# 1AC

**Plan**

**Plan: The United States Congress should require consultation between the President of the United States and Congress prior to the use of Offensive Cyber Espionage in Operational Preparation of the Environment.**

**Our Advantage is the Cyber Industrial Complex**

**The espionage scandal is creating an exodus of talent from the cyber industrial complex which endangers cyber security.**

**Economist 13**

Hiring digital 007s; Consultancies and spy chiefs¶ The Economist, June 15, 2013http://ic.galegroup.com.ezp-prod1.hul.harvard.edu/ic/bic1/MagazinesDetailsPage/MagazinesDetailsWindow?failOverType=&query=&windowstate=normal&contentModules=&mode=view&displayGroupName=Magazines&limiter=&currPage=&disableHighlighting=&displayGroups=&sortBy=&source=&search\_within\_results=&action=e&catId=&activityType=&scanId=&documentId=GALE%7CA333726100¶ A new cyber-industrial complex is rising. Should you worry?

¶ "AT BOOZ ALLEN, **we're shaping the future of cyber-security**," trumpets a recruiting message on the website of Booz Allen Hamilton, a consulting and technology firm. It is hard to argue with that blurb right now. Edward **Snowden**, the man who revealed he was **responsible for leaks about surveillance** of American citizens by the National Security Agency (NSA), was a contractor working for Booz Allen. That has turned a spotlight on the extensive involvement of private firms in helping America's spooks to do their jobs. The affair could lead to changes in the way these relationships work.¶ ¶ As a result of the leaks, **politicians are likely to debate the pros and cons of outsourcing sensitive work monitoring online communications and security threats** to firms such as Booz Allen, which has close links to the intelligence establishment. Many of its more than **25,000 employees have some form of government security clearance** and Mike McConnell, who heads its fast-growing cyber-security business, is a former Director of National Intelligence. The current director, James Clapper, is a former Booz Allen executive.¶ ¶ But while Booz Allen has hogged the headlines, much to the chagrin of its leaders, a broader trend has gone largely unremarked. A number of **high-ranking cyber-security experts** from places such as the FBI, the Department of Homeland Security (DHS) and the White House **have left government in recent years and are now working in various capacities** for specialist consulting firms or start-ups offering security technology and services. The table below lists some examples.¶ ¶ Anecdotal evidence suggests **this exodus of talent is increasing**. Peter Metzger, a headhunter at CTPartners in Washington, DC, whose work includes hiring cybersecurity officials for companies, says the number of such assignments has doubled in the past 12 months. **A recent wave ofsenior departures from the DHS has attracted politicians' attention. At a meeting in May of a House of Representatives subcommittee** that **focuses on** cyber-security issues, Yvette Clarke, one of its members, expressed concern about **"the continuing drain of senior cyber-security leadership**" at the department, noting that it "**has gotten particularly bad in the last six months."**¶¶ One of those who has left is Mark Weatherford, who quit last month as deputy under-secretary for cyber-security at the DHS to join the Chertoff Group, a consultancy. He has also joined the advisory boards of Coalfire, a firm that helps companies identify technology-related risks and deal with compliance issues, and Cylance, a cyber-security outfit.¶ ¶ Like Mr Weatherford, Sameer Bhalotra has found himself in demand. On leaving his job as senior cyber-security official at the White House last year, he was hired as chief operating officer of Impermium, a cyber-security start-up. On June 10th Mr Bhalotra also joined the advisory board of Damballa, which offers software to speed up companies' responses to attacks on their networks. He says he expects to take on more advisory positions soon.¶ ¶ **The role** of firms such as Booz **Allen in the intelligence arena and the flow of government cyber-tsars** into tech companies **are evidence of an emerging cyber-industrial complex** in which the private and public sectors are intimately linked. Some will see this as a worrying development, noting that President Dwight Eisenhower used the term "military-industrial complex" in a speech in 1961 to give warning about the dangers of too cosy a relationship between government, military men and defence contractors.¶ ¶ There are **risks inherent in the** cyber-industrial complex too. Mr Snowden's leak **will raise questions about just how watertight firms** such as Booz Allen **can keep their operations**. (The company declined to comment for this article.) There is also a theoretical risk that **former officials might tap their chums in government to give their new employers an unfair advantage in bidding for federal contracts or to influence policy for commercial advantage.**¶¶ But there are also reasons why **the cyber-industrial complex** should, on balance, be welcomed. For a start, many talented but quirky techies would refuse to work for government agencies, which are unlikely to be hoodie-friendly. Better to have them work as contractors than not to enlist their talents at all. Deep-pocketed firms may also be best placed to attract rare birds such as data scientists. Lattice Engines, a software company looking into hiring trends in the data field, reckons Booz Allen has over 300 vacancies for such people and may well be recruiting more of them than Google or Facebook.¶ ¶ Because of the danger that online security threats pose, companies need to co-operate closely with government spooks and crimebusters to counter them. Former cyber-officials can advise firms how best to do this. Moreover, if the government wants to continue to benefit from the savvy of its departing cyber-warriors, it can always hire their new firms.¶ ¶ Government types can also help cyber-security firms and consultancies, which are prime targets for hackers, to protect their own operations better. Dmitri Alperovitch, a founder of CrowdStrike, a cyber-security company that hired Shawn Henry after he retired from a senior position at the FBI, says that in addition to working with clients Mr Henry is also responsible for CrowdStrike's own internal security.¶ ¶ That still **leaves the issue of persuading enough talented cyber-warriors to remain in government.** Ironically, Mr Metzger, the headhunter, thinks the NSA furore will mean even more work for him. Some boards have been slow to wake up to the gravity of cyber-risks, he says. But now that executives realise their own calls and e-mails are being monitored, they are more likely to take the threats seriously.

