-DE)-Establishes an Executive Office in the Office of the President for Cyberspace Policy that will develop and oversee national cyber security strategy and ensures that federal agencies comply with the Department of Homeland Security standards. In addition, it allows the Department of Homeland Security to shut down or restrict access to certain websites or content. Many civil liberties groups including the ACLU and EFF protested against this bill.—Hearings were held in the Committee on Homeland Security and Governmental Affairs

Cyber Security and American Cyber Competitiveness Act of 2011- January 25, 2011-Harry Reid (D-NV)—Establishes a national center for cyber security run by an executive with the power to shut down critical infrastructure, including the Internet, in emergency situations. While many civil liberties groups like the Center for Democracy and Technology understand that the bill is meant to help in emergency situations, they also believe there were not enough safeguards in place to ensure that power is not abused—Referred to the Senate Committee on Homeland Security and Governmental Affairs.

The proposed Cyber Security Act of 2012 is meant to serve as a compromise between the bills proposed above and the dissenters worried about government regulation. The Cyber Security Act in fact will not receive presidential support if there is any possibility it could limit individual freedom and privacy.

Senate Bill S.2105-Cyber Security Act of 2012

Objectives: This bill has two objectives in the fight against cyber attacks. First, the bill promotes communication between companies and the government if a threat occurs. This bill requires companies to disclose information about attacks to other companies and to the federal government. Second, this bill establishes the Department of Homeland Security (DHS) as a regulating force in cyber security. DHS, along with other federal agencies and the National Institute for Standards and Technology, will conduct an immediate assessment of America's cyber networks to determine the biggest risks in America's cyber security. The DHS would establish computer security regulations on these critical infrastructure companies. The regulation would be "performance requirements" that allow the private sector to make the most economical and beneficial choice in terms of technology. Both the private sector and various federal agencies can propose these requirements. These requirements will mitigate the identified risks of the cyber network. The DHS does not have the power to regulate which specific security

technologies a company uses. If these companies fail to comply with DHS regulations, then the DHS has the authority to levy penalties. Every year, the owner of a regulated cyber network must write to DHS explaining the steps taken to reach the performance requirements. Once the cyber network has met the requirements, the owner of the network can petition for exemption. In addition, if the companies comply with these regulations, the government will offer them protection from civil-suits if an attack occurs.

Supporters: The sponsor of this bill is Senators Joe Lieberman(I-CT), and Senators Susan Collins(R-ME), Dianne Feinstein (D-CA), John Rockefeller(D-WV), and Sheldon Whitehouse(D-RI) cosponsor this bill as well. Lieberman is the Chair of the Homeland Security and Governmental Affairs Committee, and Susan Collins served as the ranking member. Lieberman's sponsorship for this bill stems from a need to enact legislation that promotes homeland security; "At some point, the federal government has got to be able to say to a private business that owns critical infrastructure that we all depend on, that an enemy might attack: 'You've got to meet this standard of defending yourself and defending our country." Susan Collins also approaches cyber security as a way to protect the United States from a catastrophic attack. On Susan Collins' own website, she writes, "The warnings of our vulnerability to a major cyber attack come from all directions and countless experts" and that we should be, "addressing the cyber threat with the same intensity we have applied to the terrorist threat." The Homeland Security and Governmental Affairs Committee directly oversaw the markup of this bill. Rockefeller is the Chairman of the Senate Committee on Commerce, Science, and Transportation. Rockefeller supports this bill because he believes, "the government needs a lead civilian agency to coordinate our civilian cyber security efforts, and that agency should of course be the Department of Homeland Security." Whitehouse is the Chairman of the Subcommittee on Crime and Terrorism in the Senate Judiciary Committee. Whitehouse has stated that this bill protects, "our national security, our economic well-being, the safety of our families, and our privacy." All of these Senators have proposed cyber security bills in the past that never made it past their committees. These senators have been working on cyber security since 2009 and would definitely feel relieved to finally have a bill pass. In addition, the White House has come out in support of this bill.

