# **Cybersecurity File**

**Researched and cut by Edie, Evan, Soham, Daniel, Jonathan, Michael, Yuxiao, Aaron, Roshan and Jeremy. Uniqueness: Evan Katz. Internal Links: Michael Li. Impacts: Jonathan Yu. Final Organization: Daniel Goynatsky**

# **Negative**

## 1NC Shell

#### **The bill’s moving forward, but faces an uphill battle – continued political pressure from Obama key**

Martinez and Cox, 7/26 – staff writers for The Hill (Jennifer and Ramsey, “Senate advances bill to bolster cybersecurity defenses in 84-11 vote”, The Hill, 7/26/12, <http://thehill.com/blogs/hillicon-valley/technology/240605-senate-advances-bill-to-bolster-cybersecurity-defenses-in-84-11-vote>) // EK

The Senate agreed on Thursday to move forward with Sen. Joe Lieberman's (I-Conn.) cybersecurity bill after months of contentious negotiations.¶ The motion to proceed to the Cybersecurity Act was approved 84-11 after Senate Majority Leader Harry Reid (D-Nev.) agreed to an open amendment process. ¶ The bipartisan Cybersecurity Act, S. 3414, aims to protect the nation from cyber attacks against critical infrastructure such as the electrical grid, banking systems, military operations, transportation networks and others. President Obama said Thursday that he supports that version of the bill introduced by Sen. Joe Lieberman (I-Conn.), but noted it lacked "some of the key provisions of earlier bills."¶ Although the bill cleared this test vote, it faces an uphill battle to reach the finish line. While senators are meeting to try to find an agreement both sides can agree to, they haven't reached a resolution yet. ¶ "The conversations are very productive, but obviously there's a lot of work to do and not very much time to do it," Sen. Jon Kyl (R-Ariz.), one of the lead negotiators, said Thursday morning.¶ Republicans voting against the motion to proceed to the bill were Sens. Mike Johanns (Neb.), Rand Paul (Ky.), Ron Johnson (Wis.), Marco Rubio (Fla.), Dean Heller (Nev.), Pat Roberts (Kan.), Mike Enzi (Wyo.), John Barrasso (Wyo.) and Jerry Moran (Kan.).¶ Democrats opposing the motion to proceed were Sens. Jon Tester (Mont.) and Max Baucus (Mont.).¶ In a bid to win GOP support, Lieberman introduced a revised version of the bill last week that scaled back provisions that would have mandated critical operators to meet a set of security standards developed, in part, by the Homeland Security Department. The latest version of the bill proposes to establish a program where companies operating critical infrastructure would certify that they meet security standards approved by a government-led agency in exchange for incentives, such as liability protections.¶ Senate Majority Leader Harry Reid (D-Nev.) said he would welcome more amendments during the voting process, which Republicans said was key to winning their support for the bill to move forward.¶ “There’s plenty of room for changes,” Reid said on the floor Thursday. “Let’s have as many amendments as people feel appropriate.”¶ Sen. Kay Bailey Hutchison (R-Texas), one of the sponsors of the competing SECURE IT Act, said earlier that she and the other sponsors wouldn’t block a vote on the Cybersecurity Act if the amendment process were truly open.¶ "I don't think anyone in our group wants to hold up dealing with cybersecurity. We know that America's systems could be under threat and some have been hacked into already," she said. "As long as we have an amendment process and are not shut out of this, we will vote to move forward to the bill."¶ Lieberman and the co-sponsors of his bill have been meeting with the Republican backers of the alternative SECURE IT Act to try to hammer out an agreement that would bridge the differences between the two bills. The members met Thursday morning and plan to meet again on Friday and next week.¶ Sen. Susan Collins (R-Maine), a sponsor of the Cybersecurity Act, said she’s open to changes but that legislation should to be passed quickly for the sake of national security.¶ “We must act and we must act now,” Collins said Wednesday. “We can’t afford to wait for a cyber 9/11 before taking action on this legislation.”¶ Reid said he’d like to spend most of next week voting on the amendments offered.¶ As a show of good faith that those working on the Cybersecurity Act are open to changes, Collins pointed out that some changes have already been made to the bill.¶ “We have revised our bill in a very substantial way,” Collins said citing that many of the standards related to the private sector are now optional. “This shows a willingness to adopt changes and we’re still open to changes.”¶ When originally proposed, the bill got push back from industry groups and some lawmakers concerned about Internet privacy.¶ The U.S. Chamber of Commerce and IBM sent out letters on Thursday urging senators to vote against the bill moving forward, arguing it would saddle industry with additional regulations. However, the bill won endorsements from tech giants Cisco and Oracle.¶ The cybersecurity bill is the culmination of more than a year of work by working groups compromised of staff from committees with jurisdiction over cybersecurity, including Homeland Security and Governmental Affairs, Commerce and Intelligence. The working groups spent months developing legislative language for the bill and also included language from earlier cybersecurity bills that had passed out of committee.

[Insert Specific Link Here]

#### Failure to pass legislation means cyber-terrorism goes nuclear and guts vital infrastructure, turning case

Ken 10 (writer for modern survival blog, Ausbry Ken, “Cyber Terrorism-Nuclear Power plants-Grids”, October 18th 2010, <http://modernsurvivalblog.com/nuclear/cyber-terrorism-nuclear-power-plants-grid///DG>)

The recent discovery of the “Stuxnet” computer worm cyber-weapon, apparently designed and used to infect Iran’s nuclear development control systems, presents a very powerful and dangerous new threat to our current way of life. Stuxnet, first discovered during June 2010 is the first worm of its kind to take aim at the foundation of critical industrial systems. It was uniquely written to spy on, reprogram, and attack the systems used to control and monitor industrial processes, while at the same time hiding the changes it makes. The bulk of the media reporting on Stuxnet has been focused on its apparent design to target Iranian nuclear control systems because it contains specific code to hack the underlying “Siemens” hardware and software used within the Iranian systems. Although this particular targeting may be true, the Siemens systems are used far and wide to manage other types of industrial facilities including water supplies, oil rigs, and power plants in many parts of the world. Now that Stuxnet is out in the open, the door is wide open for much wider spread and disastrous possibilities, given the will to do harm. It could conceivably be used as a blueprint, and tailored or modeled to inflict a extreme catastrophe. Think of this… a modified Stuxnet worm is introduced into the network of an operational nuclear power plant, where it silently reprograms the control systems of the nuclear reactor and waits until a pre-determined time to enact its devastating plan, a nuclear meltdown. Imagine the same worm being inserted or replicated in multiple nuclear reactor networks, all executing their devastating code at the same time, creating not only a nuclear meltdown emergency of epic proportions, but quite possibly bringing the entire electrical power grid system down from cascading tripping circuit breakers as the instantaneous demand for re-routed power is not met. To consider such possibility is not alarmist. Instead it is a responsible process to think, speak openly, and to consider the vast network of control systems that underlie our dependence on infrastructure, and to plan ahead for a cyber-weapon similar to Stuxnet that could conceivably bring it all down and change our lives in ways that we cannot imagine. While industries scramble to cope with this new threat, it would serve us all well to consider our own survival plans in this rapidly changing world of uncertain times.

#### Nuclear terrorism will cause global nuclear war, leading to extinction

Sid-Ahmed, Egyptian political analyst for the Al-Ahram newspaper, 2004:

(Mohamed Sid-Ahmed, Egyptian political analyst for the Al-Ahram newspaper, Al-Ahram online, August 26, 2004,http://weekly.ahram.org.eg/2004/705/op5.htm)

A nuclear attack by terrorists will be much more critical than Hiroshima and Nagazaki, even if -- and this is far from certain -- the weapons used are less harmful than those used then, Japan, at the time, with no knowledge of nuclear technology, had no choice but to capitulate. Today, the technology is a secret for nobody. So far, except for the two bombs dropped on Japan, nuclear weapons have been used only to threaten. Now we are at a stage where they can be detonated. This completely changes the rules of the game. We have reached a point where anticipatory measures can determine the course of events. Allegations of a terrorist connection can be used to justify anticipatory measures, including the invasion of a sovereign state like Iraq. As it turned out, these allegations, as well as the allegation that Saddam was harbouring WMD, proved to be unfounded. What would be the consequences of a nuclear attack by terrorists? Even if it fails, it would further exacerbate the negative features of the new and frightening world in which we are now living. Societies would close in on themselves, police measures would be stepped up at the expense of human rights, tensions between civilisations and religions would rise and ethnic conflicts would proliferate. It would also speed up the arms race and develop the awareness that a different type of world order is imperative if humankind is to survive. But the still more critical scenario is if the attack succeeds. This could lead to a third world war, from which no one will emerge victorious. Unlike a conventional war which ends when one side triumphs over another, this war will be without winners and losers. When nuclear pollution infects the whole planet, we will all be losers.

## Uniqueness

### Bipartisan Support Now

#### **New cybersecurity legislation will pass - compromises got new GOP support**

Silverstein, 7/25 – editor-in-chief of EnergyBiz Insider (Ken, “Cyber Security Bill Now Positioned to Pass”, EnergyBiz, 7/25/12, <http://www.energybiz.com/article/12/07/cyber-security-bill-now-positioned-pass>) // EK

Advocates of cyber security legislation have advanced the ball to the point where they might score. A new bill intended to win bipartisan support would offer “incentives” to companies that operate vital infrastructure if they participate with government authorities, which would include getting absolved of any liability. President Obama has come out in favor of the new approach, writing an op-ed in the Wall Street Journal that essentially says that any hacker from anywhere in the world can disrupt critical U.S assets if certain companies have not taken the right steps to address such pitfalls. The time is now to fix the problem, he says, pointing out that water plants in Texas have already been hacked while cyber invaders have also penetrated natural gas pipelines in the United States.   “We need to make it easier for these companies – with reasonable liability protection – to share data and information with government when they’re attacked,” the president writes in the paper. “And we need to make it easier for government, if asked, to help these companies prevent and recover from attacks.”   A recent report by the [U.S. Department of Homeland Security Control Systems Security Program](http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf) says that the number of attacks has jumped from 41 in 2010 to 198 in 2011. Many problems, it adds, could have been prevented using best security practices – things that may elude a private company but which could be resolved by sharing information. So-called spear phishing tactics where employees are tricked into giving out sensitive info to hackers is a prime problem.   About 85 percent of all critical infrastructure assets are owned and operated by private entities, which have an interest in keeping such attacks secret and which do not want to disclose any proprietary information. That’s why the re-write of the cyber security bill would “hold harmless” these companies that collaborate with the federal government – either to divulge attacks or to work with authorities to prevent them. Along those lines, owners of critical infrastructure assets would not be obligated to participate but if they do, they would have much flexibility. “These numbers demonstrate that attackers are increasingly turning their attention to critical infrastructure facilities, and are finding soft targets,” says Brian Ahern, chief executive of [Industrial Defender](http://www.industrialdefender.com/). “Doing nothing about this is like playing with fire, leaving power grids, chemical plants, oil and gas facilities, waters supplies and other key systems at significant risk.” The pending measure defines critical infrastructure as any asset that if brought down would lead to mass casualties, mass evacuation or financial collapse. The power grid fits into that categorization. According to the [General Accountability Office](http://www.gao.gov/new.items/d071036.pdf), the nation’s wires infrastructure is comprised of $1 trillion in assets that entail 200,000 miles of transmission lines. Altogether, over 800,000 megawatts of power serve more than 300 million people. Because the system is now connected to the outside world, it is open to attack. Consider the smart grid that allows utilities and customers to communicate with each other: A nemesis can manipulate the data and disrupt the network — just as a number of smaller but potent viruses have already done. The big one, of course, has been Stuxnet that this government used in coordination with that of Israel and that was intended to diminish the Iranian nuclear program. For their part, utilities are already required under the Energy Policy Act of 2005 to certify with the Federal Energy Regulatory Commission that they have developed robust systems that can continue to generate and deliver power if attacked. To comply, they are describing their potential risks based on historical accounts. Meantime, nuclear operators have their own separate requirements that they follow and that they report to the Nuclear Regulatory Commission.   That earlier law is one reason why some U.S. senators have been wary about new cyber security legislation. That is, they were concerned about redundancy, higher costs and more burdens. And, according to [Senator Lisa Murkowski, R-Alaska](http://www.murkowski.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=AFF7D318-82FB-4715-B267-1100B512AB6D), the “voluntary” aspects of the previously considered measures could later become “mandatory,” which would hamstring companies’ latitude.   As such, Murkowski and other ranking Senate Republicans have pushed for an “information sharing” arrangement between the federal government and industry. It is part of the compromise that is winning bipartisan support – and it could pass both chambers this year, says Murkowski’s office. Provisions tied to how and with whom information is shared would still need to reconciled. But, all such bills now provide liability protection for the use and disclosure of cyber threats.   By all accounts, most companies are increasing their cyber security efforts. But some are going to great lengths while others just don’t have the experience to erect better defenses. By opening the lines of communication with government authorities and eliminating the liabilities for doing so, cyber security advocates say that critical infrastructure would be much better protected.    EnergyBiz Insider is named a 2012 Finalist for Original Web Commentary presented by the American Society of Business Press Editors. The column is also the Winner of the 2011 Online Column category awarded by Media Industry News, MIN. Ken Silverstein has been named one of the Top Economics Journalists by Wall Street Economists.

#### Cyber-security is top of the docket - bipartisan compromise will be reached

Federal Computer Week, 7/24 (“Lawmakers to consider new compromise cybersecurity bill before defense budget”, 7/24/12, <http://fcw.com/articles/2012/07/24/senate-compromise-cybersecurity-bill.aspx>) // SKRG

Several top lawmakers in a July 24 press briefing on Capitol Hill announced a new deal on cybersecurity legislation, and are expected to take up the compromise bill by the end of the week given the urgency of preventing a “cyber 9/11.” ¶ “In terms of urgency, I believe the cybersecurity bill is more urgent,” Lieberman said. “We’re not imagining this threat. We’re being attacked through cyberspace every day. The reality is a lot of the private companies that own critical cyber infrastructure are doing a good job in defending that cyber infrastructure and our country, but a lot of them are not.”¶ “This bipartisan bill is the result of compromise,” Lieberman said at the briefing, where he was flanked by four other bill co-sponsors. “We co-sponsors, to be blunt, gave up some things that we thought were important in our original bill, but given the urgency and seriousness of the cyber threat to our country, we thought it was more important to move forward with a bill that we’re confident will significantly strengthen our cybersecurity.”

#### **The new bill’s designed to get Republicans on board – will be proceed to the Senate with broad support**

Eggerton, 7/24 – Washington Bureau Chief for B&C and editor of the Daily TV Fax (John, “Cybersecurity Bill Backers Say They Think Measure Can Proceed”, Broadcasting & Cable, 7/24/12, <http://www.broadcastingcable.com/article/487678-Cybersecurity_Bill_Backers_Say_They_Think_Measure_Can_Proceed.php>) // EK

The five chief Cybersecurity bill backers said Tuesday they were confident that the Senate would be able to at least consider a new, compromise cybersecurity bill, saying they had made concessions on that bill sufficient to get past at least that next hurdle.¶ Those five are Senate Commerce Committee Chair Jay Rockefeller IV, (D-W.Va.), Homeland Security and Governmental Affairs Committee (HSGAC) Chairman Joe Lieberman, (Ind.-Conn.), HSGAC ranking member Susan Collins (R-Maine), Select Intelligence Committee Chairman Dianne Feinstein, (D-Calif.), and Federal Financial Management Subcommittee Chairman Tom Carper (D-Del.).¶ They have not been shy about advertising the fact that the bill has been modified to try and draw Republican support. President Barack Obama, in an op-ed in the Wall Street Journal last week, argued that protecting cybersecurity had to be a national priority.¶ A compromise version of the bill was introduced last week. "The bill creates a "public-private partnership" to establish cybersecurity standards for critical infrastructure," then provides some immunity from liability for those who volunteer to meet those standards.¶ According to Rockefeller's office, the bill will also "Incentivize the Adoption of Voluntary Cybersecurity Practices; Improve Information Sharing While Protecting Privacy and Civil Liberties; Improve the Security of the Federal Government's Networks; Strengthen the Cybersecurity Workforce; Coordinate Cybersecurity Research and Development."¶ Senate Majority Leader Harry Reid has scheduled floor time for the cybersecurity bill, which did not sit well with Republican John McCain (R-Ariz.). In a floor statement, he questioned the apparently prioritizing of that bill over the Defense Authorization bill. "Just last week, the Majority Leader stated that Senate consideration of a controversial and flawed bill on cybersecurity – a bill that has not been considered in the regular order – is more important and of a higher national security priority than the defense authorization bill. I respectfully but vehemently disagree with that statement," he said.

#### **Cyber-security will pass before August recess – compromise**

Mills, 7/19 – Senior writer at cnet.com (Elinor, “Senators soften latest cyber security measure”, 7/19/12, cnet.com, <http://news.cnet.com/8301-13578_3-57476215-38/senators-soften-latest-cyber-security-measure/>) // SKRG

In a move to get cybersecurity legislation approved before the Senate recess, Sen. Joseph Lieberman (I-Conn.) and four colleagues introduced a modified version of their proposed cybersecurity legislation that adds privacy protections for consumers and removes government mandated security standards.¶ A compromise was needed in order for the measure to get at least 60 votes in the Senate. Lieberman acknowledged that the amended measure was watered down some, but suggested that even weakened legislation if it gets passed is better than none. "While the bill we introduced in February is stronger, this compromise will significantly strengthen the cybersecurity of the nation's most critical infrastructure and with it our national and economic security," wrote in a statement published on his Web site.¶ The measure will be debated in the Senate next week as lawmakers try to get a cybersecurity bill passed before the August recess. Lawmakers are hoping new legislation will improve the ability of the government and power companies, utilities and other firms running critical infrastructure in the country to keep hackers and cyber threats out of their networks. The emergence of malware like Stuxnet and Flame; reports of holes in SCADA software; and data theft and attacks targeted at gas pipelines and other companies have spooked Congress.

#### **Compromise and momentum in Congress**

Politico, 7/17 (“Cybersecurity bill shows signs of life in Senate”, 7/17/12, <http://www.politico.com/news/stories/0712/78629.html>) // SKRG

Key lawmakers are racing to broker a compromise on a Senate cybersecurity bill, insisting that floor action is still possible as early as next week.¶ The major players recognize they aren’t likely to find a deal that will resolve all lawmakers’ concerns before the real debate begins. But with limited time until the August recess, Sen. Joe Lieberman (I-Conn.) signaled he could introduce a new cybersecurity measure that includes a middle-of-the-road compromise on critical infrastructure while he and others reiterated a hope that members could work out remaining disagreements while a bill is on the floor.¶ “I think things are moving, yes, and I think things are generally moving well — and they’ll have to because we have to get it to the floor in the next 10 days,” said Sen. Jay Rockefeller (D-W.Va.), one of the original sponsors of Lieberman’s effort. “I think once it’s brought to the floor, everything will get resolved.”

### Obama Pushing

#### **Cybersecurity will pass – Obama focused now**

Corrin 7/24 – writer for Federal Computer Week (Amber, writer for Federal Computer Week, FCW.com, http://fcw.com/articles/2012/07/24/senate-compromise-cybersecurity-bill.aspx //EW

In a July 19 Wall Street Journal opinion [piece](http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html?mod=WSJ_Opinion_LEADTop), President Barack Obama urged Senate action on cybersecurity, urging Capitol Hill lawmakers to pass comprehensive legislation. Describing a recent cyber-attack drill exercise, Obama called for cybersecurity to be a top priority, and to pass laws that would enable information-sharing, address security concerns and protect civil liberties. “It doesn’t take much to imagine the consequences of a successful cyber-attack. In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home,” he wrote. “This is the future we have to avoid. That’s why my administration has made cybersecurity a priority, including proposing legislation to strengthen our nation’s digital defenses. It’s why Congress must pass comprehensive cybersecurity legislation.” Obama also said he would veto any cybersecurity legislation lacking strong privacy and protections for civil liberties.

Obama pushing – Wall Street Journal op-ed proves
VOA News, 7/20/12 “Obama Urges Passage of Cybersecurity Bill” Voice of America News, <http://www.voanews.com/content/president-obama-urges-passage-of-cybersecurity-bill/1441762.html> //EW

U.S. President Barack Obama is urging lawmakers in the U.S. Senate to pass a measure that will boost the nation's defenses against possible cyber-attacks. In an opinion piece published in[***The Wall Street Journal***](http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html?mod=WSJ_Opinion_LEADTop) Friday, Obama says "foreign governments, criminal syndicates and lone individuals are probing our financial, energy and public safety systems every day." "It would be the height of irresponsibility to leave a digital backdoor wide open to our cyber adversaries," the president added. The measure, known as the Cybersecurity Act of 2012, would create a public-private partnership that would set cybersecurity standards for critical infrastructure, such as water and power systems, and permit information-sharing between the private sector and the federal government.

### Will Pass - Generic

#### **Cybersecurity has support and is moving forward**

Dayen 7/27 – political blogger at FDL, known nationally as “D-Day” (David, “Cybersecurity Bill on Fast Track in Senate, With Amendments Upcoming”, FireDogLake, 7/27/12, <http://news.firedoglake.com/2012/07/27/cybersecurity-bill-on-fast-track-in-senate-with-amendments-upcoming/>) // EK

The Senate [easily advanced](http://thehill.com/blogs/hillicon-valley/technology/240605-senate-advances-bill-to-bolster-cybersecurity-defenses-in-84-11-vote) a motion to proceed on their version of a cybersecurity bill yesterday, by an 84-11 vote. Clearly this bill, a separate version of which has already passed the House, has a broad degree of support. As if on cue yesterday, the head of the National Security Agency Keith Alexander, [warned about increasing cyberattacks](http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html) on the US, which this bill would purport to stop:¶ “The top American military official responsible for defending the United States against cyberattacks said Thursday that there had been a 17-fold increase in computer attacks on American infrastructure between 2009 and 2011, initiated by criminal gangs, hackers and other nations [...]¶ General Alexander, who rarely speaks publicly, did not say how many attacks had occurred in that period. But he said that he thought the increase was unrelated to the release two years ago of a computer worm known as Stuxnet, which was aimed at taking down Iran’s uranium enrichment plant at Natanz.¶ When the worm inadvertently became public, many United States officials and outside experts expressed concern that it could be reverse-engineered and used against American targets. General Alexander said he saw no evidence of that.”¶ The comments were made at the Aspen Institute but they were pretty clearly intended to pressure folks on Capitol Hill to progress the cybersecurity bill. And it worked.¶ The bill will work through amendments next week, and Harry Reid agreed to a relatively open amendment process for the time being. Al Franken, one of the leaders in improving the bill from its invasive, privacy-destroying CISPA shell, voted to advance the bill, praising the [changes that have been made](http://news.firedoglake.com/2012/07/24/cybersecurity-bill-on-track-for-senate-floor-after-privacy-protections-added/). But Franken also said that he would introduce an amendment that would deal with provisions to grant too much leeway on Internet service providers to openly monitor private communications and deploy countermeasures on those users based on the information. The shorthand for this is the “monitoring and countermeasures authorities” in the bill. Here’s an excerpt from Franken:¶ “And after a lot of hard work and a lot of conversations, the sponsors made a series of changes to the bill that are major, unequivocal victories for privacy and civil liberties. Now, the bill is still not perfect. Far from it. But I can say with confidence that when it comes to protecting both our cybersecurity and our civil liberties, the Cybersecurity Act of 2012 is the only game in town [...]¶ Right now, the Cybersecurity Act and the President’s proposal are not in line with each other—because unlike the President’s proposal, the Cybersecurity Act does give ISPs and other companies a brand new right to monitor communications and to deploy countermeasures. That right is very broad. So broad that if a company uses that power negligently to snoop in on your email or damage your computer—they will be immune from any lawsuit.¶ I plan to offer an amendment to delete these new monitoring and countermeasures authorities and bring this bill in line with the President’s proposal. And I hope that my colleagues here in the Senate will join me in passing this amendment—seven of my colleagues have already indicated that they will cosponsor this amendment.”¶ The President has also said that the Senate bill “lacked some of the key provisions of earlier bills,” though I believe he’s talking about mandates on critical operators of US infrastructure to improve their cybersecurity systems (those standards are now voluntary).¶ Some experts have expressed [reluctance to pass this bill](http://www.dailykos.com/story/2012/07/26/1113995/-Cybersecurity-will-be-considered-in-the-Senate-next-week) out of the Senate, for fear that the bad CISPA provisions get inserted in conference. That’s a legitimate concern, although gridlock is more likely, as the Chamber of Commerce objects to the Senate version, as do House Republicans. But on one of these bills that has a lot of momentum behind it, Franken is clearly trying to do the best he can to ameliorate any issues that may arise. We’ll see if his amendment can pass.