**Leaks will continue.**

**Wolfgang 13**

Ben Wolfgang, June 30, "Julian Assange, Edward Snowden promise more secrets will be revealed", www.washingtontimes.com/news/2013/jun/30/julian-assange-there-no-stopping-edward-snowden-mo/?page=all

WikiLeaks founder Julian Assange said Sunday that Edward Snowden — the former National Security Agency and CIA contractor still holed up in a Moscow airport after leaking classified national security information to media outlets — has more secrets to reveal, and that there is nothing the U.S. government can do to stop him.¶ “Look, **there is** no stopping **the publishing process at this stage**. Great care has been taken to make sure that **Mr. Snowden can’t be pressured by any state to stop the publication process,”** Mr. Assange said during an interview on ABC’s “This Week.” The latest revelations attributed to Mr. Snowden were reported by the German outlet Der Spiegel, which claims **leaked documents show the U.S. spied on European Union officials in Washington**, New York and Brussels.¶ **Reaction was swift from European allies,** who said the allegationscould scuttle ongoing negotiations on a proposed major trans-Atlantic trade treaty. “**Partners do not spy on each other**,” said EU Justice Commissioner Viviane Reding. **European Parliament President Martin Schulz said he was “deeply worried and shocked about the allegations of U.S. authorities spying on EU offices**.”¶ Mr. Snowden, facing espionage and other charges in the U.S., continues to seek asylum from other nations such as Ecuador. Mr. **Assange** acknowledged Sunday that WikiLeaks, which gained notoriety after revealing highly classified documents, private State Department cables and other information, **is in touch with Mr. Snowden and working to ensure the secret material in his possession eventually comes to light.**¶

#### The military hides cyber operations as “operational preparation of the environment” to keep them covert. This is the root cause of the Snowden Scandal.