The main dissenters of the Cyber Security Act of 2012 are GOP leaders and business insiders. John McCain and seven other Republican senators claim that the Cyber Security Act places costly regulation on American companies. Secondly, they insist that NSA, rather than DHS, should oversee cyber security. Instead, these Republican Senators support a bill called the SECURE IT Act.

Besides John McCain, there are seven other cosponsors on the GOP cyber security bill. These senators are: Richard Burr (R-NC), Saxby Chambliss (R-GA), Daniel Coats(R-IN), Chuck Grassley (R-IA), Kay

Bailey Hutchinson(R-TX), Ron Johnson (R-WI) and Lisa Murkowski (R-AK). McCain is the Ranking Member of the Senate Armed Services Committee. McCain and Johnson serve on the Senate Homeland Security and Governmental Affairs Committee. Hutchinson serves as the Ranking Member of the Senate Committee on Commerce, Science, and Transportation Committee. Pro-business groups like the Chamber of Commerce and TechAmerica advocate for S.2151 because they want less government involvement in business affairs.

Republicans and business officials from the Chamber of Commerce and TechAmerica claim that the Cyber Security Act of 2012, by placing regulations on critical infrastructures, will force companies to bear the heavy cost of regulation. Over 85% of the critical infrastructure in the United States is owned by the private sector, causing Republicans and pro-business groups to claim that the Cyber Security Bill will burden businesses. Senator Saxby Chambliss, a co-sponsor of the SECURE IT Act, claimed, "Now is not the time for Congress to be adding more government, more regulation, and more debt—especially when it is far from clear that any of it will enhance our security." The SECURE IT Act instead does not regulate critical infrastructure and instead has similar information sharing procedures as the Cyber Security Act of 2012.

In addition, these Republicans believe that the National Security Administration (NSA) should have authority over cyber threats, and should have the ability to view these threats in real time. Currently, NSA oversees military cyber networks. Recently, NSA has proposed that major companies allow the NSA to sort through their Internet traffic and report any cyber attacks to the federal government. Recently, John McCain came out in support of this proposition. These GOP Senators believe that by granting NSA access to all Internet traffic, the government will be able to catch cyber threats in real time. In the SECURE IT Act, information sharing would operate through the NSA, instead of the Cyber Security Act that runs information sharing through the civilian DHS.

GOP leaders insist that this bill should go through multiple revisions and markups. However, Senator Reid has already publicly stated that he would like this bill brought to the floor before the end of April. Despite the fact that hearings have been help in the Committee on Homeland Security and Governmental Affairs, Republicans claim they need more time to evaluate this bill properly. These Republicans (John McCain, Mitch McConnell, and Chuck Grassley) have all publicly stated that there have not been enough opportunities for Republicans to help draft this legislation.

On the other hand, there are a few individuals who believe that the S.2105 bill is not strong enough. Technology industry insiders helped draft this bill, and as a result there are quite a few loopholes in the bill. For example, the DHS only has power to regulate cyber networks that could result in "mass" casualties if they were under attack. This means that

many companies will not be under the DHS guidelines even if their systems put citizens' critical information at risk.

The Committee of Homeland Security and Governmental Relations and its subcommittees held hearings on the bill.