#### **Cybersecurity is moving closer to a vote, but still faces challenges**

Fitzpatrick, 7/26 – reporter at Mashable’s New York headquarters, covers politics, international affairs, social media, and technology (Alex, “Cybersecurity Bill Inches Closer to Passing”, Mashable, 7/26/12, <http://mashable.com/2012/07/26/cybersecurity-bill-senate/>) // EK

The Lieberman-Collins cybersecurity bill moved one step closer to passing Thursday afternoon. The Senate voted in favor of a motion to proceed 84-11 after a lengthy and contentious debate. The bill now faces additional changes before being brought up for a full vote.¶ The Cybersecurity Act, or CSA, is the Senate’s attempt to address cybersecurity reform. Senate leadership considers such reform a priority for the current term that ends in January.¶ As written, the CSA would set up an optional program where businesses deemed critical to the national infrastructure (such as power grids) would be asked to meet cybersecurity standards set by a group of government agencies. It would also establish a protocol for government agencies and businesses to share cybersecurity threat information with one another.¶ The bill originally called for government-mandated cybersecurity standards for key infrastructure with no opt-out. Senate Rebublicans considered that to be an example of excessive regulation. The opt-in compromise was the key factor in reducing Republican opposition.¶ The CSA has support from some technology companies including Cisco and Oracle, while IBM is against it. Additionally, Internet privacy groups such as the [Electronic Frontier Foundation](https://www.eff.org/deeplinks/2012/03/dangerously-vague-cybersecurity-legislation) have warned that some of the bill’s language is dangerously vague.¶ Should the CSA eventually pass the Senate, it will move to the House, which has already passed a very different cybersecurity bill – the Cyber Intelligence Sharing and Protection Act, or CISPA. Discrepancies between the bills would have to be worked out by the two chambers before they would be able to send it to President Obama.¶ The differences between the Senate and House bills?¶ CISPA is focused on information sharing between the government and businesses, and includes no federally-mandated cybersecurity standards. It’s also opposed by the White House. President Obama has given a tentative thumbs-up to the Senate’s bill, with the caveat that the latest version dropped “some of the key provisions of earlier bills.”

## Internal Links

### Delay Internal Link

**Deadline for legislation is approaching now**Wilhelm 7/21 – writer for TheNextWeb (Alexander, “The Senate Cybersecurity showdown is approaching: A preview” thenextweb.com, <http://thenextweb.com/us/2012/07/21/the-senate-cybersecurity-showdown-is-approaching-a-preview/> //EW

Now, in the Senate, the leading bill for some time has been a law put forth by Senator Lieberman, which includes the standards that the House abhors. There has been work done by Senators Kyl and Whitehouse to drive towards a compromise. There is a deadline hanging over all of this: Congress is only in session for so long. And this Congress is moving towards an election. Senator Lieberman stated publicly that unless a bill was voted on and passed in July, nothing could get done with cybersecurity this session of Congress. Now, to the coming collision. There are only 11 days left in July. If the Senate cannot vote and pass a bill, that will then be reconciled with the House bill, in that time period, progress could be essentially stuck until after the elections, when a new Congress will be sworn in.

### Bipartisan Support is Key

#### Cybersecurity security bill needs bipartisan support – gun control amendment weakened passage

Miller, 7/27/12 – Washington Bureau Chief (Kevin, “Congress Pushing for Cyber Attack Defense”, Portland Press Herald, July 27) [http://www.pressherald.com/news/congress-pushing-for-cyber-attack-defense\_2012-07-28.html //](http://www.pressherald.com/news/congress-pushing-for-cyber-attack-defense_2012-07-28.html%20//) ML

Because the assailants' weapons were computers and malicious software, not bombs or guns, the vast majority of those 200 intrusions attracted little attention outside the U.S. Department of Homeland Security and the targets themselves. But as the number of cyber attacks rises along with their level of sophistication, members of Congress and federal officials are pushing hard to strengthen the nation's defenses against computer-borne attacks that could cause economic mayhem. "It is not a matter of whether a cyber attack will occur. The only question is when it will occur," Sen. Susan Collins, R-Maine, said earlier this week during a Washington press conference. Collins, who is a member of the Homeland Security Committee, is among the lead sponsors of a bill expected to come up for a vote in the Senate on Monday after years of discussion and months of negotiations with industry, civil libertarians and military officials. The current version of the bill is admittedly weaker than its sponsors had hoped, placing an emphasis on information sharing between the private sector and government rather than government mandates. Even so, the bill's success is not assured. Amendments on the Senate floor -- such as one to ban high-capacity ammunition magazines in response to the movie theater shooting in Colorado -- could weaken the bipartisan support needed to reach 60 votes. And aspects of the measure will likely face opposition in the more conservative House. But supporters argue it will take an important step forward in protecting the country against debilitating cyber attacks on the computer systems that keep the electric grid functioning, phones working and money flowing in the age of e-commerce. "The danger of cyber attacks against the United States is clear, present and growing, with enemies ranging from rival nations to cyber-terrorists to organized criminal organizations to rogue hackers sitting at computers almost anywhere around the world," said Sen. Joseph Lieberman, I-Conn, chairman of the Senate Homeland Security Committee and a bill co-sponsor

#### Bipartisanship is key to passing cyber security legislation - Senate Majority leader agrees

Biesecker 6/13/12 – 5 year reporter for Defense Daily on homeland security (Calvin, “Reid Says Cyber Legislation Needs Bipartisan (Republican) Support”, Defense Daily, June 13) [http://www.defensedaily.com/free/18068.html //](http://www.defensedaily.com/free/18068.html%20//) ML

Democrats and Republicans have more work to do to bridge differences in creating cyber security legislation that can pass the Congress, Majority Leader Harry Reid (D-Nev.) said on the Senate floor yesterday. “Everyone knows this Congress can’t pass laws that don’t have broad, bipartisan support,” Reid said. “So, we’ll need to work together on a bill that addresses the concerns of lawmakers on both sides of the aisle.” Reid said that before broader bipartisanship can be achieved in Congress, “more of my Republican colleagues need to start taking this threat seriously.” Cybersecurity vulnerabilities and threats threaten the nation’s national and economic security, Reid said. The House has already passed several cyber related bills this year, although with lukewarm bipartisan support (*Defense Daily*, April 30). That legislation is focused on improved information sharing between the private sector anerd the intelligence community but avoids measures the White House and many Democrats want to give the Department of Homeland Security authorities to help set and then enforce minimum cyber security standards for critical infrastructure, most of which is in the private sector. In the Senate, Senators Joseph Lieberman (I/D-Conn), Susan Collins (R-Maine), Jay Rockefeller (D-W. Va.), and Dianne Feinstein (D-Calif.) have introduced a bill that would create authorities for DHS to enforce minimum cybersecurity standards in the private sector. However, competing legislation from seven Republican senators would not give DHS such enforcement authority and would make compliance with any best practices voluntary. Reid said that Republicans need to “participate productively in the conversation, instead of just criticizing the current approach.” He added that “There is room for more good ideas on the table.”

#### Bipartisan Support is key to passing the Cybersecurity legislation

Levin 2/8 (Mintz, “Legislative Update – Cybersecurity”,  2/8/2012, <http://www.jdsupra.com/post/documentViewer.aspx?fid=0a38a729-5e76-4261-8263-e371f4cbff87>)

As the 112th Congress gets underway, many continue to feel that partisan gridlock will block movement on significant legislation, leaving congressional activity to legislation that doesn’t require a heavy lift. However, in what many view as a surprising move, Congress appears ready to address one of the most complicated issues on Congress’s agenda – cybersecurity.  There are ample disagreements in approach, but a serious effort is underway to bridge these differences and get a bill passed.  There is a strong push for information sharing between the public and private sectors as a means to protect against cyber attacks.  This concept of information sharing is a main component of a House cyber security bill that was [marked up last week](http://techland.time.com/2012/02/06/fbi-hacked-while-congress-ponders-cybersecurity-legislation/), and was also the topic of an[opinion piece](http://www.politico.com/news/stories/0112/72120.html)written by a group of Senate Republicans.  The authors – Sens. Hutchison, Grassley, Chambliss, and Murkowski – outline their approach to cybersecurity and stress that it is important for the Administration and Congress to work together to ensure a bipartisan solution.  In addition to information sharing, the overall balance between government intelligence needs and private business needs is a priority for both House and Senate cybersecurity legislation.  There have been reports that a classified briefing between Administration officials and Senators [took place last week](http://www.businessweek.com/news/2012-02-06/cybersecurity-bill-in-u-s-senate-falls-behind-reid-schedule.html)to discuss the urgency of passing a cybersecurity bill this year. A bill introduced by Cybersecurity Subcommittee chairman Dan Lungren (R-CA) and Homeland Security Committee chairman Peter King (R-NY) has drawn support from key Democrats, and will likely also gain support from Republicans because it is intended to facilitate information sharing between the government and private sector.  The Promoting and Enhancing Cybersecurity Act, H.R. 3674, represents a blend of incentives and new regulation.  This bill [was marked up on Wednesday, February 1](http://homeland.house.gov/markup/subcommittee-markup-hr-3674), and Chairman Lungren offered an amendment in the nature of a substitute.  There are other House proposals in the works, but it is unclear whether the House will follow the Senate’s lead and attempt to combine them into one comprehensive measure.  Rep. Mac Thornberry (R-TX), has indicated that the House is waiting to see what the Senate does and is aiming for getting cybersecurity bills on the floor by the end of February or beginning of March.  Rep. Thornberry has also noted that successful cybersecurity legislation should be focused on emerging threats and encourage both the public and private sector to practice good cyber hygiene and reduce clutter in their networks.

### Rider Internal Link

#### Normal means makes plan an amendment to cybersecurity legislation - destroys its passage

Romm 7/27/12 – Technology Reporter for Politico (Tony, “Amendments are Critical Hurdles in Cyber Debate”, Politico Pro, July 27) [http://www.politico.com/news/stories/0712/79051.html //](http://www.politico.com/news/stories/0712/79051.html%20//)

The fate of the Senate's cybersecurity reform measure now hinges on amendments — and bill sponsors, the White House and top Republicans have all drawn their lines in the sand. The challenge for the Cybersecurity Act of 2012 after a key procedural vote Thursday is whether a growing number of amendments can resolve enough differences to attract GOP support in the Senate — and, ultimately, the House, too — while not completely removing the teeth that Democrats and the Obama administration think is essential to protect the nation from cyber threats. Some Republicans are angling for a broad set of revisions to the critical infrastructure and information sharing bill, and a bloc of GOP members plans to pitch its own cybersecurity measure — the SECURE IT Act — as an amendment during the forthcoming floor debate. That rival bill leaves out any mention of cybersecurity protections for critical infrastructure, a change to the legislation that the White House indicated Thursday it would not support. Other amendments lawmakers are promising could add new provisions to the bill meant to improve energy-grid security or require tech companies to disclose when they have been breached by hackers. There are also members angling to amplify the privacy safeguards in the measure, or revise its section on liability protection. The coming debate over those changes and others is going to be critical for the bill’s backers as they canvass the chamber for votes and seek passage before the August break. Senate Democratic Leader Harry Reid already has made clear he will permit a broad swath of amendments — so long as they're germane — as sponsors try to cobble together a compromise that can clear the Senate and yet still prove appealing to the House. The list of amendments to be debated is still not finalized and can change. But the speeches, the letters from industry and the posturing on the floor over the past few days have provided an early glimpse of what still remains a slog ahead for the Senate. Sen. Kay Bailey Hutchison, for one, laid out a series of revisions that could make the bill more palatable to her allies. That could include more explicit provisions making the critical-infrastructure sections voluntary, a standards-setting process led by NIST and not the Department of Homeland Security, and more robust liability protections for business, among other things. However, Hutchison pledged that she and her colleagues also would unveil their cybersecurity counterplan, the SECURE IT Act, as an amendment in the form of a substitute, in addition to offering the different provisions of that bill as individual amendments. The full SECURE IT Act does not try to bring new security procedures to entities deemed critical infrastructure. Other members are angling to expand the bill's liability protections in a way to appeal to more owners of power plants, water systems and other essential entities. Sen. Joe Lieberman suggested that could come from Sens. Jon Kyl (R-Ariz.) and Sheldon Whitehouse (D-R.I.), though the two lawmakers have remained mum on their work — and no one has publicly shared any text.

### Political Capital is Key (Old)

#### Obama needs to use political capital and push cybersecurity legislation

Newmeyer 3/12 - assistant Professor in the Center for Hemispheric Defense Studies at

the National Defense university (Kevin, “Who Should Lead U.S. Cybersecurity Efforts?”, March 2012) [http://www.ndu.edu/press/lib/pdf/prism3-2/prism115-126\_newmeyer.pdf //](http://www.ndu.edu/press/lib/pdf/prism3-2/prism115-126_newmeyer.pdf%20//) ML

Cybersecurity concerns have only grown with the expansion of digital technology into all aspects of daily life and daily government operations. President Obama in the International Strategy to Secure Cyberspace stated that cybersecurity is part and parcel of everyday life for all Americans and much of the world. Maintaining the status quo of scattered responsibilities and patchwork policy solutions is not only poor governance but also potentially places the Nation’s critical assets at risk. Establishing a strong DCYBER at a Cabinet-equivalent level would provide the necessary leadership within the Federal Government. The Department of Homeland Security would continue to play an important role in protecting civilian governmental systems and coordinating with the private sector. DOD has already taken several steps to improve its capabilities for action, and senior leaders are addressing cybersecurity in a responsible manner. Congress and the President need to demonstrate the political leadership and expend the political capital to make the needed changes in legislation and structure on the domestic front. Waiting for a perfect solution to appear is not an option. Decisive action is required now

#### Political Capital is key to passing the Cybersecurity battle

Newmeyer, 12-Assistant Professor of National Security Affairs (Kevin P., “Who Should Lead U.S. Cyber Security Efforts?”, NDU Press, March 2012, <http://www.ndu.edu/press/us-cybersecurity-efforts.html#Author>

None of the options available is perfect. While several bills have been introduced to Congress over the past several years, progress has been slow. Cybersecurity must compete on the legislative and executive agenda with other significant issues. Health care, financial reform, public debt, and ongoing wars continue to dominate the news and the legislative agenda. It is clear, however, that current structures are insufficient to achieve cybersecurity. Repeated studies and reviews have yielded remarkably similar recommendations. The centralization of cybersecurity policy initiatives in the Executive Office of the President remains a leading contender; it offers the power of the Presidency to achieve cross-organizational agreement within the executive branch. Strong leadership is clearly essential for achieving sufficient cybersecurity. The most significant limitations on a White House cyber czar center on his authority to compel compliance from the disparate executive branch agencies. Without a clear establishment of authorities in legislation, the individual would only have the referent power and authority granted by his standing with the President. Lack of strong backing from the President would constrain his effectiveness in executing his mission. To be effective, the position needs a legal structure solidified in legislation similar to the DNI, which would imply greater congressional oversight. In examining the various Cabinet-level department options, it is difficult to argue that any of them could overcome the problems of the current structure. The present system has obviously failed as repeated penetration of DOD and other governmental systems has entailed the loss of terabytes of data. Placing the responsibilities in DOD presents numerous challenges. While defending systems from foreign attack could become a defense mission, the department has little experience with regulatory matters and procedures. The civil liberty implications of using the military in domestic intelligence activities are enormous. The Posse Comitatus Act would have to be significantly revised to allow for military activity beyond training inside the United States. This would cause civil liberties debates greater than those over the USA PATRIOT Act. Placing the military in charge of cybersecurity for civilian systems would not be politically viable. Creation of a new department to focus on cybersecurity would achieve many of the objectives listed in the CSIS report. It would allow for collection of the many siloed activities currently under DOD, Homeland Security, Commerce, and State. The establishing legislation would have to clarify authorities, regulatory powers, and relationships with the existing departments. The budget and nomination process provides for the needed congressional oversight. The challenges to a new department are daunting. Starting something in Washington at the Presidential level normally requires a dramatic trigger event along the lines of 9/11 or an indefatigable champion willing to expend the political capital necessary to carry the battle. To date, this has not occurred on the cyber front. Other issues have occupied the political space and pushed cybersecurity to the rear. A new department would also face significant growing pains. In the current budget and political climate, it is unlikely to garner the support needed in Congress. While it may provide the best operational and constitutional solution, it is the least likely in the near to mid term. Retaining cybersecurity leadership within the Department of Homeland Security is the most likely alternative among the Cabinet level organizations. As previously discussed, the department has the basic regulatory functions necessary and significant experience in cybersecurity issues. The relationship with DOD has improved significantly in cybersecurity and a cooperative strategy is in place. What Homeland Security lacks in the cybersecurity leadership role is consistent Presidential and congressional focus. It has a coordination role given to it by the President in a series of decision documents, but coordination is not control. Homeland Security cannot truly compel other departments to adhere to its policies and decisions. The department itself is still growing and developing. Less than 10 years old, it does not have the longstanding policies and cultures of the Department of State or DOD. Congress has not helped the problems at the department and must clarify its committee jurisdiction issues regarding not only cybersecurity but also all of the missions assigned to Homeland Security. At present, more than 80 committees have a role in the department’s oversight.18 The other significant hurdle for Homeland Security is building the human capital necessary to establish and implement policy and operations in support of cybersecurity. The department has announced ambitious plans for growing its cyber forces, but it will not be easy. Recruiting and retaining these specialists will be a constant challenge. Congress and the President need to demonstrate the political leadership and expend the political capital to make the needed changes in legislation and structure on the domestic front. Waiting for a perfect solution to appear is not an option. Decisive action is required now.

## Impacts

### Turns Case – Cybersecurity Key to Infrastructure

#### Cyber-attacks turn case- destroys infrastructure

Popular Mechanics 9- (Glenn Derene, “How Vulnerable is U.S. Infrastructure to a Major Cyber-Attack?”, Popular Mechanics, 10/1/09, http://www.popularmechanics.com/technology/military/4307521)//JY

The next world war might not start with a bang, but with a blackout. An enemy could send a few lines of code to control computers at key power plants, causing equipment

to overheat and melt down, plunging sectors of the U.S. and Canadian grid into darkness. Trains could roll to a stop on their tracks, while airport landing lights wink out and the few traffic lights that remain active blink at random. In the silence and darkness, citizens may panic, or they may just sit tight and wait for it all to reboot. Either way, much of the country would be blind and unresponsive to outside events. And that might be the enemy's objective: Divert America's attention while mounting an offensive against another country. Pentagon planners have long understood the danger of cyber attacks on U.S. military networks. Indeed, the Defense Department's Global Information Grid is one of the most frequently targeted computer networks on Earth. But the cat-and-mouse game of information espionage on military networks is not the only digital threat that keeps national-security experts up at night. There is a growing concern over the vulnerability of far more tangible assets essential to the economy and well-being of American citizens. Much of the critical infrastructure that keeps the country humming--water-treatment facilities, refineries, pipelines, dams, the electrical grid--is operated using a hodgepodge of technologies known as industrial control systems. Like banks and telecommunications networks, which are also generally considered critical infrastructure, these industrial facilities and utilities are owned by private companies that are responsible for maintaining their own security. But many of the control systems in the industrial world were installed years ago with few or no cyber-security features. That wasn't a big problem when these systems were self-contained. But in the past two decades, many of these controls have been patched into company computer networks, which are themselves linked to the Internet. And when it comes to computer security, a good rule of thumb is that any device that is computer-controlled and networked is vulnerable to hacking. Bad-guy hackers pulling the plug on public utilities is a common theme of Hollywood films, including 2007's Live Free or Die Hard, but such scenarios present more than a mere fictional scare to U.S. intelligence officials. According to Melissa Hathaway, cyber-coordination executive for the Office of the Director of National Intelligence, the list of potential adversaries in a cyber attack is long, ranging from disgruntled employees to criminals to hostile nations. Most experts agree that China and Russia routinely probe our industrial networks, looking for information and vulnerabilities to use as leverage in any potential dispute. James Lewis, a cyber-security expert for the policy think tank Center for Strategic and International Studies (CSIS), says that although cyber warfare couldn't cripple the U.S., it could serve as an effective military tactic. "If I were China, and I were going to invade Taiwan," he says, "and I needed to complete the conquest in seven days, then it's an attractive option to turn off all the electricity, screw up the banks and so on." Could the entire U.S. grid be taken down in such an attack? "The honest answer is that we don't know," Lewis says. "And I don't like that answer." Ghosts in the Machine In January 2008, senior CIA analyst Tom Donahue dropped a bombshell on a small conference of government officials and power-company engineers from the U.S. and Europe. He told them that extortionists had managed to hack into utilities in multiple regions outside the United States and disrupt power equipment. "In at least one case," he said, "the disruption caused a power outage affecting multiple cities." The CIA has been highly secretive about the incident, and Donahue would not discuss where the blackouts occurred or what companies were affected. But he admitted that the CIA had no idea who had perpetrated the attacks. Hackers had shaken down a public utility, it seems, and had gotten away with it. Some security professionals think that government officials have been guilty of as much drama-mongering on the issue as Hollywood has. "Honestly, I think the threat is overblown," says Bruce Schneier, author of Schneier on Security. "The risks today are due more to errors than to malicious intent." He sees Donahue's story as nothing more than a tenebrous rumor. Nevertheless, Schneier thinks vulnerabilities in infrastructure will eventually become a real national-security threat. The problem is that the errors that Schneier refers to can cause bad things to happen. Much of computer hacking is predicated on exploiting glitches in commonly used systems. Such exploits on a Windows PC are irritating, but at a nuclear facility, they can be unnerving. In August 2006, a glitch shut down the Browns Ferry nuclear power plant in northern Alabama. Plant administrators lost control of recirculation pumps on one of the plant's reactors because of excessive data traffic on the control-system network. The plant was forced to go offline temporarily. Nuclear plants are designed to shut down in the event of major malfunctions to prevent a Chernobyl-style catastrophe. But they also generate almost 20 percent of U.S. power. What if a hacker exploited a coding error in a cooling system to shut down a sizable piece of the nation's power supply? Incidents of digital malfunctions that cause danger to human life are rare, but such events have happened. In June 1999, in Bellingham, Wash., shortly before a routine delivery of gasoline by the Olympic Pipe Line Co., a worker updated a database for the company's pipeline computer-control system. According to a report by the National Transportation Safety Board, a simple typo in the database caused the system to fail, disabling remote control for the pipeline's operators, 98 miles away in Renton, Wash. Pressure began to build in the line, so the operator issued a command to open a secondary pump to relieve it, but the system was unresponsive. A weak point in the pipeline ruptured, releasing 237,000 gal of gasoline into nearby Whatcom Creek. An hour and a half later, the gasoline ignited. The ensuing fireball scorched more than a mile of riverbank, killing three people, including two 10-year-old boys, and damaged the city's water-treatment facility. Read more: How Vulnerable is U.S. Infrastructure to a Major Cyber Attack? - Popular Mechanics

#### Cyber-terrorists can destroy U.S. infrastructure- turns case

Homeland Security News Wire 11- (Ben Frankel, “Cyber attacks on critical infrastructure reach U.S.”, Homeland Security News Wire, 11/21/11, http://www.homelandsecuritynewswire.com/cyber-attacks-critical-infrastructure-reach-us-bf?page=0,0)//JY

Two recent cases of debilitating cyber attacks on control systems of infrastructure assets made the headlines: In the spring and summer of 2010, Israel unleashed the Stuxnet malware on uranium-enriching centrifuge farms in Iran, causing about a third of Iran’s active centrifuges to explode, disrupting the others, and slowing down Iran’s march to the bomb. Last week, Israel sent another malware, the Duqu, into Iran’s military-industrial complex to disrupt Iran’s military programs. This time, on 12 November, the malware caused the sophisticated Sejil-2 ballistic missile to explode while it was being shown to a group of scientists and top military commanders, among them Gen. Hassan Tehrani Moghaddam, the founder of Iran’s missile programs. The explosion, which killed sixteen other members of the Islamic Revolutionary Guard Corps, occurred at the Alghadir military complex near city of Bidganeh. Reports say that missile exploded while Gen. Moghaddam was describing to the group gathered around the missile the features of a new warhead for the missiles, a warhead that could carry a nuclear payload. The New York Times [reports](http://www.nytimes.com/2011/11/15/world/middleeast/iran-mourns-missile-commander-killed-in-blast.html?_r=1&ref=robertfworth) that the explosion was so powerful, it was heard twenty-five miles away in Tehran and shook windows in many towns in the area, leading some Iranian to believe that and Israeli or American attack on Iran’s nuclear facilities had began (for more on the Alghadir explosion, see this [report](http://www.debka.com/article/21496/) in the not-always-reliable Debka. “May there be more like it,” Israeli defense minister Ehud Barak [said](http://www.jpost.com/IranianThreat/News/Article.aspx?id=245467) obliquely when asked last Sunday about the explosion). For a good discussion of Israel cyberwar efforts, see Eli Lake, “Israel’s Secret Iran Attack Plan: Electronic Warfare,” [Daily Beast](http://www.thedailybeast.com/articles/2011/11/16/israel-s-secret-iran-attack-plan-electronic-warfare.html) (16 November 2011) Note that the Mossad’s killing of Moghaddam was a coup equal in its audacity and operational brilliance to the killing of Hezbollah’s military leader Imad Moughnia in Damascus in February 2008. Both stayed out of the public eye and were surrounded by very tight security (the New York Times [reports](http://www.nytimes.com/2011/11/15/world/middleeast/iran-mourns-missile-commander-killed-in-blast.html?_r=1&ref=robertfworth) that “Because of his important role, General Moghaddam had one of the strongest protection details in the country, and it was supervised by Ayatollah Khamenei”). Most critical infrastructure is civilian, not military, and events in Springfield Illinois should give us a taste of what a cyber attack on civilian critical infrastructure can do. At the beginning of November, a water pump in Springfield, Illinois burnt out and stopped functioning. The pump was destroyed after it was turned on and off repeatedly, by remote commands, over a 1-day period. The utility operating the pump noticed that the pump was behaving strangely in the weeks leading to its destruction. Joseph Weiss of [Applied Control Solutions](http://realtimeacs.com/), and author of [Protecting Industrial Control Systems from Electronic Threats](http://www.momentumpress.net/books/protecting-industrial-control-systems-electronic-threats), [told](http://www.theregister.co.uk/2011/11/17/water_utility_hacked/) the Register that a report, issued on 10 November by Illinois authorities, said that the hackers who took control of the pump and then destroyed it used an IPaddress in Russia. The hackers managed to penetrate the water district’sSCADA systems (Weiss provided more details in [ControlGlobal.com](http://community.controlglobal.com/content/water-system-hack-%E2%80%93-system-broken)). “This is really a big deal, and what’s just as big a deal is what isn’t being said or isn’t being done,” Weiss said. “What the hell is going on with DHS? Why aren’t people being notified?” Weiss also said that the hackers who attacked the Illinois water utility could have obtained passwords for many other customers of the SCADAmanufacturer, possibly leading to other industrial facilities now being susceptible to attack. Some of these facilities may already have been breached. In this light it is unsettling to note these two stories: a [report](https://infosecisland.com/blogview/18244-South-Houstons-Water-Supply-Network-Hacked.html) inInfosecIsland that a water supply network in South Houston, Texas, has been successfully hacked recently, and this [report](http://www.northjersey.com/topstories/westmilford-hewitt-newfoundland/Homeland_Security_to_look_into_attacks_on_West_Milford_water_sewer_services.html) in NorthJersey.com about how water and sewagew facilities in West Milford have been repeatedly compromised. Which brings us back to Stuxnet. “Despite [DHS’s] reassurances, online security specialists are already drawing parallels between the Illinois attack and the Stuxnet virus that impacted Iranian nuclear facilities in 2010,”Slashgear [reports](http://www.slashgear.com/us-utility-sabotage-blamed-on-russian-hackers-20196725/). These security experts are right. Most of the U.S. critical infrastructure – both the 85 percent of that infrastructure which is in private hands, and the 15 percent which is run by government agencies – is run by computers which are connected to the Internet. This makes them susceptible to cyber attacks. Stuxnet and Duqu prove that cleverly designed malware can take over control systems of infrastructure assets and then sabotage these control systems and the assets they monitor and run. A few days ago the control system of a water pump in Illinois was taken over by a hacker’s remote command, and then deliberately destroyed. What critical infrastructure facilities will hackers – nerdy teenagers, terrorists, or intelligence operatives of other nations – target next?