Dycus 10

[Stephen Dycus, internationally recognized authority on national security law and environmental law,“Congress’s Role in Cyber Warfare,” 2010, <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>

Another potential obstacle to congressional involvement is the ¶ reportedly common but statutorily unauthorized practice of informal ¶ reporting to an even smaller “Gang of Four” – the leaders of the ¶ intelligence committees – generally for sensitive non-covert intelligence ¶ activities.3¶ The Defense Department is heavily engaged in preparations for cyber ¶ warfare, having recently announced the establishment of a new U.S. Cyber ¶ Command.39 But congressional oversight of the work of this command ¶ could be hampered by the military’s reported practice of labeling its ¶ clandestine activities – those that are intended to be secret, but that can be ¶ publicly acknowledged if discovered or inadvertently revealed – as ¶ “operational preparation of the environment,” rather than intelligence ¶ activities, even though they may pose the same diplomatic and national ¶ security risks.40 As thus characterized, these activities might not be reported ¶ to the intelligence committees.41 Any oversight that occurred would be ¶ conducted instead by the House and Senate Armed Services Committees.42¶ Such a division of responsibilities might create dangerous confusion.

**Consultation solves—Prevents covert espionage but enables flexibility.**

**Dycus 10**

[Stephen Dycus, internationally recognized authority on national security law and environmental law,“Congress’s Role in Cyber Warfare,” 2010, http://jnslp.com/wp-content/uploads/2010/08/11\_Dycus.pdf]

Set out below are some steps that Congress might take **to create an appropriate partnership**. Some of these steps involve changes in congressional committees and responsibilities. Others would **require coordination of cybersecurity functions within the executive branch**. Still **others would direct the President to keep Congress fully informed about anticipated and actual uses of cyber weapons.** Several would restrict potential executive branch actions that seem – as a matter of policy – particularly unwise. **1. Designate a single committee in each House with primary responsibility for cyber warfar**e in order to develop a coherent and consistent legislative approach.60 **2. Charge the designated committees with the development of broad policy and oversight of its implementation for both offensive and defensive uses of cyber weapons**, given the close, perhaps indistinguishable, connection between the two uses. **3. Make the designated committees responsible for oversight of the relevant activities of the White House and every government agency concerned** with cyber warfare, including the Defense Department, and their contractors, **whether overt, clandestine, or covert. 4. Designate a lead federal agency to coordinate ongoing planning among agencies.**61 The congressional committees would then have a principal point of contact for the collaborative development of policy. **5. Designate a lead agency to execute the cybersecurity plan**.62 **6. Order the preparation of a National Cybersecurity Strategy at prescribed intervals**.63 This document should be **declassified to the greatest extent possible**, in order to inform every member of Congress and the public about the basic elements of U.S. cyber policy. **7. Require frequent, periodic briefings** of the congressional committees, to enable serious consultation and advice in both directions as cyber policy evolves over time. These briefings should include information about rules of engagement, procedures for deciding to use cyber weapons, and any delegations of authority for such use. 8**. Require consultation with the designated congressional committees in every possible instance** **before any significant use of cyber weapons.**64 **9. Require a written finding by the President, in advance of any significant use** of cyber weapons whenever reasonably possible, or within a day or two afterward, that such use is or was necessary to the national security of the United States, that such use is or was as limited in scope as possible and consistent with the laws of armed conflict, and that Congress was consulted or could not be consulted because of the urgency of the threat. **10. Require immediate reports to the designated committees** of any significant use of cyber weapons, either offensive or defensive**. 11. Expressly forbid any withholding of information** from the committees based on classification or for other reasons of secrecy. **12. Direct that all required reports be delivered to the designated committees as a whole,** not merely to selected members.65 **13. Expressly forbid automated offensive responses to actual or threatened cyber attacks** on the United States under any circumstances. Given the potential for misperception or misinterpretation of an enemy attack, the difficulty of identifying the attacker and of assessing any resulting damage, and the risk of inadvertent escalation, **any such response should be directed by a sentient human hand, informed by as much consultation with various government officials as the circumstances will permit**.66 **14. Create a government structure to coordinate assistance to private entities that come under cyber attack**, so that such entities do not take matters into their own hands.67 **15. Review and appropriately amend existing legislation designed to protect privacy** within the United States.68 Needed amendments might require technical fixes, such as review of email traffic in anonymized form, or appointment of privacy officers in agencies responsible for implementation of cyber policy.69 **16. Require the public disclosure of U.S. cyber warfare policy to the greatest extent possible,** in order to inform those in government who are not directly involved in its development, to promote public debate, and to let potential enemies know that the United States has a viable policy in place.70 **17. Prohibit the outsourcing of responsibility for operating cyber weapons systems either defensively or offensively**. Because of the grave potential consequences and the attendant need for close control and accountability, such operations should be undertaken only by government officials. These recommendations are, of course, riddled with terms that require careful definition. They also omit many critical details. Specific provisions relating to timing of notices and the requirement of consultation, for example, must be worked out between the political branches.