Coalition in the Homeland Security and Governmental Affairs Committee

In order to pass this bill through the Homeland Security and Governmental Affairs Committee, Reid will need a strong coalition. It is safe to assume that since none of the Democrats have a vested interest in technology and security companies (i.e., none of them represent a large portion of those businesses), these Democrats will vote along party lines and advocate for the Cyber Security Act of 2012. None of them choose to cosponsor the more "business-friendly" bill with McCain. As a result, Reid simply needs to focus on the Minority. Luckily, the Ranking Member of the Committee, Susan Collins, already is a co-sponsor of the Cyber Security Act of 2012. She can put pressure on Republican senators and encourage them to vote for the Cyber Security Act of 2012. Senator Jerry Moran (R-KS), a member of the committee, will likely vote in favor of the Cyber Security Act of 2012 in order to remain in good favor with DHS. Moran hopes to receive funding for a National Bio and Agro-Defense Facility in Arkansas, but the money was not appropriated in the original FY 2013 budget. Moran willwant to stay in DHS Secretary's Napolitano's favor in order to receive this funding for the Arkansas project. Tom Coburn(R-OK) own Senate website explains that the Pentagon wastes about $50 billion a year. He may be worried that McCain's bill will only provide another way for the Pentagon to waste money, and instead will vote for the Cyber Security Act of 2012. Collins needs to remind Coburn that S.2105 will promote necessary, not wasteful, regulation. Scott Brown(R-MA) is a former member of the National Guard, and focuses immensely on the need to protect the US from terrorists. Lieberman and Collins have already framed this bill as a security issue, and this will help Brown sway in favor of S.2105. With these three additional Republican votes, the Cyber Security Act of 2012 should safely make it through the Committee on Homeland Security and Governmental Oversight to the Senate floor.

In order to pass S.2105, Senator Reid needs a strong coalition that will deter the GOP party from pursuing their bill (S.2151) and encourage the Republicans and Democrats that already pledged to support S.2105. However, it is important that Reid and fellow supporters of S.2105 should consistently frame the issue as a national safety and security issue, not an economic issue. The Republicans do have the upper hand in terms of economic issues because their bill does not force companies to take active measures to prevent cyber threats, and hence save money. However, the McCain sponsored bill does not protect the American people, and the supporters of the Cyber Security Act of 2012 should focus on this point. By framing the issue as a way to protect children, senior citizens, and

religious groups from cyber-related crimes, Reid will be able to draw in child advocacy groups, the AARP, and religious organizations and social media users. In addition, Reid could use civil liberties groups to frame the Cyber Security Act of 2012 as the best way to protect national security and individual liberties. Reid and fellow sponsors of S.2104 can create significant harm to key constituent groups that will increase favorability for this bill. With 2012 elections coming up, it is important for incumbents to raise Congress's approval ratings. By working across party lines on a consumer advocacy issue, candidates from all parties can claim that they effectively worked with other members of Congress to pass necessary laws.

Child Advocacy groups: Czech security Avast Virus Lab reported in early January 2012 that a large number of hackers are targeting children's internet games as a way to install malicious software on computers. Over 12,600 computers were affected from these malicious sites. Children, and parents, are often unaware that certain games come from dangerous sources and could be destroying the security of their family. Reid could build a child advocacy coalition to help protect children, and families, from malicious software that targets children. This coalition should focus its media attention on Parenting Magazine, Scholastic's Parent and Child Magazine, pluggedinparents.com, kidfriendlyguide.com and television shows like Modern Family that draw in the 18-49 year old demographic. These magazines, websites and television shows will capture the major parenting demographics that Senator Reid should focus on. Advertisements should play into the fears of this demographic and should bring about issues like security and safety related to stolen data from the Internet. To add clout to these arguments, the organization Web Wise Kids should help sponsor this lobbying technique. Web Wise Kids has the incentive to gain more national coverage. The organization has a strong government relationship with the Obama administration, but is less well known with the general public in comparison to organizations like Common Sense Media. By serving as the advocate for the Cyber Security Act of 2012, Web Wise Kids will be able to increase its national popularity while helping the President draw in parents, teachers, and child advocates into his coalition.

In particular, Reid will want to work on building support in California for these initiatives. Although Barbara Boxer is a Democrat, California still is the host to a large majority of America's technology and security firms. Building support for the Cyber Security Act of 2012 amongst California citizens will put pressure on these companies to adopt and actively support S.2105. Jim Steyer and Diane Feinstein should partner together to write op-eds in major California newspapers. Jim Steyer, of Common Sense Media (and a Bay Area resident), would be a great op-ed author in particular because of his connection to the issue as a children's advocate and his connection to Tom Steyer. Tom Steyer is Jim's brother, and has a huge following in Silicon Valley due to his

investments in technology companies. Jim could skillfully advocate for the need to protect children, while articulately addressing the economic issues. Senator Feinstein is a co-sponsor of the bill, and she can adequately squelch technology companies' concerns by providing her reasoning for supporting the bill. These op-eds should run in major newspapers in California like the LA Times, the San Francisco Chronicle, and the San Diego Union Tribune. In addition, these op-eds should also be in regional Bay Area newspapers, specifically the Palo Alto Daily News and the San Jose Mercury.