#### Cyber-attacks will target U.S. infrastructure- includes transportation

ABC 11- (Michael Ono, “Nation’s Infrastructure Still Vulnerable to Cyber Attack”, ABC News, 8/4/11, http://abcnews.go.com/Politics/nations-infrastructure-vulnerable-cyber-attack/story?id=14225674#.UBBhkppYt7F)//JY

In past wars, a hostile army would send troops to sabotage a bridge. Now a terrorist can send a suicide bomber to attack a mass transit system. In the future, experts are worried that malicious hackers -- perhaps even working for China, Iran or North Korea -- could bring down America's critical infrastructure. Nuclear reactors, the electric grid and the banking sector are all attractive targets, according to testimony Tuesday before the House Subcommittee on Oversight and Investigations by the director of information security issues at the Government Accountability Office. And while foreign attackers have yet to launch a serious attack on U.S.-based infrastructure, some security experts say that terrorists are looking for ways to make it happen. The GAO didn't name specific foreign adversaries, but one security expert that spoke to ABC News provided insight into who is trying to obtain high-tech hacking tools. "We know that North Korea wants it, we know that Iran wants it and that some of the terrorist groups are interested in it," said Jim Lewis, who is a senior fellow at the Center for Strategic and International Studies. The testimony came on the heels of a report from the security firm McAfee that showed evidence of a five-year cyber data-stealing operation likely conducted by a nation state that targeted more than 70 different governmental, non-profit and corporate entities. While the security firm didn't point any fingers, many other security experts have read the data and suspect China as the point of origin. The Obamas' Bullying PSA Watch Video 'The Note': Cyber Czar Watch Video Thompson's Cyber Announcement Watch Video But people shouldn't be too worried about a massive assault anytime soon according to Lewis. "Right now, only a few nation states have the capability to disrupt critical infrastructure," Lewis said. Talented engineers are scarce and essential to building the tools necessary to attack specialized U.S. infrastructure. Attacking a power plant is different than defacing a website. The tool required to pull pranks on the public Web have existed for years, while the tools necessary to breach private networks are only available to those with the resources to build them. But that dynamic could change as those tools become more readily available. "What could happen is that one day you'll be able to buy the software that will let people do things," said Lewis. In fact, the Department of Homeland Security released a warning on Thursday that Stuxnet, a worm that used in July 2010 to breach an Iranian nuclear reactor network, could be re-purposed to attack other systems with a similar configuration. DHS is currently working with the private sector to share information on prevalent attacks, but further legislation is needed to ensure a clear chain of command in the event of a crisis. Lawmakers in Congress are stalled on legislation that would overhaul the nation's cyber security. Senate Majority Leader Harry Reid, R-Nev., sent a letter Wednesday to Senate Republican leaders urging them to put cyber security back on the agenda. Republicans have expressed concerns with provisions in the bill that they believe would grant DHS the authority to regulate the private sector. But one administration official defended the plan at a House Oversight and Government Reform hearing earlier this July. "I believe this proposal is designed to give the private sector immense input into the process," said Greg Schaffer who testified on behalf of DHS. While lawmaker from both parties have made no concrete plans to move forward with legislation, many cyber security experts believe that now is the time for action. "We have known about our vulnerabilities in our critical infrastructure for well over a decade, and while there has been some progress we are still remarkably exposed," David Bodenheimer, a lawyer with Crowell & Moring LLP who consults with businesses on cyber issues. Role of the Federal Government Infrastructure protection will fall under the jurisdiction of numerous government agencies. The GAO review has identified 18 different sectors to monitor and has suggested seven agencies to oversee responsibilities. DHS will handle most of the domestic responsibility, but other agencies will help to oversee specific areas. For example, the Treasury Department will help protect the banking sector and the Department of Energy will help protect the electric grid and oil storage facilities. With so many agencies in charge of infrastructure defense, some experts are worried that the departments will be confused on certain issues. The Obamas' Bullying PSA Watch Video 'The Note': Cyber Czar Watch Video Thompson's Cyber Announcement Watch Video "No doubt the responsibilities are fragmented," said Bodenheimer. Proposed legislative solutions could empower the president to take more direct control in a crisis. But some critics have already objected to further consolidation and view cyber security reform as a massive overreach by the federal government. "If we frame this discussion as a war discussion, then what you do when there's a threat of war is you call in the military and you get military solutions," said Bruce Schneier, a cyber security author that argued that point in 2010 at the televised Intelligence Squared debate in Washington. "You get lockdown; you get an enemy that needs to be subdued. ... And so the threat of cyber war is being grossly exaggerated, and I think it's being done for a reason. This is a power grab by government." The cyber security bill that was introduced in 2010 faced fierce criticism. Opponents slammed a provision that would give the president the ability to shut off the Internet. Opponents to the bill pointed to the Internet censorship in the middle as a reason for limiting executive power.

#### Terrorist Organization will target US Infrastructure

Gordon 12 (Senior Research Fellow at the Symantic Security Response, Sarah, Gordon, “Cyberterrorism?”, 6/13/12)//DG

New terrorist organizations are highly funded, technologically articulate groups capable of inflicting devastating damage to a wide range of targets. While most published work in the computer industry has focused on the impact of the computer as target (pure cyberterrorism) it is our belief that the real danger posed by the synthesis of computers and terrorism is not only the insertion of computer as target in the terrorism matrix, but in many of the other areas, too. The current narrowness of focus poses a significant risk to US infrastructure. By being too concerned about one particular part of the matrix, we are apt to let our guard down in areas which may be more critical. A forward-looking approach to terrorism that involves computers is highly contextual in its basis. Traditional antiterrorism defenses must be deployed, but these countermeasures must fully take into account many of the virtual factors that we have outlined in this paper. If the events of September 11th teach us one thing, it is that we should always consider the ‘big picture’ of the overall terrorist threat, rather than view one aspect in isolation. The ‘cyber’ aspects of the puzzle must be woven throughout the picture, not simply confined to one cell. To view a problem with too narrow a perspective is to invite anarchy into our lives.

#### Cyber-attacks on infrastructure rising

The Hill 7/3- (Jennifer Martinez, “Companies see spike in cyberattacks on critical infrastructure systems”, The Hill, 7/3/12, http://thehill.com/blogs/hillicon-valley/technology/236089-companies-report-spike-in-cyber-attacks)//JY

Companies that operate critical infrastructure systems have reported a sharp rise in cybersecurity incidents over a three-year period, according to a new report from an arm of the Department of Homeland Security. Companies reported 198 cyber incidents in 2011, up from 41 incidents in 2010 and just nine in 2009, the report said. The rise in reported incidents comes as the Senate is gridlocked on legislation that would require operators of critical infrastructure to meet new cybersecurity standards. The report could provide fodder for lawmakers looking to move Sen. Joe Lieberman’s (I-Conn.) cybersecurity bill to the floor. The bill has been waiting for floor time since it was introduced in February, but Senate Majority Leader Harry Reid (D-Nev.) has repeatedly said he plans to act on the measure this year. The bulk of the cybersecurity incidents in 2011 were reported by companies in the water sector, accounting for about 41 percent of the incidents submitted to the department’s cyber emergency response team for industrial control systems, known as ICS-CERT.

#### Cyber Attacks would fuel Physical Attacks

Denning 2K (Teacher of Poltical Science at Georgetown University, Dorothy Denning, “Cyberterrorism”, May 23rd 2000)//DG

#### Cyber-attacks against computer systems could potentially shut down radio, telephone, and computer networks used to control and manage city or regional services, potentially resulting in loss of those services or the inability to properly dispatch public safety and other personnel to the scenes of crimes or physical terrorist attacks. Attacks on physical components of our information infrastructure could resemble other conventional attacks: for example, a bomb could be used to destroy a government computer bank, key components of web-based infrastructure, or even telephone switching equipment. Attacks could also involve remotely hijacking control systems in efforts to breach dams, impact air traffic, or shut down the power grid. Attacks launched in cyberspace could involve diverse methods of exploiting vulnerabilities in computer security: viruses, stolen passwords, insider assistance, software with secret “back doors” that intruders can penetrate undetected, and organized electronic traffic used to overwhelm computers – known as “denial of service” attacks are known to have occured. Attacks could also involve stealing classified files, altering the content of Web pages, disseminating false information, sabotaging operations, erasing data, or threatening to divulge confidential information or system weaknesses unless a payment or political concession is made. If terrorists managed to disrupt financial markets or media broadcasts, an attack could undermine confidence or instill public panic.

#### **Cyber-terrorists will attack critical infrastructure- Al Qaeda**

ABC 5/22- (Jack Cloherty, “Virtual Terrorism: Al Qaeda Video Calls for ‘Electronic Jihad’”, ABC News, 5/22/12, http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875#.UBBkBZpYt7E)//JY

Al Qaeda may be turning its destructive attention to cyber-warfare against the United States. In a chilling video, an al Qaeda operative calls for "electronic jihad" against the United States, and compares vulnerabilities in vital American computer networks to the flaws in aviation security before the 9/11 attack. The al Qaeda video calls upon the "covert mujahidin" to launch cyber attacks against the U.S. networks of both government and critical infrastructure, including the electric grid. The video was obtained by the FBI last year, and released today by the Senate Committee on Homeland Security and Governmental Affairs. "This is the clearest evidence we've seen that al Qaeda and other terrorist groups want to attack the cyber systems of our critical infrastructure," Homeland Security and Governmental Affairs Committee Chairman Joe Lieberman, I-Conn., said in a statement. "This video is troubling as it urges al Qaeda adherents to launch a cyber attack on America," said Sen. Susan Collins, R-Maine, the ranking member on the committee. "It's clear that al Qaeda is exploring all means to do us harm and this is evidence that our critical infrastructure is a target." Al Qaeda Bomb Maker's Plot Involves Pets Watch Video Terror Alert: Forest Fires as Al Qaeda Weapon? Watch Video If Israel Attacks Iran Watch Video The national security community says the threat of cyber attack is real, and the gap between terrorist aspirations and capability is closing. The senior intelligence official at Cyber Command, Rear Adm. Samuel Cox, has said al Qaeda operatives are seeking the capability to stage cyber attacks against U.S. networks and terrorists could purchase the capabilities to do so from expert criminal hackers. Increasing evidence also suggests that Iran is looking to commit cyber attacks against the United States, according to testimony last month before the House Committee on Homeland Security. Iran's sponsorship of terrorist groups takes on a new dimension in cyberspace, where it could develop a powerful cyber weapon and pass it on to a terrorist group. Lieberman is using the al Qaeda video to underline what he says is the need for new legislation.. "Congress needs to act now to protect the American public from a possible devastating attack on our electric grid, water delivery systems, or financial networks," he said. "As numerous, bipartisan national security experts have said, minimum cyber security standards for those networks are necessary to protect our national and economic security. That is why the Senate needs to act on our bipartisan Cyber Security Act that requires minimum security performance requirements for key critical infrastructure cyber networks." The Homeland Security Committee says the Department of Homeland Security received more than 50,000 reports of cyber intrusions or attempted intrusions since October, an increase of 10,000 reports over the same period the previous year.

#### **Terrorists can take control of nuclear and government centers.**

Coleman 10 (founder of Technolyitcs University, Kevin G. Coleman, “Nuclear Control Centers are Vulnerable”, February 18th 2010, <http://www.thenewnewinternet.com/2009/07/29/nation-nuclear-control-centers-vulnerable-to-cyber-terrorism-report///DG>)

Internet attacks appeal to terrorist organizations because cyberattacks can be accomplished at offsite locations. The report gives the example of terrorists hacking into  a Russian nuclear network infrastructure from China, to make it appear that Russia is forging a nuclear attack on the United States. The report goes on to name scenarios where terrorists could shut down communication networks between nuclear countries and leak false reports to the media, causing chaos and an escalated potential for a nuclear attack under false information. Hacking into a nation’s nuclear command center is also cheaper for a terrorist organization than building a nuclear weapon from scratch.  Heavy provisions are already in place to prevent terrorist access to nuclear command centers. Yet the report suggests that terrorists could hack into government emails and private networks, eliminating the need to attack a nuclear command and control center directly. Furthermore, although orders to launch a nuclear attack are reserved for the top officials and leaders, there is a significant potential for outside individuals to feed false information through media networks, emails, and even government private networks.  The report also found that media outlets sometimes overexagerate  the threat of a devastating cyberattack and do not properly define the term ‘cyber terrorism’.

### Terrorism and War Impacts

#### Impacts include major breaches of international security and war.

Gable 11 (professor of public international law at Drexel University, Kelly A. Gable, “Cyber Apocalypse now, securing the internet against cyber-terrorism”, August 5th 2011)//DG

As will be explained in detail, the Internet poses a three-pronged threat to national and international security. The clearest manifestation of this threat is the capacity to exploit an inherent weakness in the structure of the Internet to “island-hop,” or jump from computer to computer and network to network, accessing more critical data and more vulnerable networks. This easily can be accomplished once an attacker has “spoofed” his or her way onto a network. As a result of the structure of the Internet and related networks, cyberterrorists can gain access to systems and networks that are not necessarily considered vulnerable. Second, the Internet is utterly incapable of protecting information from sufficiently persistent and knowledgeable cyberterrorists. Finally, the Internet provides cyberterrorists with the tools that they need to carry out direct attacks on the Internet and use the Internet as a springboard to attack other networks. In fact, the insecurity of the Internet and its sister networks is such that a cyberterrorist with enough knowledge and the right tools can bring the entire system crashing down. This looming danger is related to the very accessibility that makes the Internet revolutionary because, increasingly, key aspects of critical public infrastructure are connected or accessible via the Internet. In the United States, “virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions, deliver services to the public, and account for their resources without these cyber assets.” As a result, ineffective security controls can expose a broad array of government operations and assets to significant risk, including the threat that critical infrastructure could be disabled. Ironically, the necessary knowledge and tools are readily available on the Internet. There is no good outcome to cyberterrorist attacks. The best- case scenario would involve damage limited to bad publicity and international embarrassment because government websites were hacked. The seemingly inevitable worst-case scenario includes the theft of classified information, the collapse of the international financial system, major breaches of national and international security and, potentially, war.

#### Absent further action cyber-apocalypse is inevitable

Gable 11 (professor of public international law at Drexel University, Kelly A. Gable, “Cyber Apocolypse now, securing the internet against cyber-terrorism”, August 5th 2011)//DG

Cyberterrorism poses perhaps the greatest threat to national and international security since the creation of weapons of mass destruction. As states and their economies become increasingly intertwined, largely due to the Internet and the international financial system of global trade, the effects of a cyberterrorist attack will be greater. Similarly, as cyberterrorists gain experience in disrupting national governments and shutting down critical infrastructure, their attacks likely will become increasingly successful. Although states, private industry, and international organizations have made significant efforts to increase international cooperation, much more needs to be done. In taking action, however, it must be understood that, due to the fundamental weakness of the structure of the Internet, those additional efforts will not completely prevent cyberterrorism. As a result, further efforts at international cooperation and international standards must be part of a layered approach to cyberterrorism that also includes deterrence. As a result of the realities inherent to cyberspace, the most feasible way to deter cyberterrorism is through the international law principle of universal jurisdiction. This is not to say that territorial jurisdiction (or nationality, passive personality, or protective jurisdiction) could not be used to prosecute cyberterrorists, should there be sufficient information and state willingness to exercise other forms of jurisdiction. It is merely to say that universal jurisdiction is likely to be the most feasible manner of prosecution and, therefore, deterrence. A layered approach of mitigation and deterrence can reduce the threat of cyberterrorism substantially. Unless and until states are willing to exercise universal jurisdiction over cyberterrorist acts as part of that layered approach, however, it is only a matter of time before cyberterrorists are able to unleash a cyber-apocalypse.

#### Lack of Cyber-security is a major threat- it leads to terrorism

Miller, 10 – AM reporter (Lisa, “Cybersecurity Breakdown in Washington, AM News, 11/18/10, [http://www.abc.net.au/am/content/2010/s3069595.htm)//AK](http://www.abc.net.au/am/content/2010/s3069595.htm%29//AK)

The US has revealed the details of a **startling breakdown in cyber security in April when 15 per cent of the world's Internet traffic was diverted through China. For 18 minutes emails and Internet material some of it sent from the Pentagon and NASA was re-routed via Chinese servers.** A US government report doesn't blame China for intentionally hacking into the system but experts **say it's a sign of the security risks ahead.** North America correspondent Lisa Millar reports. Experts describe it as one of the biggest redirections of Internet data they've seen. For almost 20 minutes on April the 8th this year, military emails and Internet traffic from the State Department, the Pentagon, even NASA were exposed. A US government report blames China Telecom but doesn't say why it might have happened or whether it was done intentionally. The Heritage Foundation's Dean Cheng specialises in Chinese political and security affairs. There are instances where situations are not necessarily the deliberate result of government decisions, but that doesn't make them an accident. Particularly when you are talking about as I said, 15 per cent of the global Internet traffic if it had been going on for a few minutes would be one thing as servers simply got overwhelmed, that it went on for so long would suggest that that's a lot of data that could be scooped up. **And Dean Cheng is convinced lot of that data has now been archived in China and is slowly being studied. And he says even the encrypted material would eventually be broken down.** Dale Meyerrose who's a former chief information officer for the director of national intelligence says **this is a serious threat.** You can intercept those things anything in the world whether it's Shanghai or Seattle, but what we're seeing here is a technique that may have in fact as the report points out that you pulled the information from, may have been a cover for something else. In my 35 years of dealing with this, **there's an intended consequence and a series of unintended consequences and I think they always play out in these kinds of things.** And Dean Cheng says **it isn't just a US problem. This affects every country that is hooked into the Internet that communications that was re-routed includes that from the United States to third parties and so it's not simply American information that has been made vulnerable, but that of our allies including Australia.** China has denied it hijacked the Internet but **the incident has added to global concerns about cyber security.** The US Defence Secretary Robert Gates this week described potential attacks as a huge future threat and a considerable current threat. This is Lisa Millar in Washington for AM.

#### One Hacker crippled Estonia and US attack will be worse 300 Times worse

Griffin, 8- an honorable discharge of the Navy and was personally selected by the National Security Agency (NSA) Department of Defense (DoD) Information Assurance scholarship program to attend Air Force Institute of Technology (AFIT) to complete an 18-month Master of Science (MS) program in Cyber Operations, (Jane J., “DOD ROLE FOR SECURING UNITED STATES CYBERSPACE”, March, http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDYQFjAA&url=http%3A%2F%2Fwww.hsdl.org%2F%3Fview%26did%3D20857&ei=yFIQULLiGIak8AS5lIGwDg&usg=AFQjCNGWYg1ilZXeB1xocg5QFT-1FLhfSw&sig2=7HGeVnSl7h4Md-j-bi9jUQ

NATO sent several cyber experts to Estonia to assist in determining where the attacks originated and to further strengthen the cyber security procedures already in place. Analysis of these attacks categorized them as “cyber riots”. Eventually, the attacks were traced back to an Estonian student, and seven months later in January 2008, the 20-year-old Estonian hacker was fined approximately $1,620.00 for the cyber attack [4]. The scales of justice do not seem very equal when comparing the fine to the amount of losses incurred by just one of Estonia’s banks. Now, substitute the United States for Estonia. The U.S. relies on information technologies from the simplest task of making a phone call using voice over internet protocol (VOIP) to deploying a weapon against an adversary. Today's interconnected systems and networks allow us to operate around the world through cyberspace within a matter of seconds exposing our infrastructure to cyberspace threats affecting our national security, public safety and personal privacy. Comparing the number of cyber users between the two countries, the United States has nearly 300 times as many internet users as Estonia. While direct comparisons are difficult to make, it is clear that a similar type of cyber attack against the United States could affect significantly more people, impacting the safety, morale, and security of our American citizens as well as our nation’s economy. If the United States experienced cyber attacks of the same intensity as Estonia’s, what role would DoD have in securing the United States’ cyberspace from cyber attacks? How could we be sure who is attacking in a timely matter and the intent of the attack? In conventional warfare one can ascertain who performed the attack by examining the delivery method and materials in a timely matter. A cyber attack is more difficult to attribute, and the differences between warlike and criminal acts are blurred. The threats still exist for an adversary to physically attack the United States, but a skilled cyberspace state or non-state adversary could strike at the heart of America’s homeland remotely and anonymously. Our reliance on the power and capabilities of Information Technology (IT), which may contain vulnerabilities exploitable by an adversary, could ultimately be our weakness, our Achilles Heel.

#### Cyber terror attack is the greatest threat to human life

Bucci, IBM's Issue Lead for Cyber Security Programs, Ex-Deputy Assistant Secretary of Defense, 09

(Steven P., June 12, 2009, “The Confluence of Cyber Crime and Terrorism” http://www.heritage.org/Research/NationalSecurity/hl1123.cfm) BB

Terrorists will recognize the opportunity the cyber world offers sooner or later. They will also recognize that they need help to properly exploit it. It is unlikely they will have the patience to develop their own completely independent capabilities. At the same time, the highly developed, highly capable cyber criminal networks want money and care little about the source. This is a marriage made in Hell. The threat of a full nation-state attack, either cyber or cyber-enabled kinetic, is our most dangerous threat. We pray deterrence will continue to hold, and we should take all measures to shore up that deterrence. Terrorists will never be deterred in this way. They will continue to seek ways to successfully harm us, and they will join hands with criminal elements to do so. A terrorist attack enabled by cyber crime capabilities will now be an eighth group of cyber threats, and it will be the most likely major event we will need to confront. Some would say that cyber crime is a purely law enforcement issue, with no national security component. That is a dubious "truth" today. This is not a static situation, and it will definitely be more dangerously false in the future. Unless we get cyber crime under control, it will mutate into a very real, very dangerous national security issue with potentially catastrophic ramifications. It would be far better to address it now rather than in the midst of a terrorist incident or campaign of incidents against one of our countries. Terrorism enabled by cyber criminals is our most likely major cyber threat. It must be met with all our assets.

### Economy

#### Cyber-attacks lead to economic and infrastructural collapse

Reid 6/12/12- Majority Leader in the Senate, Senator of Nevada (Harry, “Reid: Attacks Cost Our Economy Billions of Dollars and Thousands of Jobs Every Year”, United States Senate Democrats, 6/12/12, http://democrats.senate.gov/2012/06/12/reid-cyber-attacks-cost-our-economy-billions-of-dollars-and-thousands-of-jobs-every-year/)//JY

Washington, D.C. – Nevada Senator Harry Reid spoke on the Senate floor today regarding cyber security and critical infrastructure. Below are his remarks as prepared for delivery: Technology has changed our world. It has changed the way we shop, the way we bank and the way we travel. It has changed the way we get information, and the way we share it. It has changed the way our country protects itself. And it has changed the types of attacks we must guard against. Some of our top national security officials – including General Martin Dempsey, Chairman of the Joint Chiefs of Staff; General David Petraeus, Director of the CIA; and Leon Panetta, Secretary of Defense – have said malicious cyber attacks are among the most urgent threats to our country. We’ve already seen cyber attacks on our nuclear infrastructure, our Defense Department’s most advanced weapons, the NASDAQ stock exchange and most major corporations. Cyber attacks don’t threaten only our national security – they also threaten our economic security. These attacks cost our economy billions of dollars a year, and thousands of jobs. So we need to act quickly to pass legislation to make our nation safer and protect American jobs. The Defense Department, Department of Homeland Security and experts from across the intelligence community have issued chilling warnings about the seriousness of this threat. Only days ago, Senator McConnell and I received a letter from a remarkable, bipartisan group of former national security officials. The group includes six former Bush and Obama Administration officials: Michael Chertoff, Paul Wolfowitz, Mike McConnell, General Michael Hayden, Retired General James Cartwright and William Lynn III. The letter presented the danger in stark terms: “We carry the burden of knowing that 9/11 might have been averted with the intelligence that existed at the time. We do not want to be in the same position again when ‘cyber 9/11’ hits – it is not a question of whether this will happen; it is a question of ‘when.’” The group called the threat of a cyber attack “imminent.” And they said it “represents the most serious challenge to our national security since the onset of the nuclear age sixty years ago.” The letter noted that the top cyber security priority is safeguarding critical infrastructure – the computer networks that control our electrical grid, water supplies and sewers, nuclear plants, energy pipelines, communications systems and financial systems. These vital networks must be required to meet minimum cyber security standards. The letter was clear that securing this infrastructure must be part of any cyber security legislation Congress considers. General Keith Alexander, director of the National Security Agency, has said the same thing. This is what he wrote to Senator McCain recently: “Critical infrastructure protection needs to be addressed in any cyber security legislation. The risk is simply too great considering the reality of our interconnected and interdependent world.” General Alexander is one voice among many: The President of the United States, President Obama The non-partisan Center for Strategic and International Studies Commission on Cyber Security The co-chairmen of the 9-11 Commission, Governor Thomas Kean and Congressman Lee Hamilton The Director of National Intelligence, James Clapper The Director of the FBI, Robert Mueller They have all echoed this call to action. In fact, the entire national security establishment – including leading officials from the Bush and Obama Administrations, civilian and military leaders, Republicans and Democrats – agree on the urgent need to protect this vital infrastructure. And yet some key Republicans continue to argue we should do nothing to secure critical infrastructure. When virtually every intelligence expert says we need to secure the systems that make the lights come on, inaction is not an option. A coalition of Democrats and Republicans – including Senators Lieberman, Collins, Rockefeller and Feinstein – has proposed one approach to address this problem. Their bill is an excellent piece of legislation, and it’s been endorsed by many members of the national security community. It’s a good approach, and it would make our nation safer. But there are many possible solutions to this urgent challenge. Unfortunately, the critics of the bill have failed to offer any alternative to securing our nation’s critical infrastructure. The longer we argue over how to tackle this problem, the longer our power plants, financial systems and water infrastructure go unprotected. Everyone knows this Congress can’t pass laws that don’t have broad, bipartisan support. So we’ll need to work together on a bill that addresses the concerns of lawmakers on both sides of the aisle. But for that to happen, more of my Republican colleagues need to start taking this threat seriously. It is time for them to participate productively in the conversation, instead of just criticizing the current approach. There is room for more good ideas on the table. And I welcome to the discussion any Republican genuinely interested in being part of the solution. But national security experts agree: we can’t afford to waste any more time. The question is not whether to act, but how quickly we can act.