**Its reverse causal—Congressional oversight creates the transparency key to recruiting. Hackers are calling for less presidential authority.**

**Sarojkar 13**

US Government Wants to Win Hackers for Data Collection at Black Hat

SAROJ KAR | AUGUST 5TH 13 Saroj is a Staff Writer at SiliconANGLE covering social and mobile news. http://siliconangle.com/blog/2013/08/05/us-government-wants-to-win-hackers-for-data-collection-at-black-hat/

**The head of the U.S. National Security Agency sees the work of his authority as a worldwide benchmark**. Courts, **Congress and government look at what we do**, the intelligence chief and leader of the U.S. Cyber troops said at the Black Hat conference, a major IT security conference in Las Vegas. **This is a standard for other countries.**¶ As director of the National Security Agency, General Keith Alexander has overseen the development of programs (also known as XKeyscore) that routinely collect records of U.S. phone calls and provide access to data held by Internet companies like Google, Facebook and Microsoft.¶ **Alexander defended** the retention of telephone data in the U.S. and **espionage** abroad **as legitimate** and necessary in the fight against terrorism. Thirteen terrorist attacks in the U.S., 25 in Europe, five in Africa and eleven in Asia were prevented by the programs initiated by the US government.¶ XKeyscore provides the technological capability, if not the legal authority, to target even US persons for extensive electronic surveillance without a warrant provided that some identifying information, such as their email or IP address, is known to the analyst, The Guardian reported.¶ In its most prominent public event since PRISM–the NSA’s controversial document filtering programs, which revealed the existence of large-scale monitoring–Alexander gave new details about how to control access to the data collected within the NSA. These measures, combined **with congressional oversight** and the courts, **represent a strong protection against abuse.**¶ **“[The programs’] reputations are tarnished because all the facts aren’t on the table.** I believe **it’s important for** you to understand what [agents] have to do in order to do their jobs to defend this nation and the oversight regime that we have with the courts, with **Congress**, and with the [Obama] administration. I think you need **to understand** that in order to get the full understanding of **what we do** and what we do not do,” he said.¶ **Public opinion and policy on the activities of the NSA is generally unfavorable after** some **leaks** demonstrate that existing laws are being used to enable the collection of data to a previously unimaginable scale.¶ Seeks Hacker Support for Data Collection¶ **Alexander wanted to change the public perception of the US government a bit**. He explained that, before a given phone number can be added to a list that is used to search the database, only 22 people within the agency are authorized to do so. Once given the go ahead, just 35 NSA analysts are allowed to do research, he added, noting that in 2012 the agency gave the nod to investigate the 300 call records of phone numbers, and only 12 reports were made to FBI, containing less than 500 numbers.¶ He further stated that **the NSA actively seeks hackers to help in the programs** as they are the largest concentration of technical talent in the world. Alexander called upon the Black Hat community to make suggestions on how they could do their jobs better and perhaps with less adverse consequences.¶ “How do we protect our civil liberties and privacy?” he asked. “This is one of the biggest issues we face today.”¶ The hacker Alex **Stamos said** in an interview in advance that **the hacking community will probably like to work** because of Prism & Co. in the future with less authority.¶ Alexander spoke less how to control access to emails and other data collected from Google, Facebook, Microsoft, and other U.S. Internet companies, but left implicit protection systems are similar. The NSA has technology to audit that records everything they do people with access to the surveillance databases, he explained, so anyone acting suspiciously would be caught.¶ **Alexander’s claims appear to be diametrically opposed to those of Edward Snowden,** who leaked material on the two monitoring programs in June this year.¶ Alexander insisted that the efforts of NSA surveillance were motivated by the need to combat terrorism, and stated that their programs on Internet phone had prevented 54 terrorist activities, 13 of them on U.S. soil.¶ Jeff **Moss, hacker and founder of the Black Hat conference, welcomed the willingness of the director of the NSA to speak publicly and provide** some **new details**, though scarce-about how programs operate.¶ “Since the details of these programs are classified, we have to get everything we can from this debate” while public attention remains focused on the NSA, said Moss. He argued that **the more we know about the NSA program, the more likely to develop better control systems**: “Can we come up something that technologically enabled to do [monitoring], but does not compromise privacy”.¶ For Alexander, at the Black Hat conference, he donned on a shirt and faded jeans to encourage hackers gathered to consider the possibility of working for the NSA. (Perhaps before he attempts to change hackers’ perception of the NSA, he should think about his perception of hackers.)