Religious Organizations: Religious organizations are often the target of malicious software and hacking incidents. In March 2012, the hacking group "Anonymous" took over the Vatican website. On the site, "Anonymous" wrote "any kind of religion is a sickness to the world." By reaching out to religious, and particularly Christian organizations, the Democrats can utilize a strong network that often has clout with Republicans. While the bill will not specifically protect religious organizations' websites, it will pave the way for future cyber security bills that protect more than critical infrastructure. Religious organizations do not want their websites attacked by hackers, and thus will support a bill like S.2105 that has stronger security features than the McCain sponsored bill. The Christian Post already has posted detailed articles about the "Anonymous" hackers attack on religion and the Vatican website. Reid should also focus on bringing in Senator Susan Collins, a Republican from Maine, should interview with these organizations' publications and frame the issue as a way for religious conservatives to protect their own organizations from harmful Internet attacks. An interview, rather than an op-ed, will fit in better with the style of these publications. Religious conservatives are a politically active constituency that can pressure Republicans into supporting the Cyber Security Act of 2012.

AARP: The AARP already is a supporter of stronger security measures for the Internet. Senior citizens are often the targets of cyber attacks. Jay Rockefeller is an extremely recognizable member of Congress that works on other issues, like Alzheimer's and net neutrality that the AARP has publicly supported. In addition, Rockefeller is also much older, which allows him to address the AARP members as his peers. Rockefeller should interview with AARP for their national publication. Jay Rockefeller's interview in AARP should highlight the Cyber Security Bill of 2012 as a way to protect senior citizens from the dangers of the Internet and reduce the number of identity thefts and financial fraud among senior citizens. By advertising through AARP's magazine, Senator Reid will reach one of the most politically active groups of constituents.

Social Media Users: Internet security is an issue that citizens do care about. According to a USA Today poll, 70% of Facebook users and 52% of Google users are concerned about their online privacy. If these citizens are active users of social media, it is highly likely they also use the Internet to purchase goods which could easily put them at risk to exposing

their Social Security numbers, addresses, and credit card numbers. Senator Reid should address these Internet and social media users directly through a social media campaign. The average Facebook or Twitter user is going to care more than the average individual does about Internet security because it is an issue that personally affects them. However, the President is the best individual to implement this part of the plan. Barack Obama has over 24 million followers on Facebook, the Barack Obama campaign Twitter account has over 11 million followers, and the White House has over 2.5 million followers. Barack Obama can reach a vast national audience instantaneously. He should post about his support for the bill and his strives to make the Internet safer for those on Facebook and Twitter. Most importantly though, he should ask individuals to "share" or "retweet" his status. This would share the President's message about the Cyber Security Act of 2012 with millions of people who do not necessarily follow the President, but are just friends with someone who does.

Civil Liberty Groups: Senator Reid could use civil libertarians to his advantage while working on the Cyber Security Act of 2012. The ACLU has already come out against the SECURE IT Act, and the ACLU could be a pivotal partner in building a civil liberty coalition. Michelle Richardson, the legislative counsel for the ACLU, stated, "the bill [SECURE IT] would allow the NSA to collect the Internet records of civilians who are not suspected of doing anything wrong." The McCain sponsored bill has very broad language that worries the ACLU. The Center for Democracy and Technology has also advocated that the Secure IT bill's language is much too vague, and could easily allow the government to violate the privacy of innocent individuals for the sake of security. This broad language includes asking for companies to share data with the NSA. These groups would prefer to have a civilian organization, rather than a military organization, be in control of information sharing. Given that so many civil liberties groups have already spoken out against the SECURE IT bill, these organizations would be perfect partners to help pass the Cyber Security Act of 2012.