#### Cyber-attacks cripple the economy

Spence 11- Contributor to The Motley Fool, a multimedia financial services company (Katie, “Cyber Attacks Capable of Crashing the U.S. Economy?” The Motley Fool, 11/14/11, http://www.fool.com/investing/general/2011/11/14/cyber-attacks-capable-of-crashing-the-us-economy.aspx#.UBA-9ZpYt7F)//JY

Recent reports of the computers used to pilot General Atomics Aeronautical Systems' Predator drones being infected with a computer virus -- one that so far has proven impossible to remove -- are a perfect example of why cyber security is becoming an increasingly hot topic in defense. General Atomics is the prime contractor for the Predator, but subcontractors include Northrop Grumman (NYSE: [NOC](http://my.fool.com/watchlist/add?ticker=NOC&source=iwlsitbut0000010)) for the synthetic aperture radar; Boeing (NYSE: [BA](http://caps.fool.com/Ticker/BA.aspx?source=isssitthv0000001) ) for the intelligence workstation and mission planning systems; and L3 Communications (NYSE: LLL ) for the wideband satellite communications link, making this and other viruses a potential widespread problem among defense heavyweights. Not just a defense problem So far there haven't been any confirmed incidents of classified information being sent out as a result of the Predator virus, but experts are reportedly struggling to remove the virus from the Predator computers. According to Richard Clarke, a top advisor to three presidents, the United States' computer networks are so vulnerable to attack that going to war against computer-savvy countries like China, North Korea, Iran, or Russia could result in a cyber attack that would crash the U.S. economic system. With the U.S. economy just barely limping along as it is, a cyber attack that could bring the economic system to a screeching halt is no laughing matter. So what can be done?

#### Cyber attacks collapses infrastructure, economy, and China relations

Money News 5/8/12- (Forrest Jones, “Chertoff: Cyber Attacks on Companies Pose Biggest Threat to U.S. National Security”, Money News, 5/18/12, http://www.moneynews.com/Economy/Chertoff-Cyber-Attacks-Security/2012/05/08/id/438333)//JY

Cyber attacks pose the biggest threats to national security, says former Department of Homeland Security Secretary Michael Chertoff. Cyber attacks against companies like Lockheed Martin, Northrop-Grumman, Sony, Google, Visa and Mastercard, among others, show just how vulnerable the economy is to tech-savvy terrorists. "This is the biggest threat we currently face," Chertoff tells Yahoo's The Daily Ticker. Editor's Note: How You Lost $85,000 During the Last Decade. See the Numbers. "Not only is there a concern about our critical infrastructure … but we are losing billions of dollars of intellectual property every year that is being stolen and it is resulting in job losses and damages to our economy." A Federal Emergency Management Agency report estimates cyber attacks jumped 650 percent from 2006 to 2010, Yahoo adds, pointing out 60 percent of U.S. companies have reported security breaches. Half of the country's so-called "high-priority facilities" like those that manage the country's electrical grids reported having been attacked. Many attackers aren't necessarily enemies of the U.S. but rather, are looking for a leg up to compete, Chertoff adds. "For many nations, they view the economic well-being of the country as part of their national security strategies. They will use their intelligence agencies as a way to enable their companies, their national champions, to compete in the market place," Chertoff says. "We don't do that in the United States. We keep the free-market separate from government, but as a result sometimes we have our rivals overseas stealing our assets." U.S. and Chinese defense ministers have agreed to cooperate on cyber issues to avoid future crises, with China saying it takes too much blame for cyber attacks on U.S. interests, adding other countries are to blame. "Obviously there are other countries, actors, others involved in some of the attacks that both of our countries receive," Defense Secretary Leon Panetta told reporters after a meeting in the Pentagon with Chinese Defense Minister General Liang Guanglie, the Associated Press reports. "But because the United States and China have developed technological capabilities in this arena it's extremely important that we work together to develop ways to avoid any miscalculation or misperception that could lead to crisis in this area."

#### Cyber-attacks devastate the economy- high repair costs and loss of jobs

Paganini 7/6/12- Security Expert with over 20 years of experience (Pierluigi, “A view on the economic impact of cyber attacks, from US to China”, Security Affiars, 7/6/12, http://securityaffairs.co/wordpress/7077/cyber-crime/a-view-on-the-economic-impact-of-cyber-attacks-from-us-to-china.html)//JY

On June 28th, a FBI official declared before a House panel that the phenomenon of cyber espionage is increasing with an alarming trend. We are living a period of great crisis and the intellectual property is becoming a privileged target for cyber attacks. It has been estimated that the economic espionage in the current fiscal year will impact with a cost superior to $13 billion, the news as made public by Frank Figliuzzi, FBI assistant director, counterintelligence division, during a communication before the House Homeland Security subcommittee on counterterrorism and intelligence. Figliuzzi declared: “Foreign nations know that it’s always cheaper to steal U.S. technology than it is to research and develop it themselves,” The cyber espionage is largely diffused both in private and governments sectors, the opportunity to acquire sensible information in this way could give a great advantage to the attackers. The practice of the cyber espionage could be perpetrated in a long interval of time causing dramatic problems, emblematic the case of Nortel firm that has terminated in bankruptcy. The repercussion are serious on internal economy, the Commerce Department estimates that due cyber espionage have been lost around 27.1 million American jobs in 2010, 18.8 percent of all employment. The MI5 chief presented a worrisome scenario, the UK industry suffers both state sponsored cyber espionage and organized cybercrime. The espionage activities are not new, but the introduction of new technology has amplified the size of the phenomenon, Greg Wilshusen, Government Accountability Office director of information security issues, said: “use of cyberspace have vastly enhanced the reach and potential impact of such threats,” The problem of cyber espionage is also targeting businesses and government all over world, the Director General of MI5, Jonathan Evans, has recently declared that “one major London listed company” estimated that it had lost “some £800m as a result of hostile state cyber attack – not just through intellectual property loss but also from commercial disadvantage in contractual negotiations.” Why choose to spy on a private firm or government in economic field? Technological instruments such as malware represents a cheaper, and less risky, solution to steal sensible secrets. The most active nations in this area are Russia and China but also countries such as Israel, US and Western States. Lets conclude this rapid view on cyber espionage with a surprising data, China is world’s biggest cyber attack victim according a recent report published by the National Computer Network Emergency Response Coordination Center of China. The situation is critical due an impressive number of attacks that hit the country. Following some figures on the security status of Chinese business and their exposure to the attacks; Over 98 percent of Chinese business websites had implemented standard protective measures against security threats in 2011, up from 92.25 percent in 2010 and 78.61 percent in 2009, the report said. Compared with 2010, it has been observed a reducion of 39.4 percent for the number of government websites that were targeted by cyber attacks in 2011.The country was hit by a total of 47,000 overseas based Internet Protocol addresses (IPs) were involved in attacks against 8.9 million Chinese computers last year, an increment of 78% respect 2010. Mainly the attacks are originated in Japan, the US and South Korea, the report said. What will expect from the future? No doubts, the attacks will increase, in particular the major increments will be registered using cloud and mobile platforms.

#### Cyber Attacks threaten Economy as well- turns case

Lewis 2 (Center for Strategic and International Studies, James A. Lewis, “Assessing the Risks of Cyber Terrorism, Cyber War, and other Cyber Threats”, 1/24/2”)//DG

Cyber attacks do pose a very real risk in their potential for crime and for imposing economic costs far out of proportion to the price of launching the attack. Hurricane Andrew, the most expensive natural disaster in U.S. history, caused $25 billion dollars in damage and the average annual cost from tornadoes, hurricanes, and flood damage in the U.S. is estimated to be $11 billion. In contrast, the Love Bug virus is estimated to have cost computer users around the world somewhere between $3 billion and $15 billion. Putting aside for the moment the question of how the estimates of the Love Bug’s cost were calculated (these figures are probably over-estimates), the ability of a single university student in the Philippines to produce this level of damage using inexpensive equipment shows the potential risk from cyber crime to the global economy. The financial costs to economies from cyber attack include the loss of intellectual property, financial fraud, damage to reputation, lower productivity, and third party liability. Opportunity cost (lost sales, lower productivity, etc) make up a large proportion of the reported cost of cyber attacks and viruses. However, opportunity costs do not translate directly into costs to the national economy. For example, if a Distributed Denial of Service attack prevents customers from reaching one online bookseller, they may instead go to another to purchase their books. The aggregate national sale of books could remain the same although the first bookseller’s market share would decline. A small number of customers may choose not to bother going to another site if their first choice is unavailable, but some of these lost sales may well be recouped by later return to the sight by the customer. Businesses face greater damage from financial fraud and theft of intellectual property over the Internet, crimes that continue to grow in number. Emphasizing the transnational nature of cyber security issues, the last few years have seen the emergence of highly sophisticated criminal gangs capable of exploiting vulnerabilities in business networks. Their aim is not terror, but fraud or the collection of economically valuable information. Theft of proprietary information remains the source of the most serious losses, according to surveys of large corporations and computer crime.18 These crimes must be differentiated from the denial of service attacks and the launching of viruses. Denial of services or viruses, while potentially damaging to business operations, do not pose the same level of risk. Cyber crime is a serious and growing threat, but the risk to a nation-state in deploying cyber-weapons against a potential opponent’s economy are probably too great for any country to contemplate these measures. For example, writers in some of China’s military journals speculated that cyber attacks could disable American financial markets. The dilemma for this kind of attack is that China is as dependent on the same financial markets as the United States, and could suffer even more from disruption. With other critical infrastructures, the amount of damage that can be done is, from a strategic viewpoint, trivial, while the costs of discovery for a nation state could be very great. These constraints, however, do not apply to non-state actors like Al Qaeda. Cyber attacks could potentially be a useful tool (albeit not a fatal or determinative tool) for non- state actors who reject the global market economy.

#### Impacts include financial crisis, loss of revenue property and collapse of the financial system

Coleman 3 (Author for the Direct Magazine, Kevin Coleman, “Cyber Terrorism”, October 3rd 2003, <http://www.directionsmag.com/articles/cyber-terrorism/123840//DG>)

The intention of a cyber terrorism attack could range from economic disruption through the interruption of financial networks and systems or used in support of a physical attack to cause further confusion and possible delays in proper response. Although cyber attacks have caused billions of dollars in damage and affected the lives of millions, we have yet witness the implications of a truly catastrophic cyber terrorism attack. What would some of the implications be? Direct Cost Implications Loss of sales during the disruption , Staff time, network delays, intermittent access for business users , Increased insurance costs due to litigation , Loss of intellectual property - research, pricing, etc. , Costs of forensics for recovery and litigation , Loss of critical communications in time of emergency, Indirect Cost Implications, Loss of confidence and credibility in our financial systems , Tarnished relationships& public image globally , Strained business partner relationships - domestic and internationally , Loss of future customer revenues for an individual or group of companies , Loss of trust in the government and computer industry New legislation is requiring system breaches to be reported (SB1386 California). Other proposed legislation would allow damages to be sought by victims of attacks that are launched from hacked web systems. California's SB 1386 is a sweeping measure that mandates public disclosure of computer-security breaches in which confidential information of any California resident may have been compromised. The bill further goes on to define personal information as an individual's first name or initial and last name in combination with a SSN, a driver's license number, or any account numbers, credit card numbers, debit card numbers, and associated passwords or codes. Think of the liability an organization would incur if their systems were compromised and thousands of individuals personal information were exposed and even exploited for financial gain - (funding terrorism). With the "LoveBug" virus costing nearly $10 billion, it is hard to fathom the financial implications of a much more serious and comprehensive attack. Each and every day corporations in the U.S. and abroad spend millions combating the threats of cyber attacks and cyber terrorism. Corporate efforts reach tens (if not hundreds) of billions of dollars annually and with the increased frequency of attacks, the cost will significantly increase in the coming years. As we face more and more complex attacks from professional cyber warriors, corporations will increasing seek help from the governments around the world to thwart these efforts and stem the financial bleeding.

#### Estonia Proves Cyberattack devastates Economy- Cyber Attacks Crippled Estonia

Griffin, 8- an honorable discharge of the Navy and was personally selected by the National Security Agency (NSA) Department of Defense (DoD) Information Assurance scholarship program to attend Air Force Institute of Technology (AFIT) to complete an 18-month Master of Science (MS) program in Cyber Operations, (Jane J., “DOD ROLE FOR SECURING UNITED STATES CYBERSPACE”, March, http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDYQFjAA&url=http%3A%2F%2Fwww.hsdl.org%2F%3Fview%26did%3D20857&ei=yFIQULLiGIak8AS5lIGwDg&usg=AFQjCNGWYg1ilZXeB1xocg5QFT-1FLhfSw&sig2=7HGeVnSl7h4Md-j-bi9jUQ

The cyber attacks on Estonia in late April and the early weeks of May 2007 significantly crippled the country, preventing it from performing banking, communications, news reporting, government transactions and command and control activities. Estonia is considered a “Wired Society”, much like the United States. Both countries rely on the cyberspace infrastructure economically and politically. Estonia sought assistance outside the country to recover from and to address the attacks. The cyber attacks on Estonia focused world-wide attention on the effects that cyberspace attacks could have on countries. If a cyber attack of national significance occurred against the United States, what would the United States do? The Department of Defense is responsible for protecting the nation and its geographical boundaries from attack, but what is DoD’s role for securing the United States’ cyberspace? Research was conducted by studying national orders, strategies, policies plans, and doctrine to determine DoD’s role for securing the United States’ cyberspace. Research revealed that DoD is assigned the lead role as Sector Specific Agency (SSA) for the Defense Industrial Base (DIB). As the lead SSA for the DIB, DoD’s role for securing the United States’ cyberspace is to identify, assess, and improve risk management of the critical infrastructure within the DIB. Our nation’s defense and military strength rely on the DoD which in turn relies on the DIB to enable DoD to perform its mission. Participation by the DIB is on a voluntary basis, with DIB participants making the risk management calls and implementing the strategies that best fit their needs, which may not serve national security objectives.

#### Cybersecurity Bill Key to the Economy- US looses 588 billion on Successful Breaches

Homeland Security and Governmental Affairs, 7/19/12- article refrences quotes by congressmen in the Homeland Security and Governmental Affairs, (“National Security, Economy, Essential Life Services At Stake”, http://www.hsgac.senate.gov/media/majority-media/lieberman-collins-rockefeller-feinstein-carper\_offer-revised-legislation-to-improve-security---of-our-most-critical-private-sector-cyber-systems- )//JH

Lieberman said: “This legislation is urgently needed to address the clear, present, and growing danger of cyber attacks against our most critical systems. In an era when anyone can buy the technological capability to cripple the electric grid, steal proprietary information from seemingly secure websites, and digitally drain bank accounts of money, our most important networks are alarmingly vulnerable. We must respond with speed and resolve to a threat that will only increase.            “This compromise bill creates a public-private partnership to set cybersecurity standards for critical American infrastructure, and offers the reward of some immunity from liability to those who meet those standards. In other words, we are going to try carrots instead of sticks as we begin to improve our cyber defenses. This compromise bill will depend on incentives rather than mandatory regulations to strengthen America's cybersecurity. If that doesn't work, a future Congress will undoubtedly come back and adopt a more coercive system.          “While the bill we introduced in February is stronger, this compromise will significantly strengthen the cybersecurity of the nation’s most critical infrastructure and with it our national and economic security.           “We responded after the 9/11 attacks to improve our security. Now we must respond to this latest challenge before a cyber 9/11 occurs.”           Collins said, “Experts have repeatedly warned that the computer systems that run our critical infrastructure – our electric grid, water systems, financial networks, and transportation systems – are vulnerable to a major cyber attack.  A cyber attack is a threat not just to our national security, but also to our economic edge and way of life. “The owners and operators of critical infrastructure reported nearly 200 cyber intrusions in 2011, a 400 percent increase from the previous year.  And these are only the intrusions that have been reported to DHS.  Many go unreported, and even worse, many owners are not even aware that their systems have been compromised.   Moreover, U.S. companies lose about $250 billion a year through intellectual property theft, $114 billion to theft through cyber crime and another $224 billion in down time the thefts caused.           “The data and the headlines make it clear that we have already waited too long to address this escalating threat.  In an effort to move this overdue legislation forward, the measure released today represents the Senate’s best chance to pass cyber legislation this year.  Our bill is a good-faith effort to address the concerns of members of both sides of the aisle by establishing a framework that relies upon the expertise of government and the innovation of the private sector.  It would set voluntary, outcome-based cybersecurity best practices and encourage adoption by companies through various incentives.  It also promotes the sharing of cyber threat information within the private sector and with government in real-time, while safeguarding privacy and civil liberties. I look forward to working with my colleagues on this bill through an open amendment process during its consideration on the Senate floor.”           Rockefeller said: “Our country, from the government to utility companies to Fortune 500 Companies – we all are unprepared when it comes to cybersecurity,” Rockefeller said.  “This legislation is a critical first step in our country’s response to this problem. I had previously sponsored a bill with a stronger regulatory approach to resolve this problem, but it’s become clear that some members of the Senate would not support that approach.  While I still prefer the regulatory approach, and believe that it would better protect our country, we are moving forward in the spirit of compromise with an incentives-based voluntary approach because it is a crucial matter of public safety and national security that we do something now to ensure our most critical infrastructure is protected from cyber-attacks.”

#### Cyber Security is Key- lack of it causes economic decline, job loss, and loss of US confidentiality

Genachowski 12/13/11- Chairman of Federal Communications Comission (Julius, “FCC: Cyber Security is Important for the future”, ICACTIVE, 12/13/11,<http://icactive.com/2012/02/fcc-cybersecurity-is-important-for-the-future/>**)** //AK

Julius Genachowski, the chairman of the Federal Communications Commission said on Wednesday **that if we fail to fight the challenges of cybersecurity, U.S. will pay the price in the form of diminishing safety, lost privacy, lost jobs, and financial vulnerability. It means that billions of dollars might lose into the digital criminals. FCC called the internet users to be careful with multiple cyber threats such as botnet attack, IP hijacking, and domain name fraud. Botnet attack means that one computer will be able to control millions of other computers with a malware downloaded by the users. IP hijacking takes advantage from the weakness in the way internet was built, causing traffic to be redirected to a network it wouldn’t normally use.** Domain name fraud is a bad actor which changes the identifying information of a website in the DNS. What about the future of security? President Barrack Obama already proposed a budget for cybersecurity programs in 2013, indicating that cybersecurity is a real emerging threat beside nuclear war and terrorism. Do you think the U.S. or the other countries are capable to deal with large scale cyberattack? Have you been alerted for these kind of attacks?

#### Cyber Attacks Cripple US economy

Liberman, 2/14/12- congressional introduction of the bill to the senate and the president, (“STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS”, <http://www.fas.org/irp/congress/2012_cr/s2105.html>, Congressional Record Volume 158, Number 24)//JH

Enemies probe the weaknesses in our critical national assets every day, waiting until the time is right, through cyber attack, to cripple our economy or attack, for instance, a city's electric grid with the touch of a key on the other side of the world. The fact is our cyber defenses are not what they should be, but such as they are they are blinking red. Yet, again, I fear we will not be able to connect the dots to prevent a 9/11-type cyber attack on America before it happens. The aim of this bill is to make sure we don't scramble here in Congress after such an attack to do what we can and should do today. [[Page S617]] Intellectual property worth billions of dollars has already been stolen, giving our international competitors access in the global marketplace without ever having to invest a dime in research. The fact is that even the most sophisticated companies are being penetrated, and our adversaries are using information learned in one intrusion to plan the next more sophisticated one. Last year, the computer security firm McAfee conducted a study of 70 specific instances of data theft, and they issued a report on those instances. They included 13 defense contractors, 6 industrial plants, and 8 American and Canadian Government networks. Based on that report, the former vice president of McAfee, Dmitri Alperovitch, issued this ominous warning: I am convinced that every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised--or will be shortly--with the great majority of the victims rarely discovering the intrusion or its impact.

### China Impact Module

#### Lack of cyber-security leads to U.S.-China cyber war

CNN 11- (David Goldman, “China vs. U.S.: The Cyber Cold War is raging”, CNN Money, 7/28/12, http://money.cnn.com/2011/07/28/technology/government\_hackers/)//JY

NEW YORK (CNNMoney) -- On April 8, 2010, traffic to about 15% of the world's websites was rerouted to China. State-owned Internet company China Telecom tricked relays from around the world into routing traffic through its servers for about 18 minutes. It isn't publicly known what happened to that traffic when it passed through China. But a report filed late last year by Congress' U.S.-China Economic and Security Review Commission said the hijacked traffic could easily have been captured, censored, or even replaced with other data without anyone's knowledge. Those scenarios were especially worrying to the U.S. government since the incident affected traffic to and from ".gov" and ".mil" sites, including those for the Senate, Army, Navy, Marines, Air Force, Defense Department, NASA, and Commerce Department. Websites for Dell (DELL, Fortune 500), Yahoo (YHOO, Fortune 500), Microsoft (MSFT, Fortune 500) and IBM (IBM, Fortune 500) were also affected. It wasn't the first time -- or the last -- that suspicious cyber activity has been traced back to China. In 2008, the FBI launched "Operation Cisco Raider," seizing 3,500 fake networking devices that originated in China, including counterfeit Cisco (CSCO, Fortune 500) routers purchased by U.S. government agencies. In late 2009, Google (GOOG, Fortune 500), Adobe Systems (ADBE), Juniper Networks (JNPR) and a dozen other technology companies were hit with a targeted attack that emanated from China. The cyber Mafia has already hacked you A white paper issued by security firm McAfee found that the attack could yield "complete access to internal systems," with the ability to collect and manipulate the companies' core assets, including source code. Google went public about the attack, said that some of its intellectual property had been stolen, and pulled its search engine servers out of China soon after. Last month, hundreds of personal Gmail accounts, including those of some senior U.S. government officials, were hacked as a result of a massive phishing scheme originating from China. Security experts and government officials have been quick to link these and similar attacks to the Chinese government. "It's no secret that government agencies are under attack from China," said Prescott Winter, public sector chief technology officer of ArcSight, a security company owned by Hewlett-Packard (HPQ, Fortune 500), and former CTO for the National Security Agency. "It's a significant problem, and the government has been aware of it for the past 10 to 15 years." China has repeatedly and vehemently denied any connection to the attacks, and proving that Beijing was behind specific hacks is difficult. But even if we can't trace individual attacks back to the Chinese government, experts say mounting evidence signals that the Chinese government is sponsoring wide-ranging cyberattacks against the U.S. government and corporations. "A review of the scale, focus, and complexity of the overall campaign directed against the United States ... strongly suggest that these operations are state-sponsored or supported," a Northrop Grumman (NOC, Fortune 500) white paper on the capabilities of the Chinese government to conduct cyber warfare concluded. "China is likely using its maturing computer network exploitation capability to support intelligence collection against the U.S. government and industry by conducting a long term, sophisticated, computer network exploitation campaign." What China is capable of By 2007, the NSA said that Chinese hackers had accumulated between 10 to 20 terabytes of data stolen from U.S. government agencies and corporation -- about a tenth of the information volume of all the books held by the Library of Congress. U.S. military networks were attacked 6 million times in 2006, according to the National Security Agency. By 2010, there were 6 million attacks per day. Government officials this month acknowledged that 24,000 Pentagon files had been stolen in March during an organized cyber attack. Experts agree China has at the very least stolen critical information about the U.S. government's defense industry, space program, China-related policy and military intelligence. LulzSec and Anonymous are the least of your hacker worries As much as China spies on our government's infrastructure, it also spies on U.S. corporations. A great number of U.S. corporations do business in China, which controls the infrastructure the companies must use to send information back and forth. Many experts believe the Chinese government actively spies on U.S. corporations working in the country -- just as China does to its own citizens' Internet communications. "Corporations can't protect themselves against that," said Dave Aitel, president of security firm Immunity Inc. and a former NSA computer scientist. "It's the equivalent of breaking in and installing bugs. Companies are now realizing the true cost of outsourcing. That's why Google left: Google said you can't do trusted business and run a company there." "I don't want to tell businesses not to go to China because it's unsafe," said Jose Granado, leader of Ernst & Young's information security practice. "At the same time, risk management is necessary. It's important to operate with your eyes wide open there. China isn't Iowa." So what could China do with all the information it collects? At best, experts say China will be able to able quickly advance its defense capabilities and save on years of research and development for its military and state-owned technology companies. At worst, the threat becomes military. In a war, that information could be enough to "delay U.S. deployments and impact combat effectiveness of troops," Northrop Grumman said in its assessment. "It's easier to go to war if you disable a country's rocket launchers first," said Bill Pennington, CEO of WhiteHat Security, a website security company. That's not a far-fetched scenario. In September 2007, Israeli F15s and F16s bombed a nuclear reactor construction site in Syria, but Syrian radars never picked up the planes crossing the border. That's because Israel had hacked Syria's radar software. And then, of course, there's Stuxnet, a bug so sophisticated that it significantly delayed Iran's nuclear program. The worm, which was likely loaded into the system on a thumb drive, ordered the centrifuges in an Iranian nuclear facility to spin out of control, ultimately destroying it. While that was happening, Stuxnet made all the meters tell Iranian engineers that everything was normal. How the United States can respond Experts say much more needs to be done by the government and corporations to ensure our national security. "The problem is we have this thicket of 20th century rules that don't work in the 21st century," said Michael Chertoff, former Secretary of Homeland Security, in a talk last month hosted by analytics company Opera Solutions. "The concept of a 'person' as the only threat has lost is meaning. It may be a server; we can be at war with a network." In other words, protecting land, sea and air borders won't save you if your attackers are seconds away no matter where they are. For all the improvements that the government needs to make, the private sector lags further behind. A recent wave of cyberthreats began to scare corporations into beefing up their security, but companies have still been reluctant to spend. "Most big corporations are only beginning to realize what's going on and are learning how to respond," ArcSight's Winter noted. Still, experts say the nightmare scenario -- China disabling our defenses and attacking the country -- remains unlikely. "The U.S. government operates on the premise that most government systems and networks have been compromised by various classes of attackers," said Jeffrey Bernstein, executive vice president of security contractor Critical Defence, who estimated that more than 150 countries have developed cyberattack capabilities. "Still, the U.S. is the 10,000-lb. gorilla in the world. We're the leader in these capabilities." It may surprise some that the U.S. Air Force's mission statement is "To fly, fight and win in air, space and cyber space." And the Obama administration has taken a very proactive approach to cybersecurity. "We are very well defended these days," Winter said. "Our agencies are not totally bulletproof, because nothing is, but they're much better off than they were before." "It's like the Cold War," said Larry Ponemon, chairman of the Ponemon Institute, a cybersecurity research organization. "We have the ability to bring you down, you have the ability to bring us down, so no one is doing anything."