**Absent the plan, the espionage scandal costs 15,000 recruits.**

**Wyler 13**

Without Def Con, the Feds Have a Hacker Recruitment Problem

By Grace Wyler, 7/17/13 reporter/staff writer. <http://motherboard.vice.com/blog/without-def-con-the-feds-have-a-hacker-recruitment-problem>

In addition to unveiling wholesale data collection systems, it appears that Edward **Snowden's revelations may now be getting in the way of federal efforts to recruit the cybersecurity experts it needs to conduct electronic surveillance and fight the US government's cyber wars.** ¶ Last week, **organizers for the annual hacker confab Def Con politely requested that the feds** sit out this year's conference**, a move that will effectively** deprive federal **law enforcement and intelligence** agencies of prime recruiting opportunities among **the conference's** 15,000+ **talent pool of** hackers, **cyber security researchers, and corporate InfoSec experts.**¶ **"When it comes to sharing and socializing with feds, recent revelations have made many in the community uncomfortable about this relationship,"** Def Con founder Jeff Moss, a.k.a. "The Dark Tangent," wrote in a blog post announcing the decision. "Therefore, I think it would be best for everyone involved if the feds call a "time-out" and not attend Def Con this year. This will give everybody time to think about how we got here, and what comes next." ¶ Until now, Def Con has gone out of its way to welcome the feds into its hacker love-in, which unites disparate factions of the cyber security community in their common love of playing with computers. Three-letter federal agencies have been a fixture at Def Con since its inception in 1992, and the conference has become famous for its annual "Spot The Fed" contests, where hackers compete to identify government officials sticking out in the crowd. ¶ And over the past decade, "Spot The Fed" contests have become increasingly irrelevant, as federal officials with agencies like the CIA, the Defense Department, and the National Security Administration started taking the stage to pitch hackers on the benefits of working for the government.¶ **Ever since** US DOD director Jim Christy gave his first "Meet the Fed" Def Con panel in **1999, the conference has become a breeding ground for federal recruitment efforts.** Past **attendees include former CIA and NSA director Michael Hayden**, who spoke at Def Con 2010, **and US Air Force Colonel Michael Convertino,** who tried to win over new recruits in 2009.