To promote the protection of civil liberties through S.2105, John D. Rockefeller should be the head spokesperson on this issue. Rockefeller already recently has spearheaded several projects that the ACLU applauded, including tbe "Do Not Track" bills. In order to explain the civil liberties issues behind the Secure IT Act, Rockefeller needs space to thoughtfully convey his concerns with the Secure IT Act. This means that a longer written piece, like an op-ed, would probably be best. Rockefeller should partner with the ACLU's Director of the Washington Legislative Office, Laura W. Murphy, to write this op-ed. Working with the ACLU will give Rockefeller's op-ed more credibility. This op-ed should run in the ACLU's national publications and in the New York Times. The New York Times has a huge reach and national clout, but it also has a huge presence in social media. Individuals often share New York Times articles

regularly on Facebook and Twitter, but the New York Times does an amazing job promoting its own articles in the social media sphere. Using the New York Times will allow Rockefeller's message to reach as many individuals as possible.

Bipartisanship: A recent NY Times poll put the Congressional approval rating at 9 percent. In 2012, 33 of the U.S. Senate's 100 seats will be up for reelection. Democrats and Republicans alike can use the Cyber Security Act as proof that Congress is working together to promote the safety and security of the American public. Susan Collins and Joe Lieberman would be the perfect people to bring this message to the American public. Lieberman and Collins are the Chairman and Ranking Member of the Senate Homeland Security and Governmental Affairs Committee. Their co-sponsorship of this bill indicates a willingness to compromise in order to produce better legislation. To advocate for this position, I propose that Lieberman and Collins write op-eds for the New York Time and for the Wall Street Journal, respectively. These national newspapers often spur subsequent articles in smaller newspapers because they represent a national trend. By placing their work towards bipartisanship in the Cyber Security Act of 2012 in national newspapers, Lieberman and Collins will be able to build positive feedback for the bill. They will also be able to frame McCain and his cosponsors as individuals who are both unwilling to accept compromise and delaying the progress on a bill that will protect Americans.

Economic Reasoning

While it is necessary to frame the Cyber Security Act of 2012 as a homeland security issue, it is unreasonable to expect economic issues not to come up, especially during the Recession and in a reelection year. However, there are ways to frame the bill as to entice coalitions that focus solely on the economic costs of the Cyber Security Act of 2012. The Cyber Security Act of 2012 would require companies to take security measures to protect critical infrastructure, and some estimates place that collective cost at $46 billion per year. This large upfront cost is what worries many Republicans and business groups.

Senator Reid can frame the bill as a way to fix a market failure in order to build support for the Cyber Security Act of 2012. McCain and his cosponsors believe that government regulation is inappropriate because it is too costly. However, this is simply not true. While the upfront cost of creating a stronger security system seems huge, cyber attacks cost $114 billion per year, and $338 billion if one includes time lost. In 2011, Sony estimated that cyber security attacks would cost the company at least $170 million. At the end of the day, America will be saving itself a significant amount of money over a long period of time. Even if one discounts the future benefits, the amount of money companies would save in one year could validate the regulation in the Cyber Security Act of 2012. Democratic Senators need to advocate for these sound economic reasons

behind the Cyber Security Act of 2012 in order to win over pro-business individuals. By framing the legislation as a way to invest in the security of American companies, Democrats can counter the negative comments from Republicans and tech industries.