#### US China war goes nuclear

Hadar, adjunct scholar at Cato, ‘96

(Louis Hadar , The Sweet and Sour Sino-American Relationship, 1/23/96, http://www.cato.org/pubs/pas/pa-248.html)

Some analysts, including Nicholas D. Kristof, former Beijing chief of the New York Times, have drawn a historical parallel between the rise of Germany as a world economic and military power at the end of the 19th century and China's rise in the last decade of the 20th century. They suggest that, given the similar authoritarian and insecure nature of the regimes in post-Bismarck Germany the post-Deng China, China could emerge as a leading anti-status quo player, challenging the dominant position of the United States, which like Great Britain in the 19th century occupies the leading economic and military position in the world. "The risk is that Deng's successor will be less talented and more aggressive--a Chinese version of Wilhelm II," writes Kristof. "Such a ruler unfortunately may be tempted to promote Chinese nationalism as a unifying force and ideology, to replace the carcass of communism." For all the differences between China and Wilhelmine Germany, "the latter's experience should remind us of the difficulty that the world has had accommodating newly powerful nations," warns Kristof, recalling that Germany's jockeying for a place in the front rank of nations resulted in World War I.(66) Charles Krauthammer echoes that point, contending that China is "like late 19th-century Germany, a country growing too big and too strong for the continent it finds itself on."(67) Since Krauthammer and other analysts use the term "containment" to describe the policy they urge Washington to adopt toward China, it is the Cold War with the Soviet Union that is apparently seen as the model for the future Sino- American relationship. Strategist Graham Fuller predicts, for example, that China is "predisposed to a role as leader of the dispossessed states" in a new cold war that would pit an American-led West against an anti-status quo Third World bloc.(68) Although Krauthammer admits that China lacks the ideological appeal that the Soviet Union possessed (at least in the early stages of the Cold War), he assumes that, like the confrontation with the Soviet Union but unlike the British-German rivalry, the contest between America and China will remain "cold" and not escalate into a "hot" war. That optimism is crucial. Advocates of containment may be able to persuade a large number of Americans to adopt an anti-China strategy if the model is the tense but manageable Soviet-American rivalry. However, not many Americans are likely to embrace containment if the probable outcome is a bloody rerun of World War I--only this time possibly with nuclear weapons.

### China Internal Link Extensions

#### The PLA eager for a US cyber attack.

Smith 3 (Speaker at NPR and author for Newsmax, Charles R. Smith, “Blackout, not an attack but a Warning”, August 13th 2003, <http://archive.newsmax.com/archives/articles/2003/8/19/121729.shtml//DG>)

Al-Qaeda represents only one threat to U.S. computer systems. It is a fact that America is not the only nation that has professional cadres of hackers inside its military. China is frantically working on its own cyber war plans. In November 2000, Maj. Gen. Dai Qingmin, director of the People’s Liberation Army Communications Department of the General Staff HQ, wrote a major paper on "Information Warfare." According to Gen. Dai, pre-emptive attacks by the Chinese army on American civilian computer and information systems will use "information warfare techniques which differ from U.S. IW [information warfare] plans." The PLA has reserve information warfare units located in the cities of Datong, Xiamen, Shanghai, Echeng and Xian. Each of these units is developing specialty capabilities to attack U.S civilian computers. For example, the Shanghai unit is focusing on attacking wireless telecom networks and double-encryption passwords. Gen. Dai outlined several Chinese info war strategies, including such hacker techniques as jamming or sabotaging enemy info systems, giving a false impression while launching an info war attack, and blinding and deafening an enemy with false impressions. The Chinese army is deadly serious about attacking U.S. civilian computers. The recent massive PLA Taiwan invasion exercise included an info warfare operation in the Shenyang Military Region simulating attacks on U.S. civilian computers. American computer security weakness, according to former defense adviser William Triplett, could spell disaster in the near future. According to Triplett, co-author of "Year of the Rat" and "Red Dragon Rising," the possible Chinese army penetration of critical computer systems is part of an ongoing information war being waged against America. "This has enormous implications for Communist Chinese cyber warfare against the United States," stated Triplett, who has studied Chinese army information warfare. "In the event of a conflict, they could hold hostage the very lives of hundreds of thousands of American men, women and children." According to Triplett’s 1999 book, "Red Dragon Rising," Chinese army information warfare is an "unheralded national security threat to the United States." "The American economic, political and social system is essentially unprotected against a Chinese information warfare attack. As the PLA notes, ‘America’s economic system is extremely vulnerable to information attacks.’ Senior PLA officers have begun to talk among themselves about a pre-emptive strike using information warfare," noted Triplett.

#### China will attack our cyberspace

Billo and Chang 4 (Institute for Security Technology Studies at Dartmouth College, Charles Billo and Welton Chang, “Cyber Warfare: the Analysis of the means and motivations of Selected Nation States”, November 2004)//DG

China: Within the framework of an integrated national plan, the People’s Liberation Army (PLA) has formulated an official cyber warfare doctrine, implemented appropriate training for its officers, and conducted cyber warfare simulations and military exercises. Beijing’s intelligence services continue to collect science and technology information to support the government’s goals, while Chinese industry gives priority to domestically manufactured products to meet its technology needs. The PLA maintains close ties with its Russian counterpart, but there is significant evidence that Beijing seeks to develop its own unique model for waging cyber warfare.

### India-Pakistan Module

#### India Pakistan cyber war will escalate

Billo and Chang 4 (Institute for Security Technology Studies at Dartmouth College, Charles Billo and Welton Chang, “Cyber Warfare: the Analysis of the means and motivations of Selected Nation States”, November 2004)//DG

India: Cyber attacks pose more than a theoretical challenge to the Indian government’s day-to-day national security agenda due to the intrusions and web defacements experienced after New Delhi’s nuclear weapons test and in the confrontation with Pakistan over Kashmir. The Indian authorities announced a shift in military doctrine in 1998 to embrace electronic warfare and information operations. An IT roadmap, enumerating a comprehensive ten year plan, was published. In the framework of the roadmap, the government has granted permission for closer government/industry cooperation to leverage the output of India’s world-class IT software industry. In addition, a new National Defense University and Defense Intelligence Agency (DIA) have been established. According to journalistic accounts, the armed forces plan to establish an information warfare agency within the DIA with responsibility for cyber war, psychological operations, and electromagnetic and sound wave technologies.

#### India and Pakistan will attack each other

Billo and Chang 4 (Institute for Security Technology Studies at Dartmouth College, Charles Billo and Welton Chang, “Cyber Warfare: the Analysis of the means and motivations of Selected Nation States”, November 2004)

Pakistan: Well-documented hacker activity in Pakistan and possible ties between the hacker community and Pakistani intelligence services indicate that Pakistan appears to possess a cyber attack capability. However, the published evidence is lacking concerning the exact nature of the capability; it is quite possible that the government of Pakistan has made only a minimal investment in its cyber warfare program. The available evidence suggests that the main target of Pakistan’s offensive capability is India—Islamabad’s rival on the sub-Continent and adversary in the Kashmir dispute. Pakistan’s developed IT industry, well-educated computer programmers, and supportive government that is concerned with security in Kashmir and parity with India provides circumstantial evidence suggesting a cyber warfare program.

#### India Pakistan War leads to extinction

Gertz, Staff Writer at the Washington Times, 2001

(Bill Gertz, Staff writer at the Washington Times 12/31/2001, India, Pakistan prepare nukes, troops for war, Lexis)

Pakistan and India are readying their military forces - including their ballistic missiles and nuclear weapons - for war, The Washington Times has learned. U.S. intelligence officials say Pakistani military moves include large-scale troop movements, the dispersal of fighter aircraft and preparations for the transportation of nuclear weapons from storage sites. India also is moving thousands of its troops near the border with Pakistan and has dispersed some aircraft to safer sites away from border airfields, say officials familiar with intelligence reports of the war moves. Pakistan is moving the equivalent of two armored brigades - several thousand troops and hundreds of tanks and armored vehicles - near the northern part of its border with India. Indian and Pakistani troops exchanged heavy mortar fire over their border in southern Kashmir today, Agence France-Presse reported. Five Indian soldiers were seriously injured in the heaviest shelling in four months, a senior Indian army official said. More than 1,000 villagers were evacuated from their homes overnight for the operation, according to the report. Officials say the most alarming signs are preparations in both states for the use of nuclear-tipped missiles. Intelligence agencies have learned of indications that India is getting its short-range Prithvi ballistic missiles ready for use. The missiles are within range of the Pakistani capital, Islamabad. Meanwhile, Pakistan is mobilizing its Chinese-made mobile M-11 missiles, also known as the Shaheen, which have been readied for movement from a base near Sargodha, Pakistan. Intelligence reports indicate that India will have all its forces ready to launch an attack as early as this week, with Thursday or Friday as possible dates. Pakistan could launch its forces before those dates in a pre-emptive strike. Disclosure of the war preparations comes as President Bush on Saturday telephoned leaders of both nations, urging them to calm tensions, a sign of administration concern over the military moves in the region. The administration also fears that a conflict between India and Pakistan would undermine U.S. efforts to find terrorists in Afghanistan. U.S. military forces are heavily reliant on Pakistani government permission to conduct overflights for bombing and other aircraft operations into Afghanistan, primarily from aircraft carriers located in the Arabian Sea. With tensions growing between the states, U.S. intelligence officials are divided over the ultimate meaning of the indicators of an impending conflict. The Pentagon's Joint Staff intelligence division, known as J-2, late last week had assessed the danger of conflict at "critical" levels. Other joint intelligence centers outside the Pentagon, including those supporting the U.S. military forces responsible for the Asia-Pacific region and for Southwest Asia, assess the danger of an India-Pakistan war as less than critical but still "serious." Intelligence officials are especially worried about Pakistan's nuclear arsenal because control over the weapons is decentralized. Even before the latest moves, regional commanders could order the use of the weapons, which are based on missiles or fighter-bombers.

### Iran Internal Link

#### Iran will cyber attack us

Billo and Chang 4 (Institute for Security Technology Studies at Dartmouth College, Charles Billo and Welton Chang, “Cyber Warfare: the Analysis of the means and motivations of Selected Nation States”, November 2004)//DG

Iran: U.S. national security experts have included Iran on a published list of countries said to be training elements of the population in cyber warfare. The leadership in Tehran is known to sponsor terrorist groups and for many years has chafed in the face of perceived Iranian inadequacy in the conduct of modern information warfare. Although the rhetoric of the clerical regime has been more prudent in recent years (at least until recently), the government nevertheless continues to accord economic and political priority to extending the technological threshold of its defense sector. This is illustrated in two ways: first, the armed forces and technical universities have joined in an effort to create independent cyber R & D centers and train personnel in IT skills; and second, Tehran actively seeks to buy IT and military related technical assistance and training from both Russia and India. Overall, we assess that Iran is leveraging its resources in the non-conventional weapons and IT sector as a “force multiplier” to gain greater influence in Central Asia.

### North Korea Impact Module

#### North Korea will destroy our cyberspace

Billo and Chang 4 (Institute for Security Technology Studies at Dartmouth College, Charles Billo and Welton Chang, “Cyber Warfare: the Analysis of the means and motivations of Selected Nation States”, November 2004)//DG

North Korea: Although U.S. national security officials include North Korea on a published list of countries believed to be developing information warfare units either in the military or the intelligence services, the open literature contains no North Korean military doctrinal or policy statement to that effect. South Korea’s defense community alleges cyber reconnaissance or network hacks sponsored by Pyongyang, but such charges may only represent “disinformation.” Due to the closed, Stalinist make-up of the North Korean regime and society, concrete evidence is difficult to obtain. There are few credible first-hand sources. We believe it is possible North Korea is experimenting with offensive cyber attack capabilities, based on Pyongyang’s track record of priority resource allocations to the military, its evident endowment of scientists and engineers, and its documented achievements in missile and related military technologies.

#### North Korean War goes nuclear

CNN 2003

[CNN, “N K. Warns of nuclear conflict,” 2/26/2003 , http://www.cnn.com/2003/WORLD/asiapcf/east/02/25/nkorea.missile/index.html]

Pyongyang cites upcoming U.S.-South Korean joint military exercises scheduled to begin on March 4, as "reckless war moves" designed to "unleash a total war on the Korean peninsula with a pre-emptive nuclear strike". "The situation of the Korean Peninsula is reaching the brink of a nuclear war," the statement, issued by the official Korean Central News Agency, says. The North also called on South Koreans to "wage a nationwide anti-U.S. and anti-war struggle to frustrate the U.S. moves for a nuclear war." The United States denies it has any plans to attack North Korea, consistently saying it is seeking a diplomatic and political solution to the increasing tensions sparked by Pyongyang's decision to reactivate its nuclear program. U.S. Secretary of State Colin Powell on Tuesday wrapped up a four-day tour of Japan, China and South Korea during which he lobbied Asian leaders to support a multi-lateral approach to pressure North Korea to abandon its nuclear ambitions. Powell repeated the U.S. position that it had no intention of invading North Korea and had no plans to impose fresh economic sanctions on the impoverished communist nation. While Japan and South Korea indicated they might support a regional initiative to sway Pyongyang, China -- a key ally and aid donor to the North -- appeared to remain unconvinced. China says the United States must deal with Pyongyang equally on a one-to-one basis. "We believe diplomatic, political pressure still has a role to play. And there are countries who have considerable influence with the North Koreans who will continue to apply pressure," Powell said Tuesday. "We also made it clear that if they begin reprocessing (nuclear material), it changes the entire political landscape. And we're making sure that is communicated to them in a number of channels." Powell would not be drawn on how would Washington react if Pyongyang did begin reprocessing but did say that the U.S. had "no intention of invading" North Korea. Tensions on the peninsula have been ratcheting up over the past few weeks with North Korea becoming increasingly provocative. On Monday, the North fired a short-range missile into the Sea of Japan, or East Sea, an act many believe was designed to upstage the inauguration of new South Korean President Roh Moo-hyun. ([Roh sworn in](http://www.cnn.com/2003/WORLD/asiapcf/east/02/24/skorea.inauguration.reut/index.html%22%20%5Ct%20%22_blank)) Last week, a North Korean MiG-19 fighter briefly flew into South Korean air space. ([MiG incursion](http://www.cnn.com/2003/WORLD/asiapcf/east/02/20/skorea.mig/index.html%22%20%5Ct%20%22_blank)) The North has also threatened to abandon the 1953 armistice that ended the fighting of the Korean War.

### Russia

#### Russia will infiltrate our vulnerable cyber space

Billo and Chang 4 (Institute for Security Technology Studies at Dartmouth College, Charles Billo and Welton Chang, “Cyber Warfare: the Analysis of the means and motivations of Selected Nation States”, November 2004)//DG

Russia: Russia’s armed forces, collaborating with experts in the IT sector and academic community, have developed a robust cyber warfare doctrine. The authors of Russia’s cyber warfare doctrine have disclosed discussions and debates concerning Moscow’s official policy. “Information weaponry,” i.e., weapons based on programming code, receives paramount attention in official cyber warfare doctrine. Moscow also has a track record of offensive hacking into Chechen websites. Although we assess it likely that Moscow will continue to scout U.S. military and private sector networks and websites, available evidence is inadequate to predict whether Russia’s intelligence services or armed forces would attack U.S. networks, especially after taking into account present-day political and economic ties between the two nations.

#### Russia-US conflict guarantees nuclear Armageddon – nuclear stockpiles

Bostrom Professor of philosophy at Yale, 2002

(Nick, Professor of Philosophy at Yale. “Existential Risks: Analyzing Human Extinction Scenarios and Related Hazards,” 2002, www.transhumanist.com/volume9/risks.html)

A much greater existential risk emerged with the build-up of nuclear arsenals in the US and the USSR. An all-out nuclear war was a possibility with both a substantial probability and with consequences that might have been persistent enough to qualify as global and terminal. There was a real worry among those best acquainted with the information available at the time that a nuclear Armageddon would occur and that it might annihilate our species or permanently destroy human civilization.[4] Russia and the US retain large nuclear arsenals that could be used in a future confrontation, either accidentally or deliberately. There is also a risk that other states may one day build up large nuclear arsenals. Note however that a smaller nuclear exchange, between India and Pakistan for instance, is not an existential risk, since it would not destroy or thwart humankind’s potential permanently.

### Generic Terrorism Terminal Impacts

#### Nuclear Terrorism leads to global nuclear war

Chesney, JD candidate at Harvard Law, 1997

 (Robert, Loyola of Los Angeles International & Comparative Law Journal, November)

The horrible truth is that the threat of nuclear terrorism is real, in light of the potential existence of a black market in fissile material. Nuclear terrorists might issue demands, but then again, they might not. Their target could be anything: a U.S. military base in a foreign land, a crowded U.S. city, or an empty stretch of desert highway. In one fell swoop, nuclear terrorists could decapitate the U.S. government or destroy its financial system. The human suffering resulting from a detonation would be beyond calculation, and in the aftermath, the remains of the nation would demand both revenge and protection. Constitutional liberties and values might never recover. When terrorists strike against societies already separated by fundamental social fault lines, such as in Northern Ireland or Israel, conventional weapons can exploit those fault lines to achieve significant gains. [n1](http://www.lexisnexis.com/us/lnacademic/frame.do?tokenKey=rsh-20.923397.6564759723&target=results_DocumentContent&reloadEntirePage=true&rand=1248188387888&returnToKey=20_T7002619888&parent=docview#n1) In societies that lack such pre-existing fundamental divisions, however, conventional weapon attacks do not pose a top priority threat to national security, even though the pain and suffering inflicted can be substantial. The bedrock institutions of the United States will survive despite the destruction of federal offices; the vast majority of people will continue to support the Constitution despite the mass murder of innocent persons. The consequences of terrorists employing weapons of mass destruction, however, would be several orders of magnitude worse than a conventional weapons attack. Although this threat includes chemical and biological weapons, a nuclear weapon's devastating [\*32]  potential is in a class by itself. [n2](http://www.lexisnexis.com/us/lnacademic/frame.do?tokenKey=rsh-20.923397.6564759723&target=results_DocumentContent&reloadEntirePage=true&rand=1248188387888&returnToKey=20_T7002619888&parent=docview#n2) Nuclear terrorism thus poses a unique danger to the United States: through its sheer power to slay, destroy, and terrorize, a nuclear weapon would give terrorists the otherwise-unavailable ability to bring the United States to its knees. Therefore, preventing terrorists from obtaining nuclear weapons should be considered an unparalleled national security priority dominating other policy considerations.

#### Nuclear terrorism will cause global nuclear war, leading to extinction

Sid-Ahmed, Egyptian political analyst for the Al-Ahram newspaper, 2004:

(Mohamed Sid-Ahmed, Egyptian political analyst for the Al-Ahram newspaper, Al-Ahram online, August 26, 2004,http://weekly.ahram.org.eg/2004/705/op5.htm)

A nuclear attack by terrorists will be much more critical than Hiroshima and Nagazaki, even if -- and this is far from certain -- the weapons used are less harmful than those used then, Japan, at the time, with no knowledge of nuclear technology, had no choice but to capitulate. Today, the technology is a secret for nobody. So far, except for the two bombs dropped on Japan, nuclear weapons have been used only to threaten. Now we are at a stage where they can be detonated. This completely changes the rules of the game. We have reached a point where anticipatory measures can determine the course of events. Allegations of a terrorist connection can be used to justify anticipatory measures, including the invasion of a sovereign state like Iraq. As it turned out, these allegations, as well as the allegation that Saddam was harbouring WMD, proved to be unfounded. What would be the consequences of a nuclear attack by terrorists? Even if it fails, it would further exacerbate the negative features of the new and frightening world in which we are now living. Societies would close in on themselves, police measures would be stepped up at the expense of human rights, tensions between civilisations and religions would rise and ethnic conflicts would proliferate. It would also speed up the arms race and develop the awareness that a different type of world order is imperative if humankind is to survive. But the still more critical scenario is if the attack succeeds. This could lead to a third world war, from which no one will emerge victorious. Unlike a conventional war which ends when one side triumphs over another, this war will be without winners and losers. When nuclear pollution infects the whole planet, we will all be losers.

#### Terrorist attack risks extinction.

Alexander Prof and Director of Inter-University for Terrorism Studies 3

(Yonah, Terrorism Myths and Realities, Washington Times, Prof and Director of Inter-University

For Terrorism Studies)

Last week's brutal suicide bombings in Baghdad and Jerusalem have once again illustrated dramatically that the international community failed, thus far at least, to understand the magnitude and implications of the terrorist threats to the very survival of civilization itself. Even the United States and Israel have for decades tended to regard terrorism as a mere tactical nuisance or irritant rather than a critical strategic challenge to their national security concerns. It is not surprising, therefore, that on September 11, 2001, Americans were stunned by the unprecedented tragedy of 19 al Qaeda terrorists striking a devastating blow at the center of the nation's commercial and military powers. Likewise, Israel and its citizens, despite the collapse of the Oslo Agreements of 1993 and numerous acts of terrorism triggered by the second intifada that began almost three years ago, are still "shocked" by each suicide attack at a time of intensive diplomatic efforts to revive the moribund peace process through the now revoked cease-fire arrangements (hudna). Why are the United States and Israel, as well as scores of other countries affected by the universal nightmare of modern terrorism surprised by new terrorist "surprises"? There are many reasons, including misunderstanding of the manifold specific factors that contribute to terrorism's expansion, such as lack of a universal definition of terrorism, the religionization of politics, double standards of morality, weak punishment of terrorists, and the exploitation of the media by terrorist propaganda and psychological warfare. Unlike their historical counterparts, contemporary terrorists have introduced a new scale of violence in terms of conventional and unconventional threats and impact. The internationalization and brutalization of current and future terrorism make it clear we have entered an Age of Super Terrorism (e.g. biological, chemical, radiological, nuclear and cyber) with its serious implications concerning national, regional and global security concerns.