**The government is currently recruiting for the National Mission Force which will defend against cyber-attacks.**

**Hayes 13**

Seeking Hackers: The Military Aims to Recruit More Cyber Soldiers¶ The U.S. Cyber Command looks to add 4,000 cyber soldiers to boost its cyber-warfare efforts.¶ PATRICK HAYES¶ posted February 6, 2013 http://www.fedtechmagazine.com/article/2013/02/seeking-hackers-military-aims-recruit-more-cyber-soldiers

**The U.S. Cyber Command (Cybercom) plans to boost its numbers in the coming years by adding 4,000 cyber soldiers to its current workforce of 900 military and civilian personnel. These new employees will be part of Cybercom’s expanded hands-on fight against cyber terrorism.**¶As these cyber soldiers are brought into the fold at Cybercom, **the force will become the major player in national cyber defense.**¶ With the additional hands on deck, the U.S. Cyber Command will be divided into three distinct teams: National Mission Forces, Combat Mission Forces and Cyber Protection Forces. Each team will have a very specific area of responsibility, according to a report from ReadWrite:¶ **The National Mission Force will protect computer networks for infrastructure like electrical grids, telecommunications and power plants from overseas attacks.** The Combat Mission Force will provide assistance to the military to respond or implement cyber attacks of their own; and the Cyber Protection Force will add protection levels to Department of Defense websites.¶ There are, however, some practical concerns with these cyber-warfare endeavors: Recent Department of Defense budget cuts could make it difficult to hire a host of new personnel.¶ Moreover, **demand for employees with cyber-defense skills is at an all-time high** as officials in every segment of **he** economy scramble to find candidates who can defend against hackers.¶ Despite the potential obstacles, Cybercom has no choice but to press on, because **the expansion is part of the government’s new offensive stance against cyber terrorism.**¶Defense officials realize that **the next great terrorist threat will likely come from the Internet and, as a result, have moved to bolster defenses.**¶ If we think about the increased reliance our society has on network connectivity, **it’s not difficult to imagine how any cyber attack could have catastrophic ramifications.**¶ While boots on the ground won’t be going away anytime soon, Cybercom’s vow to bring in new cyber soldiers highlights that it’s just as important to have boots — or rather, fingers and eyes — on the information superhighway as well.

**The few good recruits go to the NSA for offense—DHS recruiting is key to defense.**

**Boston Globe 13**

US looks to recruit student hackers¶ Wants them to defend against foreign attacks¶ By Nicole Perlroth | NEW YORK TIMES MARCH 25, 2013 <http://www.bostonglobe.com/business/2013/03/24/looks-recruit-student-hackers-help-defend-nation-cyberspace/1YurGnlyEKgVP77zy1MQsK/story.html>

He was grounded and got detention. Yet he is just the type of youngster **the** Department of Homeland Security **is looking to hire.**¶ The secretary of that agency, Janet Napolitano, knows she has a problem that will only worsen. **Foreign hackers have been attacking her agency’s computer systems. They have also been busy trying to siphon the nation’s wealth and steal valuable trade secrets. And they have begun probing the nation’s critical infrastructure — the power grid and water and transportation systems.**¶ So she needs her own hackers — **600,** the agency estimates. But **potential recruits with the right skills too often have been heading for business, and those who do choose government often go to the** National Security Agency**,** where they work on offensive digital attacks on foreign nations. At Homeland Security, the emphasis is on **keeping hackers out, or playing** defense.¶

**Strong defense solves cyber-attacks.**

**McGraw 10**

Gary McGraw Jun 17, 2010 Software [In]security: Cyber War - Hype or Consequences? <http://www.informit.com/articles/article.aspx?p=1597476> (Gary McGraw is the CTO of Cigital, Inc., a software security consulting firm with headquarters in the Washington, D.C. area and offices throughout the world. He is a globally recognized authority on software security. Dr. McGraw has also written over 100 peer-reviewed scientific publications.)