Next, Reid, Lieberman, and their supporters can focus on the fact that many company representatives were involved in drafts and markups of S.2105. Business partners asked that the bill define precisely what "critical infrastructure" means. As a result, there are many companies that will not need to be under the regulation of S.2105. It is important to note that not every Internet company will be regulated, just those that essential to America's safety. In addition, the Democrats can point out that thanks to business involvement, companies can take their own measures to meet security standards. Microsoft's Corporate Vice President of Trustworthy Computing, Scott Charney, spoke at the hearing for the Cyber Security Act of 2012. Charney articulated that the bill's "technology neutral policies" would allow, "flexible and agile risk management, narrowly focused on risks of greatest concern." Instead of forcing companies to use a particular protection method, the bill allows companies to choose whichever method works best for them. This way, innovation will evolve in the cyber security sector, and companies can choose lower cost methods. This point, if advocated successfully in the media, can mitigate the Chamber of Commerce's complaints about the bill's cost to industry. Microsoft should step out publicly and create a campaign that endorses the bill they helped to write. It should place adds in national business focused publications, like the Wall Street Journal, Forbes, and Business Week, that detail the costs to the public if no action is taken, versus the cost to companies if S.2105 passes. In addition, to place pressure on other technology companies, Microsoft should advertise via Internet ads on sites like Mashable, TechCrunch, and DailyTech. Microsoft will have an incentive to do this because they put a lot of effort into crafting this legislation in Microsoft's favor, and they would not want a different bill, like the SECURE IT Act, to pass instead.

Lastly, Democrats can advocate that they are technically protecting American profits by instituting this legislation. American companies and their trade secrets are often the target of cyber attacks. By forcing cyber networks to update their security, the government is protecting American companies in all sectors of the economy. Being a Republican, Susan Collins would be the perfect messenger for this idea. The Republican Party traditionally tries to protect American companies, and this case would be no exception. Collins could easily play into Republican sympathies with companies in order to convince fellow Republicans to support her bipartisan bill.

Conclusion

While the future of the Cyber Security Act of 2012 is currently at risk, there are steps that Reid and other sponsors of S.2105 can take to ensure

its success. It would be a legislative victory for the Democrats if they could set the language and tone on cyber security. To defeat the Republican sponsored SECURE IT Act, Susan Collins needs to use her influence as Ranking Member on the Committee of Homeland Security and Governmental Affairs to secure votes from key Republicans on the committee. In addition, Reid needs to form a broad coalition of advocacy groups that includes child advocates, senior citizens, religious groups, social media users, and civil libertarians. Cyber security crimes target these groups, and the supporters of S.2105 can frame the Cyber Security Act of 2012 as a way to protect these key constituent groups. However, supporters of S.2105 are also going to have to address economic concerns of the bill. Luckily, the costs of cyber security crimes outweigh the upfront security costs, and there was plenty of business involvement during hearings and drafting of the legislation. Using these techniques, Reid, Lieberman, Collins, Feinstein, and Rockefeller can ensure success for S.2105 and successfully pass cyber security legislation.

References

Acohido, Byron. "Most Google, Facebook Users Fret Over Privacy", USA Today, http://www.usatoday.com/tech/news/2011-02-09-privacypoll09_ST_N.htm?AID=4992781&PID=4165004&SID=137i1hrytn4co(accessed on February 20, 2012).

Boland, Trevor. "Despite Recent Threats Infrastructure is Still Vulnerable To Cyber Attack", Security News, http://www.securitypronews.com/insiderreports/insider/spn-49-20120202DespiteRecentThreatsAmericanInfrastructureisStillVulnerabletoCyberAttack.html (accessed on March 20, 2012).

Brown, Donald C. "Worries Abound Over US Cyber-Emergency Internet Policy", *Technology News*, Commerce Times http://www.ecommercetimes.com/rsstory/71953.html?wlc=1299623061 (Accesses on March 3, 2012).

Brown, Scott. "Key Issues", http://www.scottbrown.senate.gov/public/index.cfm/keyissues (accessed on March 21, 2012).

Charney, Scott. Hearing on the Cyber Security Act of 2012, http://www.hsgac.senate.gov/hearings/securing-americas-future-the-cybersecurity-act-of-2012(accessed on March 20, 2012).