## Solvency – Current Legislation Solves

### Key to prevent Cyber Attack

#### Bipartisan cyber-security legislation solves cyber-attacks and protects infrastructure

Obama 7/19/12- President of the United States (Barack, “Taking the Cyberattack Threat Seriously”,Wall Street Journal, 7/19/12, http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html)//JY

Last month I convened an emergency meeting of my cabinet and top homeland security, intelligence and defense officials. Across the country trains had derailed, including one carrying industrial chemicals that exploded into a toxic cloud. Water treatment plants in several states had shut down, contaminating drinking water and causing Americans to fall ill. Our nation, it appeared, was under cyber attack. Unknown hackers, perhaps a world away, had inserted malicious software into the computer networks of private-sector companies that operate most of our transportation, water and other critical infrastructure systems. Fortunately, last month's scenario was just a simulation—an exercise to test how well federal, state and local governments and the private sector can work together in a crisis. But it was a sobering reminder that the cyber threat to our nation is one of the most serious economic and national security challenges we face. Enlarge Image Associated Press So far, no one has managed to seriously damage or disrupt our critical infrastructure networks. But foreign governments, criminal syndicates and lone individuals are probing our financial, energy and public safety systems every day. Last year, a water plant in Texas disconnected its control system from the Internet after a hacker posted pictures of the facility's internal controls. More recently, hackers penetrated the networks of companies that operate our natural-gas pipelines. Computer systems in critical sectors of our economy—including the nuclear and chemical industries—are being increasingly targeted. It doesn't take much to imagine the consequences of a successful cyber attack. In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home. Taking down vital banking systems could trigger a financial crisis. The lack of clean water or functioning hospitals could spark a public health emergency. And as we've seen in past blackouts, the loss of electricity can bring businesses, cities and entire regions to a standstill. This is the future we have to avoid. That's why my administration has made cybersecurity a priority, including proposing legislation to strengthen our nation's digital defenses. It's why Congress must pass comprehensive cybersecurity legislation. We all know what needs to happen. We need to make it easier for the government to share threat information so critical-infrastructure companies are better prepared. We need to make it easier for these companies—with reasonable liability protection—to share data and information with government when they're attacked. And we need to make it easier for government, if asked, to help these companies prevent and recover from attacks. Yet simply sharing more information is not enough. Ultimately, this is about security gaps that have to be filled. To their credit, many of these companies have boosted their cyber defenses. But many others have not, with some lacking even the most basic protection: a good password. That puts public safety and our national security at risk. The American people deserve to know that companies running our critical infrastructure meet basic, commonsense cybersecurity standards, just as they already meet other security requirements. Nuclear power plants must have fences and defenses to thwart a terrorist attack. Water treatment plants must test their water regularly for contaminants. Airplanes must have secure cockpit doors. We all understand the need for these kinds of physical security measures. It would be the height of irresponsibility to leave a digital backdoor wide open to our cyber adversaries. This approach stays true to our values as a society that cherishes free enterprise and the rights of the individual. Cybersecurity standards would be developed in partnership between government and industry. For the majority of critical infrastructure companies already meeting these standards, nothing more would be expected. Companies needing to upgrade their security would have the flexibility to decide how best to do so using the wide range of innovative products and services available in the marketplace. Moreover, our approach protects the privacy and civil liberties of the American people. Indeed, I will veto any bill that lacks strong privacy and civil-liberties protections. This is exactly the kind of responsible, collaborative approach to an urgent national-security challenge that Americans expect but that Washington too rarely provides. It reflects the insights and ideas of industry and civil libertarians. It is sponsored by a bipartisan group of senators. It is supported by current and former homeland security, intelligence and defense leaders from both Republican and Democratic administrations. Today we can see the cyber threat to the networks upon which so much of our modern American lives depend. We have the opportunity—and the responsibility—to take action now and stay a step ahead of our adversaries. For the sake of our national and economic security, I urge the Senate to pass the Cybersecurity Act of 2012 and Congress to send me comprehensive legislation so I can sign it into law. It's time to strengthen our defenses against this growing danger.

#### Cyber-security key to solving cyber-attacks- prevents instability and collapse

Daily Mail 12- (“Cyber attacks now fourth biggest threat to global stability, says World Economic Forum”, Daily Mail UK, 1/12/12, http://www.dailymail.co.uk/news/article-2085876/Cyber-attacks-fourth-biggest-threat-global-stability-says-World-Economic-Forum.html)//JY

A report from the World Economic Forum (WEF) shows cyber attacks on governments and businesses are considered to be one of the top five risks in the world. The report, Global Risks for 2012, examined 50 global risks in the areas of the economy and the environment and in geopolitics, society and technology, and was based on interviews with more than 460 experts from industry, government and specialist areas. The international organisation concluded from its research that fourth on the list of Top 5 Global Risks in terms of likelihood is cyber attacks. Risk: The WEF has concluded that fourth on the list of Top 5 Global Risks in terms of likelihood are cyber attacks 'Severe income disparity' was at number one, second-placed was 'chronic fiscal imbalances' and concern about rising greenhouse gas emissions was third-placed. Fifth on the list was 'water supply crises'. Experts said they were most afraid of cyber attacks that might spark malfunctions in power plants, water supplies and other critical systems, but added that the likelihood of this was still relatively low. More... Global financial crisis 'threatens to drag the world back to the 1930s' 'Twitter needs to do more to protect children from abuse and exploitation' Steve Wilson, chief risk officer for general insurance at Zurich, who contributed to the report, said the biggest concern for the WEF was the complexity of internet security. The report, which aims to look at the next 10 years in terms of risk, points out that due to the speed of technological developments, it is difficult to keep up with security. British Prime Minister David Cameron addresses the World Economic Forum (WEF) at its annual meeting in Davos The WEF dossier says: 'A healthy digital space is needed to ensure stability in the world economy and balance of power' and calls for investment into the exploration of digital vulnerabilities. The UK government has already made a start in this area with its Cyber Security Strategy published at the end of 2011. The strategy announced on 25 November 2011, outlined how the government intends to spend £650m earmarked for cyber security and introduced a Cyber Crime Unit, which the government wants to be set up by 2013. The document sets out plans for greater information sharing between government and private sector on threats and the creation of 'an easy-to-use single point for reporting cyber fraud' to encourage victims to report crime more readily. Although technological concerns is in the Top 5 most likely risks this year for the first time since 2007, experts are still most worried about the ongoing financial crises around the world. With severe income disparity topping of the list, the report says: 'There is a sense of receding hope for future prospects...discontent is exacerbated by the starkness of income disparities: the poorest half of the global population owns barely 1 per cent of the global wealth, while the world’s top 1 per cent owns close to half of the world’s assets.' Gallup data from 2011 reveals that, globally, people believe living standards are falling and express diminishing confidence in the ability of their government to reverse the trend.

#### Cyber-security legislation key to prevent cyber attacks- short timeframe

GCN 4/24/12- Government Computer News (William Jackson, “Major Cyberattack on U.S. ‘inevitable’, experts tell Congress”, Government Computer News, 4/24/12, http://gcn.com/Articles/2012/04/24/Cybersecurity-hearing-major-attack-inevitable.aspx?s=gcndaily\_250412&Page=1)//JY

A panel of cybersecurity professionals warned lawmakers that voluntary guidelines for securing the nation’s critical infrastructure have not worked and that Congress must pass strong cybersecurity legislation that sets basic security standards in order to avoid a damaging cyberattack. “If we don’t do that this year, an attack is inevitable,” James Lewis, a senior fellow at the Center for Strategic and International Studies, told a House Homeland Security Committee's Oversight, Investigations and Management Subcommittee during the April 24 hearing. Rep. Michael McCaul (R-Texas), the subcommittee's chairman, called the hearing in advance of scheduled debate and votes later this week on three cybersecurity bills introduced by Republican legislators. Related coverage: Bipartisan cyber bill now the center of partisan turf war Democrats on the subcommittee criticized the bills as dangerously broad and ineffective because they encourage sharing of information between government and industry without privacy safeguards, do not require security standards for privately owned networks, and undermine the role of the Homeland Security Department in protecting critical infrastructure. The panel of government, former government, academic and private-sector professionals told the subcommittee that America is at risk of losing its technological leadership and economic competitiveness and that national security is being jeopardized by an onslaught of online espionage and theft. Despite the urgency, however, Lewis was not optimistic about the chances for passing strong legislation. “If I have learned anything this year, it is that you shouldn’t try to move major legislation in an election year,” he said. Shawn Henry, who until this month was executive assistant director of the FBI’s Criminal, Cyber, Response and Services Branch, said that networks are not defensible and that operators need to assume that they have or will be compromised. “The threat has reached the point that a determined adversary will access any system that is directly accessible from the network,” said Henry, who now is president of CrowdStrike Services, a cybersecurity intelligence start-up. “They will keep coming until they come in.” He called the drumbeat of cyber crime reports that have been made public “the tip of the iceberg” and that the real threat lies “below the waterline” in the classified arena. “The public sees the tip,” he said. “I have seen below the waterline.” He said that nation-states are gathering data on our next generation of weapons and are developing capabilities to counter them. Stephen Flynn, founding co-director of Northeastern University’s George J. Kostas Research Institute for Homeland Security, criticized the government for working too much “below the surface” and said greater candor was needed in dealing with cyber threats. “Err on the side of openness,” he advised. McCaul identified China and Russia as our most aggressive cyber adversaries, accusing both of military and industrial espionage. But Lewis said they are not the greatest threat. “I don’t worry about China and Russia,” he said. “They aren’t going to start a war just for fun. I don’t know if we can say that for Iran and North Korea.” Both of those nations are working to achieve a cyber war capability, Lewis said, and reconnaissance and attack tools are becoming more powerful and being commoditized by criminals and hackers, lowering the bar for countries that would like to enter the fray. “The greatest threat to cybersecurity in the United States is complacency.” Although witnesses and lawmakers alike agreed on the urgency of the cyber threat and the need for action, there remained divisions on what action to take. Previous panels of private-sector executives have warned legislators that industry needs to be left free of regulations in order to innovate and adapt to changing threat landscapes. But this panel took a different tack. “At the end of the day, purely voluntary approaches will not get us where we need to be,” Flynn said. “We know what to do to solve the problem,” said McAfee Chief Technology Officer Stuart McClure. “It’s a matter of getting people to do it.” A Republican task force on cybersecurity legislation last year recommended that Congress take a non-regulatory, piecemeal approach to cybersecurity rather than considering comprehensive legislation that would empower DHS to establish security requirements for privately owned infrastructure. The House is scheduled to vote April 26 on three of the bills resulting from the task force: HR 4257, sponsored by Oversight and Government Reform Subcommittee Chairman Rep. Darrell Issa, (R-Calif.), which would update a 2002 law governing the defenses of federal networks. HR 2096, sponsored by McCaul (R-Texas), to boost research and development for cybersecurity, focusing on defenses against threats. HR 3834, sponsored by Rep. Ralph Hall (R-Texas), to boost research and development on cybersecurity, focusing on general IT.

#### Cyber-security bill solves attacks- security measures

Langevin Press Release 11- U.S. Congressman Jim Langevin (“Langevin Introduces Bill to Strengthen Cybersecurity, Prevent Attacks”, U.S. Congress, 3/16/11, http://langevin.house.gov/news/press-releases/2011/03/langevin-introduces-bill-to-strengthen-cybersecurity-prevent-attacks.shtml)//JY

Congressman Jim Langevin (D-RI), co-founder of the Congressional Cybersecurity Caucus, is introducing legislation today to significantly strengthen protections against dangerous cyber threats. The Executive Cyberspace Coordination Act would establish a National Office for Cyberspace to evaluate and enforce requirements for federal agencies to protect themselves and the public, make certain that the government buys the most advanced and secure technology possible, and train a workforce with the ability to defend us against attacks. Langevin’s proposals would address the troubling report released last month revealing that in the past two years little was done to protect our power grid and critical infrastructure from unprecedented damage. The bill has received bipartisan support, including co-sponsorship by: Rep. Roscoe Bartlett (R-MD), a senior member of the House Armed Services Committee (HASC); C.A. Dutch Ruppersberger (D-MD), Ranking Member of the House Permanent Select Committee on Intelligence; and Loretta Sanchez (D-CA), Ranking Member of the HASC Strategic Forces Subcommittee and a senior member of the House Committee on Homeland Security. “Our nation sits at a crucial moment, where cyber attacks are common, but have not yet significantly impacted or endangered the American way of life,” said Langevin. “As the Director of the CIA said at a hearing last month, ‘This is the battleground for the future.’ Those charged with protecting the American people must be vigilant and responsive as serious threats grow, whether they come from practices on Wall Street, poor environmental safeguards or cyberspace. In this case, we have the opportunity to improve prevention and response to cybersecurity threats, but we must take action now.” Langevin’s legislation would accelerate the sluggish progress in cybersecurity on the heels of the second version of a report by the CSIS Commission on Cybersecurity for the 44th Presidency, which Langevin co-chaired. The report found that we are “still unprepared” to meet the challenges of securing cyberspace and “many important actions have been deferred.” (The full review can be read at: http://csis.org/files/publication/110128\_Lewis\_CybersecurityTwoYearsLater\_Web.pdf.) In a February 10th hearing held by the House Intelligence Committee on which Langevin sits, CIA Diretor Leon Panetta and Director of National Intelligence James Clapper described the United States’ vulnerability to terrorist attacks on the country’s computer networks that could shut down government agencies, power grids or financial markets. Panetta told the Committee, “The next Pearl Harbor may very well be a cyber attack,” and warned that Russia, China, Iran and other countries had begun developing capacities to launch cyber attacks. This bill particularly expands Langevin’s past efforts by dealing with the lack of young people entering the job market with the math and science skills necessary to keep up with ever-changing cyber threats. In February, he announced the launch of the Rhode Island Cyber Foundations Competition to test the computer networking skills of high school students, while introducing them to the field of information technology. This bill would require that programs address these goals nationally at the secondary and post-secondary education levels. Among the top ten recommendations of the CSIS report that this legislation addresses directly are: Developing coherent organization and leadership for federal efforts for cybersecurity and recognition of cybersecurity as a national priority; Providing clear authority to mandate better cybersecurity in critical infrastructure and develop new ways to work with the private sector; Building an expanded workforce with adequate cybersecurity skills; Enhancing outdated Federal Information Security Management Act (FISMA) policies; and Changing federal acquisition policy to drive the market toward more secure products. The Executive Cyberspace Coordination Act includes provisions to: Establish a National Office for Cyberspace (NOC) The NOC, within the Executive Office of the President, will coordinate and oversee the security of agency information systems and infrastructure. This office will have strong budgetary oversight powers that are backed by financial pay-for-performance authorities, while remaining accountable to Congress. Federal agencies will be responsible for reporting on their information security threats, practices and history to the NOC before submission of their budgets to OMB. The Director of the NOC would be appointed by the President, subject to Senate confirmation, and will also have a seat on the National Security Council. This will allow the Director to review agency information security budgets and make recommendations back to the Agencies as well as the President. Create secure federal acquisition policies The bill requires development of secure acquisition policies to be used in the procurement of information technology products and services, including a vulnerability assessment for any major system and its significant items of supply prior to development. Improve our workforce by establishing Cyber Challenge Programs Given the great deficiency of advanced cybersecurity capabilities in today’s workforce, it is imperative that the government support educational programs designed to engage students in the skill sets that they will need to keep our country competitive and safe online into the future. Cement FISMA Reforms The legislation includes requirements for agencies to undertake automated and continuous monitoring of their systems to ensure compliance and identify deficiencies and potential risks caused by cyber incidents or threats to an agency's information technology assets. These activities are intended to move agencies away from current manually intensive, compliance focused, periodic assessments. Require annual independent audit of federal agencies Agencies must obtain an annual independent audit of their information security programs to determine their overall effectiveness and compliance with FISMA. Audits would also be required of contractors responsible for managing agency systems or programs on their behalf. Additionally, the legislation will: Establish a Federal Cybersecurity Practice Board This Board within the NOC will develop policies and procedures for agencies to meet FISMA requirements and to oversee the implementation of approved standards and guidelines by the National Institute of Standards and Technology. The Board would be chaired by the Director of NOC, and include standing members from OMB, DoD, and selected members from civilian and law enforcement agencies. Establish Office of the Chief Technology Officer The Chief Technology Officer within the Executive Office of the President will work collaboratively across the government and private sector to analyze and improve the use of information technology. The head of this Office, the Federal Chief Technology Officer (Federal CTO), would be appointed by the President and subject to Senate confirmation. In addition, the Federal CTO would also be a standing member of the Cybersecurity Practice Board outlined above. Grant authority to protect critical infrastructure Homeland Security Presidential Directive-7 provides authority to the Secretary of Homeland Security to coordinate the protection of critical infrastructure. This bill clarifies this authority to include the creation, verification, and enforcement of measures with respect to the protection of the information systems that control critical infrastructure. This does not give DHS control over private systems, but it allows them to establish risk-informed security practices and standards for critical infrastructure. Develop better cooperation across agencies The bill brings the Departments of Defense and Homeland Security to the table to better coordinate their resources under the appropriate authority of the Office of the President. Define the sectors of our society that most urgently need protection The Secretary of Homeland Security will determine what critical infrastructure should fall under cyber regulation and receive new protections developed between industry and government, recognizing that not every part of our critical infrastructure is as vulnerable to cyber threats as our power grid is. Enhance the Public Private Partnership for Critical Infrastructure The bill requires DHS to work with the Departments of Defense and Commerce, the National Institute of Standards and Technology and the sector specific Federal regulatory agencies to establish standards to protect critical infrastructure. These efforts will also be carried out with the consultation of appropriate private sector bodies, including private owners and operators of the infrastructure affected. This will ensure that standards are based on the recommendations of cyber experts as well as those with first hand knowledge of the reality of the challenges facing each industry. Ensure the above protections are carried out The bill provides the authority to ensure these standards and practices are carried out. Coordinating through a new National Office for Cyberspace in the Executive Office of the President, DHS will work with sector-specific Federal regulators to establish enforcement mechanisms. These include the ability to conduct security audits or issue subpoenas to determine compliance with regulatory requirements for securing critical infrastructure.

### Key to protect Infrastructure

#### Cyber-security solves case- protects infrastructure from attack

NewsMax 7/24/12- (Henry J. Reske and John Bachmann, “Lieberman Worried That Cyber Attack Could Be Imminent”, NewsMax, 7/24/12, http://www.newsmax.com/TheWire/cyber-attacklieberman-bill/2012/07/24/id/446429)//JY

Congress must pass the Cybersecurity Act of 2012 if the United States hopes to prevent a cyberspace version of the Pearl Harbor attack that could cripple key electrical and transportation systems, the bill’s sponsor Sen. Joe Lieberman tells Newsmax.TV in an exclusive interview. The independent Connecticut senator, who is chairman of the Senate Homeland Security Committee, reintroduced a version of the still-controversial measure July 19. The revised version is designed to address concerns from the right and left about government regulation and privacy and the new measure has so far gained the support of President Barack Obama. To Lieberman, the goal of the bill is simple: to protect the electric grid, water systems, financial networks, and transportation systems from cyberattacks. Story continues below. “The threat is extremely dire,” Lieberman said. “I am literally worried that an attack could be imminent. We know that both states, countries like China, Russia and Iran are constantly probing our cyber networks, both government and private, and both civilian and defense. "We know that countries and terrorist groups and organized crime groups are constantly trying to steal industrial secrets form American companies that they’ve invested millions in, sometimes billions in, to basically get it for nothing and then create those industries and jobs over in other countries. “Leon Panetta the Secretary of Defense has said that he’s convinced that the next Pearl Harbor like attack on America will be launched from cyber space and there’s some countries out there who are prepared and have the capability to do it now. I just think we’ve got to raise our guard and if we work together we can.” Lieberman also noted that Gen. Keith Alexander, head of the National Security Agency in Cyber Command, said recently that theft over the Internet has amounted now to the largest involuntary transfer of money in the history of the world, as much as $1 trillion. “We’re very vulnerable to attack and some of the private owners of critical cyber infrastructure, like the electric grid or the financial system, banking systems, transportation, water,” he said. “Some of them are doing a pretty good job at defending their cyberspace, but some are not, and the main aim of this bill is to make sure that the private owners – 85 percent of our infrastructure … are taking steps to defend the cyberspace they own because that may well represent defense of our country. “ To assuage concerns from Republicans that the measure would add yet another layer of regulation on private businesses, Lieberman, along with cosponsor Sen. Susan Collins, R-Maine, removed “mandatory, regulatory sections” and instead offered incentives to comply. Nonetheless, he acknowledged if he had the votes he would have stayed with the mandatory provisions. “I want to get something done to begin to raise our defenses,” he told Newsmax. “So what are the incentives? The most explicit in our bill is that we say specifically if any company that complies with these standards, voluntarily, is sued after a cyber-attack, they will be immune from liability for punitive damages, and those are usually the ones that really blow up the bill for companies that are sued." To address privacy concerns from Democrats, the bill sets up a National Cyber Security Council that does not have direct involvement the military or national security agencies. “We wanted to set up a system where, to the greatest extent we possibly could, we guarantee people that their privacy would not be compromised, their personal privacy, in pursuit of making the country safer from cyber-attack,” he said. “We’ve done that.” Lieberman said the measure has the support of the “major security officials of the last two administrations,” including President George W. Bush’s Secretary of Homeland Security, Michael Chertoff, and his director of National Intelligence, Admiral Mike McConnell.

#### Cyber Security is key to maintaining infrastructure

Chertoff, 2006 – Secretary of the Department of Homeland Security (Michael, “National Infrastructure Protection Plan”, Department of Homeland Security, 3/17/6 ,http://www.scd.hawaii.gov/documents/ NationalInfrastructure ProtectionPlan.pdf) //AK

**The U.S. economy and national security are highly dependent upon the global cyber infrastructure.** **Cyber infrastructure enables all sectors’ functions and services, resulting in a highly interconnected and interdependent global network of CI/KR; A spectrum of malicious actors could conduct attacks against the cyber infrastructure using cyber attack tools. Because of the interconnected nature of the cyber infra- structure, these attacks could spread quickly and have a debilitating impact**; The use of innovative technology and interconnected networks in operations improves productivity and efficiency, **but also increases the Nation’s risk to cyber threats if cyber security is not addressed and integrated appropriately**; The interconnected and interdependent nature of the Nation’s CI/KR makes it problematic to address the protection of physical and cyber assets independently; **Cyber security includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability**. Cyber security also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster; and The NIPP addresses reducing cyber risk and enhancing cyber security in two ways: (1) as a cross-sector cyber element that involves DHS, SSAs, and private sector own- ers and operators; and (2) as a major component of the Information Technology sector’s responsibility in partner- ship with the Telecommunications sector.

#### Maintaining our critical infrastructure is key to solve the economy, terrorism, natural disasters, and overall crisis

Chertoff, 2006 – Secretary of the Department of Homeland Security (Michael, “National Infrastructure Protection Plan”, Department of Homeland Security, 3/17/6 ,http://www.scd.hawaii.gov/documents/ NationalInfrastructure ProtectionPlan.pdf) //AK

**America is an open, technologically sophisticated, highly interconnected, and complex Nation with a wide array of infrastructure that spans important aspects of U.S. Government, economy, and society**. The majority of the CI/KR-related assets, systems, and networks are owned and operated by the private sector. In some sectors, however, such as Water and Government Facilities, the majority of own- ers and operators are government or quasi-governmental entities**. The great diversity and redundancy of the Nation’s CI/KR provide for significant physical and economic resilience in the face of terrorist attacks, natural disasters, or other emergencies, and contribute to the unprecedented strength of the Nation’s economy.** However, this vast and diverse aggregation of highly interconnected assets, systems, and networks may also present an attractive array of targets to ter- rorists and magnify greatly the potential for cascading failure in the wake of catastrophic natural or manmade disasters**. Improvements in protection focusing on prioritized elements of CI/KR deemed nationally critical through implementation of the NIPP can make it more difficult for terrorists to launch attacks and lessen the impacts of any attack or other disaster that does occur.**

#### Cybersecurity Bill Will Strengthen Security- Cybersecurity key to Critical Infrastructure and Economic Security

Clayton, 12- Staff writer at Southern Arizona News- Examiner ( Mark, “Cybersecurity: Does Senate deal on legislation compromise defenses?”, 7/20, http://www.bis.doc.gov/news/2004/cybersecurityspeech.htm)//JH

|  |
| --- |
|  |

In a desperate bid to get a cybersecurity bill passed before Congress adjourns in August, Senate hawks seeking to protect vital national assets like the power grid blinked – offering up compromise legislation that substitutes voluntary measures for government mandates. Under the compromise, unveiled late Thursday, operators of gas pipelines, refineries, water supply systems and other physical assets vital to modern life in the US would voluntarily submit their computer networks to testing by the Department of Homeland Security. In return, they would get protection from financial liability in case of a devastating cyberattack. Key to the revamped version of the Cybersecurity Act is a public-private partnership – a multi-agency National Cybersecurity Council – chaired by the secretary of Homeland Security. It would assess risks and vulnerabilities, but allow industry to recommend voluntary practices to deal with cyberthreats. Standards would be reviewed, modified or approved by the council. Industry could also show their systems to be secure through self-certification or third-party assessment. The companies would then be eligible for liability protection. "We are going to try carrots instead of sticks as we begin to improve our cyberdefenses," Sen. Joe Lieberman (I) of Connecticut, a co-sponsor of the legislation, said in a statement. "This compromise bill will depend on incentives rather than mandatory regulations to improve America's cybersecurity. If that doesn't work, a future Congress will undoubtedly come back and adopt a more coercive system." While he acknowledged the bill previously introduced in February by himself and Sen. Susan Collins (R) of Maine "is stronger," Lieberman said the new "compromise will significantly strengthen the cybersecurity of the nation’s most critical infrastructure and with it our national and economic security."