Clayton, Mark. "Loopholes Leave America With Weak Cyber Security Plan, Experts Say", Christian Science Monitor, http://www.csmonitor.com/USA/2012/0216/Loopholes-leave-America-with-weak-cybersecurity-plan-experts-say, (accessed on February 21, 2012).

Coburn, Tom. "Legislation and Issues", http://www.coburn.senate.gov/public/?p=national-security(accessed on March 21, 2012).

Collins, Susan. “The Time To Strengthen Cyber Security it Now”, *Weekly Column*, US Senate, http://collins.senate.gov/public/continue.cfm?FuseAction=PressRoom.WeeklyColumn&ContentRecord_id=8c54c290-e7fa-6cb4-146c-4b82274585aa& (accessed on March 20, 2012).
Cross, Grant. “Republican Senators Introduce Their Own Cyber Security Bill”, *Business*, PC World, http://www.pcworld.com/businesscenter/article/251105/republican_senators_introduce_their_own_cybersecurity_bill.html(accessed on March 10, 2012).
Eggerton, John. “Lieberman: Cyber Security Bill Without Enforceable Standards Doesn’t Get Job Done”, Multichannel News, http://www.multichannel.com/article/481560-Lieberman_Cybersecurity_Bill_Without_Enforceable_Standards_Doesn_t_Get_Job_Done_.php (accessed on March 9, 2012).
Gorman, Siobhan. “Cyber Security Bills Duel Over Rules for Firms”, Wall Street Journal, http://online.wsj.com/article/SB10001424052970203961204577269832774110556.html (accessed on March 4, 2012).
Gorman, Siobhan. “NSA Chief Seeks Bigger Cyber Security Role”, *Business,* Wall Street Journal, http://online.wsj.com/article/SB10001424052970203833004577247710881763168.html?mod=googlenews_wsj(Accesed on March 1, 2012).
Gorman, Siobhan. “China Hacker Hits US Chamber”, *China News*, Wall Street Journal, http://online.wsj.com/article/SB10001424052970204058404577110541568535300.html (accessed on Feb 29, 2012).
Greene, Brett. “Big Brother May Be Your Employer, Not Just Your Government” *Tech*, Huffington Post, http://www.huffingtonpost.com/brett-greene/secure-it-act_b_1332987.html (accessed on March 12, 2012).
Harris, Leslie. “NSA”s Cyber Power Grab”, *Tech*, Washington Post, http://www.huffingtonpost.com/leslie-harris/nsa-cyber-security_b_1321809.html (accessed on March 6, 2012).
Huffington Post, “Anonymous Hacks Vatican Website In Cyber Attack On Holy See, Sources Say”, http://www.huffingtonpost.com/2012/03/07/anonymous-hacks-vatican-website_n_1327297.html (accessed on March 14, 2012).
Huffington Post, “Nasdaq’s Poor Computer Security Led to Cyber Attack, Probes Say”, *Business,* http://www.huffingtonpost.com/2011/11/18/nasdaqs-poor-computer-security-cyber-attack_n_1101142.html(accessed on March 1, 2012).
Jacobs, Andrew. “Google, Citing Attack, Threatens to Leave China”, New York Times,