### Solvency: India Relations

#### Cybersecurity Bill Key to US- India Relations- without Security we run risk of backlash

Juster, 4- Under Secretary of Commerce United States Government at the India-U.S. Information Security Summit 2004(Kenneth I.,” Cybersecurity: A Key to U.S.-India Trade”, 10/12, <http://www.bis.doc.gov/news/2004/cybersecurityspeech.htm>)//JH

Information security – also known as cybersecurity – is one of the keys to unlocking the full potential of the trade and technology relationship between the United States and India. All levels of society today – from individuals, to companies, to governments – rely on information technology and information networks in their daily lives – to communicate, to manage activities, to transact business, and to provide essential services to the public. As commerce between the United States and India continues to expand, consumers and corporations will seek to ensure that their personal information and business proprietary data are secure, and that information services are reliable and protected. Without an adequate level of security, we run the risk of backlash among consumers and loss of confidence among business people, which could severely limit progress in our trade and technology relationship.  This conference provides an ideal venue to consider these issues and focus on best practices for improving cybersecurity policies in the public and private sectors. I want to thank the two principal sponsors who have organized this conference – the National Association of Software and Service Companies (NASSCOM) and the Information Technology Association of America (ITAA). In addition, I would like to recognize the support provided by the various ministries and departments of the Indian and U.S. governments that are participating in this conference. I might add that I am particularly pleased to be sharing the podium this afternoon with Minister Sibal. His brother, former Foreign Secretary Kanwal Sibal, joined me in November 2002 in launching the U.S.-India High Technology Cooperation Group, which has played an important role in promoting bilateral trade and, more broadly, U.S.-Indian relations. It augurs well for our success that Kanwal’s brother Kapil is now also a joint venture partner in this collaboration. I would like to begin this afternoon by addressing the relationship between international trade and security. I will then focus on the critical of role of cybersecurity in the U.S.-India trade and technology relationship, on our joint efforts to enhance cybersecurity, and on the importance of working in partnership with private industry to develop and implement cybersecurity policies and practices. International Trade and Security  As Under Secretary of Commerce in the U.S. Government, I oversee the Bureau of Industry and Security. As our name suggests, we are responsible for issues where business and security intersect. These include strategic trade controls, imports and foreign acquisitions that affect U.S. security, and industry compliance with international arms control agreements.  One of the basic truths that I have learned in managing these issues is that international trade can only flourish if it is built on a solid foundation of security. Indeed, in today’s world, trade and security are more closely intertwined than ever before. While globalization has brought increased trade and economic interaction, which have contributed to economic growth and the generation of wealth, it has also presented new threats and new risks. Many of the forces that drive globalization and facilitate commerce – such as our globally integrated information and communication networks, transportation systems, and financial networks – can also be used by criminals and terrorists to threaten our security and our economic well being. That is why trade and security must be pursued in tandem; they are and must be seen as complementary rather than competing mandates. The U.S.-India High Technology Cooperation Group  It is this principle – security as the foundation for trade – that drives the growing high-technology relationship between the United States and India. As the United States and India expand economic interaction, each partner must have confidence that the other will protect the privacy of personal and financial data, protect the rights of intellectual property holders, and not permit the diversion of sensitive goods and technologies to unauthorized destinations or inappropriate users. If these security concerns are properly addressed, then I firmly believe that we will continue to see an upward trajectory in our trade and technology relationship.

### Solvency: Transportation Infrastructure

#### Cybersecurity Bill Key to Transportation Infrastructure- Banks, postal, energy sectors, etc.

DHS, 6/15/12- Department of Homeland Security for The USFG, (Communications Sector: Critical Infrastructure, http://www.dhs.gov/files/programs/gc\_1189102978131.shtm) // JH

The Communications Sector is an integral component of the U.S. economy underlying the operations of all businesses, public safety organizations, and government. Over 25 years, the sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry using terrestrial, satellite, and wireless transmission systems. The transmission of these services has become interconnected; satellite, wireless, and wireline providers depend on each other to carry and terminate their traffic and companies routinely share facilities and technology to ensure interoperability. The responsibility for protecting Communications Sector infrastructure and assets lies mostly within the private sector, because most communications infrastructure is privately owned. Working with the federal government, owners and operators are able to predict, anticipate, and respond to sector outages and understand how they might affect the ability of the national leadership to communicate during times of crisis, impact the operations of other sectors, and affect response and recovery efforts. The Communications Sector is closely linked to other sectors, including: [The Energy Sector](http://www.dhs.gov/files/programs/gc_1189013411585.shtm) provides power to run cellular towers, central offices, and other critical communications facilities; [The Information Technology Sector](http://www.dhs.gov/files/programs/gc_1188479464996.shtm) provides critical control systems and services, physical architecture and Internet infrastructure; [The Banking and Finance Sector](http://www.dhs.gov/files/programs/gc_1188566544964.shtm) relies on telecommunications for the transmission of transactions and operations of financial markets; [The Emergency Services Sector](http://www.dhs.gov/files/programs/gc_1189094187811.shtm) depends on telecommunications for directing resources, coordinating response, alerting the public, and receiving emergency 911 calls; and [The Postal and Shipping Sector](http://www.dhs.gov/files/programs/gc_1188412546210.shtm) uses telecommunications for its control systems, tracking shipments, and regular communications requirements.

#### Cybersecurity Bill Key to Transportation Infrastructure and Economy-Key to Next gen, electrical grid, rails and more

Collin, No date- Institute for Security and Intelligence, (Barry C., “The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge”, http://afgen.com/terrorism1.html)//JH

A CyberTerrorist will remotely access the processing control systems of a cereal manufacturer, change the levels of iron supplement, and sicken and kill the children of a nation enjoying their food. That CyberTerrorist will then perform similar remote alterations at a processor of infant formula. The key: the CyberTerrorist does not have to be at the factory to execute these acts. A CyberTerrorist will place a number of computerized bombs around a city, all simultaneously transmitting unique numeric patterns, each bomb receiving each other's pattern. If bomb one stops transmitting, all the bombs detonate simultaneously. The keys: 1) the CyberTerrorist does not have to be strapped to any of these bombs; 2) no large truck is required; 3) the number of bombs and urban dispersion are extensive; 4) the encrypted patterns cannot be predicted and matched through alternate transmission; and 5) the number of bombs prevents disarming them all simultaneously. The bombs will detonate. A CyberTerrorist will disrupt the banks, the international financial transactions, the stock exchanges. The key: the people of a country will lose all confidence in the economic system. Would a CyberTerrorist attempt to gain entry to the Federal Reserve building or equivalent? Unlikely, since arrest would be immediate. Furthermore, a large truck pulling along side the building would be noticed. However, in the case of the CyberTerrorist, the perpetrator is sitting on another continent while a nation's economic systems grind to a halt. Destabilization will be achieved. A CyberTerrorist will attack the next generation of air traffic control systems, and collide two large civilian aircraft. This is a realistic scenario, since the CyberTerrorist will also crack the aircraft's in-cockpit sensors. Much of the same can be done to the rail lines. A CyberTerrorist will remotely alter the formulas of medication at pharmaceutical manufacturers. The potential loss of life is unfathomable. The CyberTerrorist may then decide to remotely change the pressure in the gas lines, causing a valve failure, and a block of a sleepy suburb detonates and burns. Likewise, the electrical grid is becoming steadily more vulnerable. In effect, the CyberTerrorist will make certain that the population of a nation will not be able to eat, to drink, to move, or to live. In addition, the people charged with the protection of their nation will not have warning, and will not be able to shut down the terrorist, since that CyberTerrorist is most likely on the other side of the world. Sadly, these examples are not science fiction. All of these scenarios can be executed today. As you may know, some of these incidents already have occurred in various nations. More of such acts will

### Answers To: Status Quo Solves

#### Current U.S. cyber security failing

Ferran 7/27- staff writer at ABC News (Lee, “America’s Failing Grade on Cyber Attack Readiness”, ABC News, 7/27/12, http://abcnews.go.com/Blotter/americas-terrible-failing-grade-cyber-attack-readiness/story?id=16870064#.UBL5SZpYt7F)//JY

The man in charge of America's cyber operations said that on a scale of one to 10, the nation's preparedness to deal with a major cyber attack on critical infrastructure sits at a dismal three. "Somebody who finds vulnerability in our infrastructure could cause tremendous problems," Army Gen. Keith Alexander, Director of the National Security Agency and chief of U.S. Cyber Command, told audience members at the Aspen Institute's annual security forum late Thursday, according to multiple reports. Alexander said that since 2009, attempted cyber attacks on the nation's infrastructure systems have risen seventeen-fold. "I'm worried most about power. I'm worried about water. I think those are the ones that need the most help," he said. Top current and former U.S. security officials have for years been decrying vulnerabilities in the computer networks of critical infrastructure industries from water treatment centers to electric power plants -- largely facilities owned and operated by private entities. In his remarks, Alexander reportedly pushed for greater role of government, specifically the Department of Homeland Security, in regulating security measures across industries. Two years ago, computer experts discovered Stuxnet, a cyber weapon of unprecedented power and complexity that was apparently designed to damage an Iranian nuclear facility. The worm had demonstrated what computer experts had long though possible but had never actually seen: computer code that was no longer confined to disrupting computer systems internally but could reach out and physically alter how a facility works, or potentially destroy it. Before the worm was alleged to have been a creation of a joint U.S.-Israeli cyber operation, other U.S. officials quickly realized that such a powerful cyber tool may be turned on the homeland. In a Senate Homeland Security committee hearing in November 2010, committee chairman Joe Lieberman (D.-Connecticut) warned the worm could be used as a "blueprint" for other "malicious hackers." Richard Clarke, former White House counterterrorism advisor, cyber security expert and ABC News consultant, said in January that since Stuxnet was a "plug-and-play" worm, other hackers or foreign governments could take it, modify it and turn it against the U.S. "You can take out certain components and put in others and you have a very powerful weapon that could be used against the electric power grid or any other system that has computers telling machines what to do," he said. "The best cyber weapon in the world has been spread around for other people to have copies of… I think it's very likely that somebody could do this." READ: Beware the Cyber Boomerang Months later, the Department of Homeland Security revealed that the original Stuxnet worm did manage to infiltrate a computer system in the U.S., but since it was only tailored to hit the Iranian nuclear facility, it didn't do any known damage to the American facility. READ: When Stuxnet Hit the Homeland Sean McGurk, a former DHS official who is now senior policy officer at the Industrial Controls Systems Information Sharing and Analysis Center, told a radio show in early June that he had already seen hackers modifying Stuxnet for their own uses. He also noted that as one of the most computer-reliant nations on the planet, the U.S. is also one of the most vulnerable. "Because everything from elevators to prison doors are controlled by computers in our country, these systems lend themselves to manipulation and potentially to destruction," he said. Since Stuxnet's discovery, cyber experts have found two other highly-sophisticated cyber weapons: [Duqu](http://abcnews.go.com/Blotter/stuxnet-returns-duqu-researchers-warn-similar-cyber-attack/story?id=14763854" \t "_blank), a cyber program built in the style of Stuxnet but for espionage rather than offensive operations, and [Flame](http://abcnews.go.com/Blotter/flame-cyber-attack-israel-largest-cyber-spy-weapon/story?id=16449339), the largest espionage program in history designed to capture any keystroke, image and conversation even near the infected system. Based on stunning similarities in the code of all three programs, researchers said they believe they were all created by either the same team, or at least teams of computer experts with access to each other's original work.

#### U.S. needs to overcome current vulnerability to cyber attacks

The Washington Post 7/25- (“Stockpiling arms against cyberattacks”, The Washington Post, 7/25/12, http://www.washingtonpost.com/opinions/going-on-the-offensive-against-cyberattacks/2012/07/25/gJQAke0x9W\_story.html)//JY

FRESH ALARMS are being sounded about the dangers of cyberattack, and they are serious enough to give pause. Evidence suggests an unprecedented wave of cyber-espionage, and theft is underway. A cyber-arms race is gathering steam. Unfortunately, the policy response is lagging. Gen. Keith B. Alexander, who heads the National Security Agency and U.S. Cyber Command, recently described the theft of intellectual property in cyberspace as “the greatest transfer of wealth in history.” He estimated that hundreds of billions of dollars have been lost by U.S. companies and institutions, “our future disappearing in front of us.” He warned of a coming shift in cyberattacks from “disruptive to destructive,” that is, from annoying Web site interruptions to damaging takedowns of financial systems or power grids. Mr. Alexander also said that, while the world’s population will be 7.3 billion by 2016, the world’s mobile device population will be 10 billion. “Our companies use these, our kids use these, we use these devices,” he said. “They’re not secure.” On July 10, cybersecurity experts James Mulvenon and Gregory Rattray unveiled a study that concludes “the current strategic cyber environment is fundamentally unstable.” Their message: Security concepts the United States has relied upon for decades, such as deterrence, may be weak or useless in the face of cyber-conflict, where offense dominates, preemption is impossible and assaults come at network speed. This instability is “highly dangerous” for the United States, which has “so much to lose” because it is heavily dependent on networks. If we have so much to lose, why is the response so tepid? The private sector stands at the front lines of the assault on intellectual property, especially the attacks on critical infrastructure, yet corporations are often loath to acknowledge that they have been looted, so they remain silent. This contributes to complacency. There is an urgent need for legislation to improve cooperation between the private sector and the U.S. government, which possesses valuable tools for fighting cyber-intrusions and malware. The House has acted, and compromise legislation proposed in the Senate would set voluntary security standards for companies that run critical infrastructure. The bill, though not optimal, would be a worthwhile start and should be passed. The global cyber-arms race is a reality. By deploying a computer worm known as Stuxnet in a covert operation intended to damage Iran’s equipment for enriching uranium, the United States crossed a line. Stuxnet was designed to do physical harm. What if other nations do the same — and do it to us? The U.S. government has revealed little about its offensive activities in this sphere. We think this is shortsighted. Two years ago, the National Research Council found that the government’s policy and legal framework for offensive cyber-programs was “ill-formed, undeveloped and highly uncertain.” Is it any different today? An open, vigorous debate is needed about the threat of cyberwar and the potential response. We had a decades-long debate about nuclear weapons, and it was healthy for the country and the world. We ought to bring the discussion about offensive cyber-conflict out of the shadows.

#### Status quo doesn’t solve cyber security- Intelligence report proves

Ewing 9/12/11- DoD Buzz Publisher, Political Reporter (Philip, “Is a cyber 9/11 inevitable?”, 9/12/11,[http://www.dodbuzz.com/2011/09/ 12/](http://www.dodbuzz.com/2011/09/%2012/)**is-a-cyber-911-inevitable/)** //AK

Another day, another report warning that the **U.S. is dangerously unprepared for the realities of 21st century cyber-warfare. Monday’s study, which was the subject of a story by AP’s Lolita Baldor and which is slated for full release in the coming weeks, doesn’t say anything you haven’t heard before: The computer networks of the military-industrial complex, and the U.S. generally, are very vulnerable to mischief and attack because the feds can’t talk amongst themselves and also can’t coordinate with the private sector.** The Intelligence and National Security Alliance says the dramatic **expansion of sophisticated cyber-attacks has moved beyond acceptable losses for government and businesses that simply threaten finances or intellectual property.** “**The impact has increased in magnitude, and the potential for catastrophic collapse of a company has grown**,” said the report, which is slated to be released later this month. It adds that it is not clear that the business community understands or accepts that. **The report comes amid growing worries the U.S. is not prepared for a major cyberattack, even as hackers, criminals and nation states continue to probe and infiltrate government and critical business networks millions of times a day.** But in Washington, when you say “The sky is falling and everyone’s responsible!” **that means no one will pay attention, because no one person’s job is on the line.** When Adm. Thad Allen was the commandant of the Coast Guard, he used to say the U.S. needed to have a “national discussion” about whether it wanted to continue permitting small vessels to operate mostly out of sight of state and federal regulators, given the terrorism dangers of having no “air traffic control system” for American coasts and waterways. Well, we didn’t have a “national discussion,” the Coast Guard didn’t get better monitoring or a more robust system for testing and licensing boaters, and the risk of a Mumbai-style terror attack remains. **Cyber-security and cyber-warfare are the same way: Every month brings another speech, or hearing, or white paper that points up the weaknesses of our American cyber-defenses, and calls for a “discussion” and “better coordination with industry,” and — you’ve heard it all.** Last year, a congressional report said that China had improperly redirected some 15 percent of the world’s Internet traffic through its systems in April 2010, for purposes about which we can only speculate. **Every time he gets a chance, Rhode Island Rep. Jim Langevin warns about the dangers of a so-called SCADA attack, in which a cyber-attacker might try to sabotage the supervisory control and data acquisition networks in a factory or power plant. In short, the cyber-security situation is roughly where terrorism was in the months before Sept. 11, 2001. The U.S. had been attacked several times, including at the World Trade Center; in Dar es Salaam and Nairobi; and in Yemen with the bombing of the destroyer USS Cole.** But the **threat of terror wasn’t truly driven home until the Sept. 11 attacks, which prompted massive federal reorganization, two wars, trillions in new spending and a “new normal” of electronic eavesdropping, heightened security, and all the rest of it.**

### Answers To: Legislation Doesn’t Solve International Cyberterrorism

#### Cyber Security is key to the DoD, global economy, International Security, technology, energy, and transportation

Department of Defense July 2011- US Federal Government (Department of Defense Strategy for Operating in Cyberspace, July 2011, <http://www.defense.gov/news/d20110714cyber.pdf>) //AK

**Cyberspace is a defining feature of modern life.** Individuals and communities worldwide connect, socialize, and organize themselves in and through cyberspace. **From 2000 to 2010, global Internet usage increased from 360 million to over 2 billion people.** As Internet usage continues to expand, cyberspace will become increasingly woven into the fabric of everyday life across the globe. **U.S. and international businesses trade goods and services in cyberspace, moving assets across the globe in seconds. In addition to facilitating trade in other sectors, cyberspace is itself a key sector of the global economy. Cyberspace has become an incubator for new forms of entrepreneurship, advances in technology, the spread of free speech, and new social networks that drive our economy and reflect our principles.** **The security and effective operation of U.S. critical infrastructure – including energy, banking and finance, transportation, communication, and the Defense Industrial Base – rely on cyberspace, industrial control systems, and information technology that may be vulnerable to disruption or exploitation. Along with the rest of the U.S. government, the Department of Defense (DoD) depends on cyberspace to function.** It is difficult to overstate this reliance; DoD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe. DoD uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations. The Department and the nation have vulnerabilities in cyberspace. **Our reliance on cyberspace stands in stark contrast to the inadequacy of our cybersecurity – the security of the technologies that we use each day. Moreover, the continuing growth of networked systems, devices, and platforms means that cyberspace is embedded into an increasing number of capabilities upon which DoD relies to complete its mission.** Today, many foreign nations are working to exploit DoD unclassified and classified networks, and some foreign intelligence organizations have already acquired the capacity to disrupt elements of DoD’s information infrastructure. **Moreover, non-state actors increasingly threaten to penetrate and disrupt DoD networks and systems.** We recognize that there may be malicious activities on DoD networks and systems that we have not yet detected. **DoD, working with its interagency and international partners, seeks to mitigate the risks posed to U.S. and allied cyberspace capabilities, while protecting and respecting the principles of privacy and civil liberties, free expression, and innovation that have made cyberspace an integral part of U.S. prosperity and security.** How the Department leverages the opportunities of cyberspace, while managing inherent uncertainties and reducing vulnerabilities, will significantly impact U.S. defensive readiness and national security for years to come.

### AT: Risk Overstated

#### Threat is Real

Cloherty 12 (Writer for the NY times, Jack Cloherty, excerpt from NY Times “Virtual Terrorism: Al Quda Video calls for Electronic Jihad”, May 22 2012, <http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875#.UBA6cETiU3I//DG>)

Al Qaeda may be turning its destructive attention to cyber-warfare against the United States. In a chilling video, an al Qaeda operative calls for "electronic jihad" against the United States, and compares vulnerabilities in vital American computer networks to the flaws in aviation security before the 9/11 attack. The al Qaeda video calls upon the "covert mujahidin" to launch cyber attacks against the U.S. networks of both government and critical infrastructure, including the electric grid. The video was obtained by the FBI last year, and released today by the Senate Committee on Homeland Security and Governmental Affairs. "This is the clearest evidence we've seen that al Qaeda and other terrorist groups want to attack the cyber systems of our critical infrastructure," Homeland Security and Governmental Affairs Committee Chairman Joe Lieberman, I-Conn., said in a statement. "This video is troubling as it urges al Qaeda adherents to launch a cyber attack on America," said Sen. Susan Collins, R-Maine, the ranking member on the committee. "It's clear that al Qaeda is exploring all means to do us harm and this is evidence that our critical infrastructure is a target." The national security community says the threat of cyber attack is real, and the gap between terrorist aspirations and capability is closing. The senior intelligence official at Cyber Command, Rear Adm. Samuel Cox, has said al Qaeda operatives are seeking the capability to stage cyber attacks against U.S. networks and terrorists could purchase the capabilities to do so from expert criminal hackers. Increasing evidence also suggests that Iran is looking to commit cyber attacks against the United States, according to testimony last month before the House Committee on Homeland Security. Iran's sponsorship of terrorist groups takes on a new dimension in cyberspace, where it could develop a powerful cyber weapon and pass it on to a terrorist group. Lieberman is using the al Qaeda video to underline what he says is the need for new legislation.. "Congress needs to act now to protect the American public from a possible devastating attack on our electric grid, water delivery systems, or financial networks," he said. "As numerous, bipartisan national security experts have said, minimum cyber security standards for those networks are necessary to protect our national and economic security. That is why the Senate needs to act on our bipartisan Cyber Security Act that requires minimum security performance requirements for key critical infrastructure cyber networks." The Homeland Security Committee says the Department of Homeland Security received more than 50,000 reports of cyber intrusions or attempted intrusions since October, an increase of 10,000 reports over the same period the previous year.

# **Affirmative**

## Uniqueness

### Won’t Pass House

#### Cybersecurity has no chance of passing in the House- and Defense Authorization bill solves their offense anyway

The Hill, 7/23 (“McCain questions Reid's decision to take up cyber security bill before defense authorization”, 7/23/2012) [http://thehill.com/blogs/floor-action/senate/239527-mccain-questions-reids-decision-to-take-up-cyber-security-bill-instead-of-defense-authorization //](http://thehill.com/blogs/floor-action/senate/239527-mccain-questions-reids-decision-to-take-up-cyber-security-bill-instead-of-defense-authorization%20//) RM

Sen. John McCain (R-Ariz.) asked if Senate Majority Leader Harry Reid (D-Nev.) was “oblivious” to the national security needs of the country. “Can’t we as a body for the sake of those men and women who’s lives are on the line pass a defense authorization bill,” MccCain said on the floor Monday. “Is the Senate Majority Leader oblivious?” McCain urged Reid to allow a vote on the defense authorization bill. Instead Reid has indicated that the Senate would first vote on a cyber security bill — a decision McCain called “bizarre.” McCain said the cyber security bill, S. 2105, is flawed and won’t pass the in the House. “The Major Leader intends to rush through the Senate a flawed piece of legislation,” McCain said. “The cyber security bill is in great need of improvements … [and] it has zero chance of passing in the House of Representatives.” McCain said the defense authorization bill addresses cyber security needs among many others, which is why it would be better for those serving in the military. “For the life of me I do not understand why the Majority Leader should have so little regard for the men and women serving in the military today,” McCain said. The Cyber Security Act was introduced by Sen. Joseph Lieberman (I-Conn.) and is co-sponsored by Sens. Susan Collins (R-Maine), Dianne Feinstein (D-Calif.), John Rockefeller (D-W.Va.) and Sheldon Whitehouse (D-R.I.).

#### **Resistance in the House will prevent passage**

Romm, 7/24 – technology reporter for POLITICO (Tony, “Harry Reid urges action on cybersecurity”, POLITICO, 7/24/12, <http://www.politico.com/news/stories/0712/78926.html>) // EK

Senate Majority Leader Harry Reid on Tuesday defended his decision to address cybersecurity reform before the defense reauthorization — and he used the words of his chief critic on the timing, Sen. John McCain, as justification.¶ After McCain (R-Ariz.) slammed Reid’s legislative priorities on the floor Monday as “bizarre,” Reid opened the session Tuesday by recalling McCain’s own comments months ago about the need to protect power, water and air traffic control systems from cyberattacks.¶ Without the cybersecurity bill, Reid said, the vulnerabilities would put “our national security at risk.” He added that the absence of new protections “recklessly endangers our armed forces.”¶ McCain doesn’t support the approach to cybersecurity reform backed by Reid and other members. Sen. Joe Lieberman (I-Conn.) and other sponsors of the bill plan to emphasize the concessions they’ve made to win Republican support at a press conference later Tuesday.¶ McCain, however, said on the floor Monday the new measure is still flawed. While criticizing Reid’s decision not to turn to defense after the tax bill, McCain said cybersecurity reform has “zero chance of passing the House of Representatives or even ever being signed into law.”

Even if the president is pushing the bill, it won’t pass without compromise from congress
Wilhelm 7/21 – writer for TheNextWeb (Alexander, “The Senate Cybersecurity showdown is approaching: A preview” thenextweb.com, <http://thenextweb.com/us/2012/07/21/the-senate-cybersecurity-showdown-is-approaching-a-preview/>) //EW

So, the President is pushing Lieberman’s bill. That’s all well and good, but it can’t pass the House, unless Congress behaves in a way that it hasn’t for some time now. Thus, the President is urging the Senate to pass something that almost certainly can’t make it to his desk. This is either a dare to the House, to oppose the bill if it passes, or is an indirect push on the work being done to find a compromise. The President could be staking a position farther away from the middle than he might, just so that he can move towards the center, and appear to be compromising later. That’s politics. However, unless a compromise is reached that can pass both the Senate and House, we’re going to end up, possibly, with two bills from two houses that cannot be harmonized. Right back into the muck we go.

### Business Opposition

#### Business Leaders and U.S Chamber of Commerce oppose Bill

Treasury and Risk, 7/20 – (Dave Lindorff, “Businesses Push Back on Cybersecurity” Finance Magazine, 12, http://www.treasuryandrisk.com/2012/07/20/businesses-push-back-on-cybersecurity) // YL

In November 2011, hackers using an IP address in Russia attacked a water plant in Illinois. The hackers were able to turn a water pump on and off so frequently that it broke. While the incident caused no other damage and did not shut down the water system, it was the first known instance of a malicious foreign attack on this nation’s critical infrastructure, and it demonstrated how vulnerable such vital services as waterworks, the electrical grid, oil and gas pipelines and the telecom system are to hackers. It also lent urgency to efforts in Congress to enact legislation to make critical industries less vulnerable to attack.¶ For several years, Sen. Joe Lieberman (I-Conn.), pictured at right, has been trying to pass a cybersecurity bill that would resolve issues around privacy and the sharing of information among critical industries and the Department of Homeland Security, and also require Homeland Security to establish standards and a testing program to make sure those industries are taking the needed steps to harden their operations against cyberattacks.¶ His bill, the Cybersecurity Act of 2012, has been stalled by opposition from much of the business community, including the U.S. Chamber of Commerce. The Chamber objects to the measure’s emphasis on increased regulation. Lieberman’s office insists that the regulations would only apply to a narrow group of critical industries such as power companies and telecom companies, whose failure could be “devastating to the U.S. economy and even to people’s lives,” as one staffer puts it. Such companies, the staffer adds, are “already heavily regulated by the government.”

#### Businesses won’t support cyber security legislation – Mozilla proves

Greenberg 5/1/12 – information security and privacy reporter for Forbes (Andy, “Mozilla Slams CISPA, Breaking Silicon Valley’s Silence on Cybersecurity Bill”, Forbes, May 1, 2012) <http://www.forbes.com/sites/andygreenberg/2012/05/01/mozilla-slams-cispa-breaking-silicon-valleys-silence-on-cybersecurity-bill/> // ML

Late Tuesday, Mozilla’s Privacy and Public Policy lead sent me the following statement: While we wholeheartedly support a more secure Internet, CISPA has a broad and alarming reach that goes far beyond Internet security. The bill infringes on our privacy, includes vague definitions of cybersecurity, and grants immunities to companies and government that are too broad around information misuse. We hope the Senate takes the time to fully and openly consider these issues with stakeholder input before moving forward with this legislation. CISPA was introduced to the House in November with the intention of allowing more sharing of cybersecurity threat information between the private sector and the government, but has since been criticized for a provision that would also allow firms to share users’ private data with agencies like the National Security Agency or the Department of Homeland security without regard for any previous privacy laws. Time For Google To Speak Out Against CISPA Andy Greenberg Forbes Staff As House Passes CISPA, The Fight Is Just Beginning Andy Greenberg Forbes

### Won’t Pass - Generic

#### Won’t pass before August and no threat of Chinese cyber-attack

Osnos, 7/25 – staff writer and Chinese correspondent for the New Yorker {an interview of Adam Segal, a Maurice R. Greenberg Senior Fellow in China Studies at the Council on Foreign Relations; questions are noted in italics} (Evan, “Q. & A.: The Cybersecurity Bill, China, and Innovation”, The New Yorker, 7/25/12, <http://www.newyorker.com/online/blogs/evanosnos/2012/07/adam-segal-on-cybersecurity-china-and-innovation.html>) // EK

After years of debate, the Senate is set to take up a cyber-security bill that would force power companies and other vulnerable parts of the infrastructure to meet a certain level of security. President Obama is [backing](http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html) the bill, the Cybersecurity Act of 2012, as a response to “one of the most serious economic and national security challenges we face,” though it has been watered down in response to industry and G.O.P. critics who oppose mandatory standards (and it very well [might die](http://www.nationaljournal.com/tech/mccain-blasts-senate-cybersecurity-bill-as-flawed%E2%80%9420120723) in the House). China, meanwhile, is also [trying to defend](http://blogs.cfr.org/asia/2012/07/24/china-moves-forward-on-cybersecurity-policy/) itself against cyber threats. For more on this, and on how the U.S. and China stack up on technology innovation, I turned to [Adam Segal, the Maurice R. Greenberg Senior Fellow in China Studies](http://www.cfr.org/experts/china-innovation-cybersecurity/adam-segal/b8863) at the Council on Foreign Relations. He is the author of “[Advantage: How American Innovation Can Overcome the Asian Challenge](http://www.amazon.com/Advantage-American-Innovation-Overcome-Challenge/dp/0393068781),” and he tweets at [@adschina](https://twitter.com/adschina).¶ *In “*[*Chinese Computer Games*](http://www.foreignaffairs.com/issues/2012/91/2)*,” in the March/April edition of Foreign Affairs, you argued against hoping for a grand bargain: “Washington should focus on improving its defenses.” President Obama supports the Cybersecurity Act of 2012. Should the Senate pass it?¶* We need effective legislation, but it doesn’t look like the Cybersecurity Act of 2012 is going to be it. After opposition surfaced to provisions requiring power grid, gas pipeline, water supply, and other critical infrastructure providers to meet a certain level of security defined by the Department of Homeland Security, a compromise version of the bill that made industry participation voluntary was introduced. The D.H.S. will help develop best practices with industry and companies will be offered incentives to adopt them. The bill still needs votes to pass the Senate, faces stiff opposition from Senator John McCain, and it is uncertain if it will be taken up by the House before the session concludes. In the unlikely case that it does pass, the best that can be said of it will probably be that it was better than doing nothing.¶ While China could attack critical infrastructure, it is unlikely to do so unless the two sides are seriously considering or already engaged in military conflict. The most pressing threat from China now is cyber espionage, and if the bill fails, Congress will have to revisit the question of how the government and private sector can improve information-sharing on threats and vulnerabilities. It is interesting that as the government struggles to come up with a policy solution, an increasing number of private firms appear to be willing to consider more active defense measures. Hacking back into computers in China would be illegal, but companies are mapping out the attackers’ networks and they can also plant disinformation and waste hackers’ time by building fake systems.¶ *The proliferation of Weibo and cheap smartphones seems to pose a fundamental challenge; the scale of data may grow even faster than China’s ample human resources can manage. How will China’s Internet censorship evolve to keep up, or is it outmatched?¶* I suspect the technology pendulum will continue to swing back and forth, sometimes favoring the C.C.P., other times netizens. With Chinese netizens now totaling five hundred and thirty-eight million, with three hundred and thirty-eight million accessing the Web through smartphones, data will proliferate at a massive rate and will be increasingly mobile. Chinese web users will think of new ways to outsmart censors, at least for a few hours. This is clearly putting increasing pressure on the government to be more responsive and transparent, but the state can also rely on new surveillance technologies and exploit big data to pinpoint and repress protests and dissidents.¶ The important change will not be simply technological but also in user behavior and expectations. Most Chinese netizens, like their counterparts every else in the world, do not use the Web for political purposes. As Rebecca MacKinnon and others have pointed out, the relatively open nature of the Web in China allows people to vent their frustration and debate, under constricted circumstances, sensitive topics, perhaps making them less likely to question the government directly. Moreover, many in China seem to accept the government’s explanation that it regulates the Internet to control dangerous or harmful material like pornography. Only when these assumptions change, and when more Chinese are willing to question the legitimacy of one-party rule, will the full force of new technologies be channelled to political change.¶ *Cyber is often mentioned as one of the leading potential flashpoints in the U.S.-China relationship. Where would you rank that risk compared to potential conflict in the South China Sea, Taiwan, or trade disputes?¶* While strategic mistrust is high between the two sides, Cyber alone is unlikely to be a major flashpoint. Attacks designed to steal intellectual property and other trade secrets occur with such regularity and at such a pace and scope that General Alexander, head of U.S. Cyber Command, has called them “the greatest transfer of wealth in history”—yet the United States continues to engage China on a range of issues, from Iran and Syria to trade and the environment. Washington has raised the pressure on Beijing about cyber, publicly calling out Chinese hackers and addressing it in bilateral meetings, but clearly has not made it an issue that it is willing to go to the mat for.¶ There is little doubt, however, that cyber will be part of any political, military, or economic conflict in the future, and that it has high a probability of making the situation more difficult to resolve. Web-site defacements were an annoyance in the standoff between China and the Philippines over the Scarborough Shoal/Huangyan Island, but more serious cyber attacks could have escalated the situation, making signalling much more complicated. This is why it is so important that the United States and China continue to talk about cyber and to develop points of contact and other communication mechanisms in case of crisis.¶ *In “Advantage,” you make the case for American “software” in innovation, but American executives often say we shouldn’t be confident; they cite some familiar numbers on Chinese engineers graduating each year, rising Chinese investment in R. & D., new infrastructure, and so on. Are they right?¶* I agree that we should not be overconfident. Our software—the social, political, and cultural institutions and understandings that move ideas from the lab to the marketplace—cannot operate on autopilot. There is much to be done—reforming immigration and visa laws, preserving and enlarging investment in basic R. & D., reinvigorating university-industry collaboration, and re-energizing science and math education.¶ But much of the news over the last few years reinforces my argument that China’s software is a real impediment to building a truly innovative economy. American C.E.O.s love to quote China’s rising investment in R. & D., but they never follow with Chinese reporting that suggests sixty per cent of state R&D funds are lost to corruption. High-profile plagiarism and academic malfeasance cases continue to surface, and the education system struggles with fostering creativity and individual initiative. A recent study conducted by the World Bank and the State Council concluded that research quality falls short, scientists publish relatively few high-impact articles, and that the majority of Chinese patents constitute minor tweaks rather than real inventions. Market incentives are still orienting Chinese entrepreneurs to adapting technologies developed in the West for the local market, not thinking long-term and investing in high-risk, high-return breakthroughs. Most important, the government still fears the intellectual competition and freedom to debate the new ideas necessary for innovation.

## Legislation Doesn’t Solve

### **Compromise Watered Down**

#### Can’t solve – legislation will be watered down and will become ineffective

#### UPI, 7/25 **– leading provider of critical information to media outlets, businesses, governments, and researchers worldwide (United Press International, “Cybersecurity law at risk of watering down”, 7/25/12,** <http://www.upi.com/Business_News/Security-Industry/2012/07/25/Cybersecurity-law-at-risk-of-watering-down/UPI-26541343213669/>**) // EK**

Ambitious new U.S. legislation to fight cybercrime and cyberterrorism is at risk from revisions that may water it down so much that it is no longer effective, critics say.¶ The revised cybersecurity bill introduced in the U.S. Senate has drawn criticism for being too soft on the corporate sector, which is likely to be let off easily on what are basically compliance issues, analysts said.¶ In previous versions of the Cybersecurity Act, businesses and the corporate sector at large were put under various obligations to ensure security of their systems against cybercrime and cyberterrorism.¶ But Republican objections made those provisions unsustainable and further changes eliminated those clauses.¶ Security analysis and numerous expert assessments over the past two years have maintained that businesses that run the power grid, gas pipelines, water supply systems and other critical infrastructure elements are most at risk from hostile action aiming either to disable their computer systems or manipulate those systems with adverse outcome.¶ In earlier versions of the bill the corporate firms were required to meet certain levels of security and, failing that, were warned of penalties.¶ The lawmakers insist the bill can still be effective but critics within Congress and outside it say they aren't so sure.¶ In March, National Security Agency chief Gen. Keith Alexander warned Congress the law needed to have more clout because operators of critical infrastructures didn't follow even basic security procedures like updating software.

### Regulations Won’t Work

Cybersecurity act won’t protect from attacks
HeritageAction 7/24 (“Key Vote Alert: ‘NO’ on the Cybersecurity Act of 2012” 7/24/12, heritageaction.com, <http://heritageaction.com/2012/07/key-vote-alert-no-cybersecurity-act-2012/>) // EW

As The Heritage Foundation notes, “The specter of a crippling attack on critical industries, such as the electrical grid or the financial system, looms in the minds of many.” However, Congress should not rush to pass legislation without fully considering the consequences of the bill to ensure that the legislation does not do more harm than good. The Cybersecurity Act of 2012, commonly referred to as Lieberman-Collins, falls into the “more harm than good” category. The federal government does not have a good track record of properly regulating industries without causing harm. They are ill-equipped to develop effective cybersecurity regulations, and would instead create a cumbersome regulatory process that would pose an undue burden to the industry. Even though this bill makes adherence to the regulations “voluntary,” the regulatory footprint imposed by this bill would still be too cumbersome and include too many unknowns to adequately protect the industry from an attack without damaging the internet industry itself.  Although it is marginally better than a fully mandatory paradigm of regulations, it would leave open the strong possibility of individual agencies making their regulations binding.

## Turns

### Innovation Turn

#### Revised cybersecurity legislation does the opposite of its intended purpose – hurts innovation, angers businesses, kills information-sharing

Rosenzweig, 7/23 – visiting fellow at the Heritage Foundation (Paul, “Cybersecurity Act of 2012: Revised Cyber Bill Still Has Problems”, The Heritage Foundation, 7/23/12, <http://www.heritage.org/research/reports/2012/07/cybersecurity-act-of-2012-revised-cyber-bill-still-has-problems>) // EK

Senators Joseph Lieberman (I–CT) and Susan Collins (R–ME) recently released a revised version of their Cybersecurity Act of 2012. The expectation is that Senate leadership will attempt to bring the bill to the floor before the August recess. Though an able effort, the revised bill still has grave problems that are likely to chill innovation without improving cybersecurity.¶ The Regulatory Morass¶ The original bill would have assigned the Department of Homeland Security (DHS) the role of creating mandatory cybersecurity standards for critical infrastructure industries.[1] To its authors’ credit, the bill moves away from that mandatory system, but it still has far too great an intrusive federal role in defining cybersecurity standards.¶ The revised bill still requires the creation of industry best practice standards for protecting critical infrastructure. Instead of making those standards mandatory, it pushes the owners of critical infrastructure to adopt new “voluntary” standards. Those incentives include liability protection, priority assistance for cyber threats, and access to classified information about threats.¶ There are several problems with this new approach. First, the government should not be in the position of denying its threat information to critical infrastructure owners who choose not to adopt the voluntary standards, likely for justifiable business reasons. If the infrastructure in question is truly “critical,” it is in America’s collective interest to protect it as much as possible.¶ Second, the liability protections provided as an incentive are far too weak. If a company adopts the voluntary standards, it could still be sued for consequential damages. All it gains is protection against punitive damages, which it would almost certainly obtain anyway for any reasonable effort at providing cybersecurity. Additionally, these government standards would likely form the basis for lawsuits against those who do not adopt them, giving business to trial lawyers at the expense of real security.¶ Third, voluntary standards would stifle innovation and likely be obsolete by the time they are written. Over the multi-year process when standards are being written and adopted, innovation and investment in cybersecurity products will cease. No thoughtful investor will invest in a product that might not be one of the standard-approved methods of providing cybersecurity, even if it might be a better one. Given the government’s own track record of combating cyber threats and the glacial pace at which it develops rules and regulations, there is good reason to be deeply skeptical that the government can set the right standards in a dynamic environment such as cybersecurity.[2]¶ Finally, a voluntary standard system is a short step from a mandatory one. Senator Lieberman has already said that if industries do not adopt the voluntary standards, Congress will make them do so. Indeed, it appears that the “voluntary standards” may not even be voluntary after all. Under section 103(g) of the bill, federal regulatory agencies are free to make the voluntary regulations mandatory in the sectors they regulate, and they are required to report to Congress if they choose not to do so—which is a strong incentive to adopt the “voluntary” rules.¶ Information Sharing Weakened¶ The other critical portion of the bill is the set of information-sharing provisions. This bill continues the earlier focus of the prior version on the creation of cybersecurity exchanges in the federal government for sharing threat and vulnerability information. As drafted, the bill is likely to fail to achieve these modest objectives.¶ The bill requires the creation of a federal civilian cybersecurity information exchange, presumably led by DHS. The idea of strengthening DHS’s role in this program is laudable, but the bill deliberately excludes the possibility that the Department of Defense and/or the National Security Agency might also operate an exchange. While there is a legitimate reason for concern over the militarization of cyberspace defense, it seems highly inefficient and ineffective to require all defense efforts go through DHS to get information in all cases. Surely there must be a subset of cases where direct military engagement is both appropriate and even necessary.¶ Additionally, the bill would limit the sharing of cyber threat information with other federal agencies, recreating the stovepipes that contributed to the 9/11 attacks. This is a step backward. The cyber exchanges may disclose information to law enforcement only to prevent a cyber threat, to combat an imminent threat of death or serious bodily injury, or to protect minors—e.g., from child pornography. While these are clearly important goals, the bill prohibits sharing with law enforcement for other equally or more important reasons, such as to protect the nation from a biological threat or to combat serious crime, such as that of Mexican drug cartels.¶ The bill also authorizes lawsuits against the U.S. government for violations of the limitations and authorizes the award of attorney’s fees. This inclusion is clearly an attempt to create an incentive for lawsuits, which would chill information sharing.¶ A final and serious weakness is that the bill provides insufficient liability protection for the private-sector actors who share information. The bill protects only those who act in good faith and without gross negligence. Any clever lawyer can find a way to sue, and the private-sector actors are at risk of years of long litigation with all of the attendant costs. This provision alone is likely to ensure that nobody shares cyber threat information at all for fear of being sued.¶ The Way Forward¶ Congress should reject any effort to create a new regulatory system for cybersecurity. Furthermore, it should strengthen protections for private-sector actors in order to authorize and incentivize the sharing of cyber threat and vulnerability information. As drafted, the new offering from Senators Lieberman and Collins does neither of these things.

### Defense Bill Turn

#### **Cybersecurity prevents the defense bill from being passed before August – the link means the plan’s key to reverse this**

Herb, 7/26 – defense reporter for The Hill (Jeremy, “Senate’s move to cybersecurity means no defense bill before recess”, The Hill, 7/26/12, <http://thehill.com/blogs/defcon-hill/budget-appropriations/240603-senates-move-to-cybersecurity-means-no-defense-bill-before-recess>) // EK

The Senate’s vote to proceed with the cybersecurity legislation means the Defense authorization bill will not be taken up before the August recess, pushing back the hopeful predictions made about getting the bill on floor by the Senate Armed Services Committee leaders.¶ Senate Armed Services Chairman Carl Levin (D-Mich.) told The Hill that the Senate’s plan to take up cyber next week kills any chance of getting to the defense bill before the August recess, although he contended that there was still some hope for the defense bill until the vote Thursday.¶ The House and Senate take off for the month-long recess at the end of next week.¶ “Unless some unexpected disaster occurred to cyber, it can’t come up,” Levin said. “Until this vote today, there was still a good chance.”¶ The Defense authorization bill passed the Armed Services panel in May, at which time Levin and ranking member John McCain (R-Ariz.) perhaps overly optimistically predicted it would get on the floor by June or July.¶ Levin said earlier this month he remained hopeful about the bill’s chances of coming up before the August recess, while McCain took to the floor multiple times to assail Senate Majority Leader Harry Reid (R-Nev.) for pushing political bills to the floor instead of the defense bill.¶ McCain [also complained](http://thehill.com/blogs/floor-action/senate/239527-mccain-questions-reids-decision-to-take-up-cyber-security-bill-instead-of-defense-authorization) this week when Reid indicated he would move forward with the cybersecurity legislation.¶ Reid’s reluctance to bring the authorization bill to the floor isn’t about partisanship, as the measure has passed for 50 years straight. But it would eat up several days of floor time with a number of potentially prickly amendments, and could spark a fight over the Budget Control Act Reid is not interested in having.¶ Those same issues could stall the bill further in September when Congress returns, although Levin said he will push for the bill to get floor time then.¶ “He knows how strongly I feel about it,” Levin said of Reid.¶ The House passed its Defense authorization bill in May.

#### **The defense bill’s key to military power and the navy**

McKeon, 12 – Chairman of Armed Services Committee (Buck, “The National Defense Authorization Act for Fiscal Year 2013: Highlights of H.R. 4310, HASC Communications Office, 5/14/12, <http://armedservices.house.gov/index.cfm/files/serve?File_id=2a2e1b35-2fdc-404b-ab42-f929c34ca273>, page 3) // EK

*Note: NDAA = National Defense Authorization Act, the real name of the defense bill*

The bill restores and retains vital systems, platforms, and authorities needed to maintain America’s combat power after a decade of war while declining to take up Administration requests, such as two rounds of base closure, which could damage vital military infrastructure. In addition, the NDAA:¶ Preserves Air National Guard Aircraft & Manpower: In contrast to the President’s budget proposal, the FY13 NDAA preserves tactical airlift crucial to DOD’s ability to support warfighters on the ground with agile combat support, such as C-130 Hercules, C-23 Sherpas, and C-27J Spartan aircraft proposed for early retirement. Maintains close air support and ground interdiction capabilities provided by A-10 Warthogs and F-16 Fighting Falcons slated for premature divestment prior to the forecasted service-life end of each aircraft. The Committee believes these assets remain vital to governors who have important roles as first responders in times of crisis.¶ Navy Cruisers: Restores three of the four Navy cruisers proposed for early retirement in Fiscal Year 2013, each of the cruisers has more than a decade of useful service left, and can help make up the lack of combat power behind the President’s “pivot” to Asia.

#### **The defense bill’s key to space control and security, cyber operations, and is key to solve Iran nukes**

McKeon, 12 – Chairman of Armed Services Committee (Buck, “The National Defense Authorization Act for Fiscal Year 2013: Highlights of H.R. 4310, HASC Communications Office, 5/14/12, <http://armedservices.house.gov/index.cfm/files/serve?File_id=2a2e1b35-2fdc-404b-ab42-f929c34ca273>, page 2-3) // EK

*Note: NDAA = National Defense Authorization Act, the real name of the defense bill*

The FY13 NDAA requires the President to notify Congress of any planned force reductions in Afghanistan prior to any public announcement of such a decision. Notification would include assessment of conditions on the ground that enable such a force reduction, including the relevant security risks associated with the reduction in force levels, and an assessment of the operational capability of the Afghan National Security Forces (ANSF).¶ The FY13 NDAA also includes a Sense of Congress that we should: maintain security gains as the U.S. transitions security to the Afghans; transition to advise and assist at the earliest as conditions on the ground allow; and not maintain an indefinite combat mission. The President should: consider our Commander on the ground’s assessment for a combat presence through 2013; maintain a force of at least 68,000 through 2014 unless fewer forces achieves objectives (68,000 is the post surge withdrawal level expected this September 2012); and maintain troop presence and funding sufficient to advise and assist the ANSF after 2014.¶ Force Protection. Prohibits use of private security contractors for force protection of US troops in Afghanistan.¶ Special Operations. Enables Special Operations Forces to sustain the current fight and rebalance across the globe where appropriate to counter and mitigate threats, and work with partner nations. Preserves and institutionalizes other capabilities such as irregular warfare and security force assistance within the services and U.S. Special Operations Command.¶ North Korea, China, Iran. Requires Combatant Commanders to give their assessment of capability gaps against North Korea, China, and Iran.¶ Iran. Reinforces the United States’ commitment to use all elements of national power to prevent Iran from acquiring a nuclear weapon and enhances the credibility of the military option, should it prove necessary.¶ Support for Israel. Supports key allies, including Israeli Cooperative Missile Defense programs like Iron Dome.¶ Pakistan. Freezes security assistance funding to Pakistan until Pakistan reopens vital supply routes to U.S. troops in Afghanistan.¶ Nuclear Modernization, Oversight and NNSA Reform. Modernizes and supports DOD’s nuclear forces, including intercontinental ballistic missiles and nuclear bombers and the Navy’s strategic submarines and submarine-launched ballistic missiles. Strengthens congressional oversight of the nation’s nuclear weapons war plan. Reforms the National Nuclear Security Administration’s governance and management systems to make the agency more independent and efficient.¶ Homeland Missile Defense. Supports a robust national missile defense, including $100 million for an East Coast third site for national missile defense to align with the rising threat from Iran.¶ Space. Provides additional funding for national security space programs, approximately $50 million above the Administration’s request.¶ Cyber. Increases oversight on development of cyber operations capabilities.¶ Science and Technology. Supports several key areas of science and technology investments to ensure the Department meets future defense needs.¶ Audit Readiness. Implements recommendations from the HASC Financial Management and Auditability Reform Panel that will improve execution and management of Department of Defense Enterprise Resource Planning systems.

### Status Quo Solves

#### Status Quo Solves Cyber security- DHS, SCC, and GCC prove

Chertoff, 2006 – Secretary of the Department of Homeland Security (Michael, “National Infrastructure Protection Plan”, Department of Homeland Security, 3/17/6, http://www.scd.hawaii.gov/documents/ NationalInfrastructure ProtectionPlan.pdf) //AK

**The goal of these organizational structures, partnerships, and information-sharing networks is to establish the context, framework, and support for activities required to implement and sustain the national CI/KR protection effort**. **DHS will issue coordinated guidance on the framework for CI/KR public-private partnerships, as well as metrics to measure their effectiveness.** The NIPP relies on the sector partnership model, illustrated in figure 4-1, as the primary organizational structure for coordinating CI/KR efforts and activities. The sector partnership model encourages formation of SCCs and GCCs as described below**. DHS also provides guidance, tools, and support to enable these groups to work together to carry out their respective roles and responsibilities. SCCs and corresponding GCCs work in tandem to create a coordinated national framework for CI/KR protection within and across sectors.**

#### Status Quo Solves- we already have a sophisticated system of Cyber Security

Chertoff, 2006 – Secretary of the Department of Homeland Security (Michael, “National Infrastructure Protection Plan”, Department of Homeland Security, 3/17/6, http://www.scd.hawaii.gov/documents/ NationalInfrastructure ProtectionPlan.pdf) //AK

**The National Strategy to Secure Cyberspace sets forth objectives and specific actions needed to prevent cyber attacks against America’s CI/KR; identifies and appropriately responds to those responsible for cyber attacks; reduces nationally identified vulnerabilities; and minimizes damage and recovery time from cyber attacks.** **This strategy articulates five national priorities**, including the establishment of a security response system, a threat and vulnerability reduction **National Infrastructure Protection Plan program, awareness and training programs, efforts to secure government cyberspace, and international cooperation.** Priority in this strategy is focused on **improving the national response to cyber incidents; reducing threats from and vulnerabilities to cyber attacks; preventing cyber attacks that could affect national security assets; and improving the inter- national management of and response to such attacks.**