http://www.nytimes.com/2010/01/13/world/asia/13beijing.html?pagewanted=all(accessed March 5, 2012)
Kain, Eric. "Does the Cyber Security Act of 2012 Mark the Beginning of the War on Cyber-terrorism?", Forbes, http://www.forbes.com/sites/erikkain/2012/02/22/does-the-cybersecurity-act-of-2012-mark-the-beginning-of-the-war-on-cyber-terrorism/(accessed on March 2, 2012).
Lenzer, Robert. ""China's Cyberattacks on US Corporations Could Hurt Stock Prices", Forbes, http://www.forbes.com/sites/robertlenzner/2011/10/27/american-corporations-asked-to-disclose-costly-cyberattacks-that-might-impact-share-prices/ (accessed on March 1, 2012).
Madison, Lucy. "Congressional Approval at All Time Low of 9%", *Political Hotset,* CBSNews, http://www.cbsnews.com/8301-503544_162-20125482-503544/congressional-approval-at-all-time-low-of-9-according-to-new-cbs-news-new-york-times-poll/ (accessed on February 21, 2012).
Moran, Jerry. "News Releases" http://moran.senate.gov/public/index.cfm/news-releases?ID=af0bc6c5-c121-46e6-9c32-81ccba071b53(accessed on March 21, 2012).
MSNBC, "Civil Libertarians Slam McCain's Cybersecurity Bill", http://www.msnbc.msn.com/id/46644471/ns/technology_and_science-security/#.T2qX3GKXSjM(accessed on March 14, 2012).
Muncaster, Phil. "Malware Found in Children's Gaming Websites", V3.co.uk, http://www.v3.co.uk/v3-uk/news/2139322/malware-childrens-gaming-web-sites (accessed on March 14, 2012).
Nakashima, Ellen. "White House, NSA Weigh Cyber Security and Privacy", *National Security,* Washington Post, http://www.washingtonpost.com/world/national-security/white-house-nsa-weigh-cyber-security-personal-privacy/2012/02/07/gIQA8HmKeR_story.html(accessed on March 1, 2012).
Newsweek, "Hackers and Spending Sprees", *U.S. Politics,* http://www.thedailybeast.com/newsweek/2008/11/04/hackers-and-spending-sprees.html(accessed March 2, 2012).
Perlroth, Nicole. "Traveling Light in an Age of Digital Thievery", *Business Day: Technology,* New York Times, http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?pagewanted=all (accessed on February 28, 2012).
Rockefeller, John. Hearing on the Cyber Security Act of 2012. http://www.hsgac.senate.gov/hearings/securing-americas-future-the-cybersecurity-act-of-2012 (accessed on March 20, 2012).
Rodriguez, Salvador. "Attacks on Website Spark Demand for Cyber-Security Experts" , LATimes,

http://articles.latimes.com/2011/jul/05/business/la-fi-hacking-security-20110705 (accessed on March 20, 2012).
Sasso, Brendan. "ACLU Warns of Expanded Spying Powers in New GOP Cybersecurity Legislation", *Hillicon Valley*, The Hill, http://thehill.com/blogs/hillicon-valley/technology/215323-aclu-warns-of-expanded-spy-powers-in-gop-cybersecurity-bill (accessed on March 12, 2012)
Sasso, Brendan. "Longtime Friends Lieberman, McCain Divided over Cybersecurity Legislation", *Hillicon Valley*, The Hill, http://thehill.com/blogs/hillicon-valley/technology/215907-senators-mccain-lieberman-disagree-its-a-real-doozy(accessed on March 14, 2012).
Schmidt, Michael. "New Interest in Hacking as Threat to Security", *U.S.*, New York Times, http://www.nytimes.com/2012/03/14/us/new-interest-in-hacking-as-threat-to-us-security.html (accessed on March 14, 2012).
Smith, Gerry. "Cyber Security Bill Faces Uncertain Future in Fight Over Regulation", *Tech,* Huffington Post, http://www.huffingtonpost.com/2012/03/19/cybersecurity-bill-regulation_n_1362529.html(accessed on March 19, 2012).
Symantec, "Press Releases", http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 (accessed on March 20, 2012)
Toor, Amar. "The Internet 'Kill Switch' Bill" , *Switched*, Huffington Post, http://www.switched.com/2011/02/01/internet-kill-switch-bill-what-it-is-wont-die/ (accessed on March 1, 2012).
US Chamber of Commerce, "Defense" http://www.uschamber.com/issues/defense/critical-infrastructure-protection-information-sharing-and-cyber-security(accesed on March 20, 2012).
Whitehouse, Sheldon. "Whitehouse Statement on New Cyber Security Legislation", http://whitehouse.senate.gov/newsroom/press/release/?id=faf25d6c-a1d7-4b40-9e4d-083fddccbd8b (accessed on March 20, 2012).