You won't be surprised to hear me say that the only way we can lessen both the potential impact and the very possibility of cyber war is to build more secure systems. This starts with the software we all rely on to work. What's the root of smart grid insecurity? Software. Malicious code? Software vulnerability. For what it's worth, Clarke resonates with this view, and makes the point of saying so on page 86 where he says, "Of the three things that make cyber war possible, the most important may be **the flaws in software** and hardware." Fortunately we are making important tangible progress on software security. However, I would like to see the palpable sense of urgency that can be observed among major international banks when it comes to computer security spread to the government — and in particular to the civilian side of the government. The Department of Homeland Security has a huge job to do to help defend the nation against cyber attack, and they are doing a particularly namby-pamby job of it. Just for the record, filling out common criteria forms is not at all what I'm talking about.

**The shortage forces the government to hire bad or corrupt defensive experts**

**Michaels 13**

Tech hiring binge may pose security risks for government

Jim Michaels, USA TODAY 1:18 a.m. EDT June 13, 2013

Edward Snowden is a high school dropout. How did he land a $122,000-a-year job in a sensitive government program? http://www.usatoday.com/story/news/nation/2013/06/12/hackers-cyber-nsa-intelligence/2413183/

WASHINGTON — **Among the more curious revelations to emerge from the recent National Security Agency leak saga is how a 29-year-old high school dropout landed a $122,000 job** in a sensitive government program.¶ Edward Snowden, the contractor who spilled top secret information about a sensitive government electronic data-collection program, said he did so out of idealism. His actions have triggered a debate about privacy and national security.¶ **His case also highlights just how hungry the government and private industry are for people with computer skills.**¶ "**They're competing heavily for anyone who can get** a clearance and has **computer skills**," said Jeffrey Carr, founder of Taia Global, a cybersecurity consultancy.¶ How a low-level insider could steal **from NSA**¶ **The Pentagon and the intelligence community are both ramping up cyber capabilities in the face of repeated attacks** on U.S. companies from China and elsewhere and concerns about how terrorists use technology to communicate and raise money.¶ **The Snowden case raises questions about whether the government has opened itself to security breaches** in its rush to hire computer experts.¶Carr said his failure to complete high school and military training should have raised concerns about his employment prospects. The Army said Snowden attempted to complete Special Forces training but was administratively discharged after several months of training.¶ **"I would see too many danger signals** with this guy," Carr said.¶ **The government and industry have been on a hiring binge** for workers with computer skills, cybersecurity analysts say. "We're all looking at the same résumés," said Dickie George, who retired from the NSA in 2011 after 41 years.¶ **"There's a job shortage of 340,000 in cybersecurity**," said Robert Rodriguez, a cybersecurity analyst and former Secret Service agent.¶ Workers on government contracts have to pass extensive background checks before they can be hired, shrinking the pool of potential employees even further.¶ Often the government and contractors are looking for computer experts with a rebel streak who can think like enemy hackers. They work alongside more buttoned-down government bureaucrats.¶ "There is a cultural difference," said George, who during his career has seen the NSA go from hiring mathematics geniuses who could crack codes to the latest generation of computer nerds.¶ He said they are patriotic Americans, though they may exhibit a different style in dress. "There were people who I don't know what color their hair is going to be next time I see them," he said.¶ Some cybersecurity analysts say **the new generation of computer enthusiasts has been shaped by the Internet, where national borders have little meaning. In some cases, they** don't have the same loyalties **to the United States.**¶ "You live online where the Internet has completely erased boundaries of nation states," Carr said. "You don't think of yourself as a U.S. citizen."

**Either scenario destroys cyber defense.**

**USA Today 13**

Snowden case: How low-level insider could steal from NSA

Byron Acohido and Peter Eisler, USA TODAY 7:16 a.m. EDT June 12, 2013 http://www.usatoday.com/story/news/nation/2013/06/11/snowden-nsa-hacking-privileged-accounts/2412507/

**Edward Snowden's ability to extract sensitive data from the NSA, working as a low-level contract consultant, comes as no surprise to the security community.**¶ Security experts say **Snowden,** a Booz Allen Hamilton network analyst based in Hawaii, **had the technical savvy to take full advantage of two major security challenges** all organizations face: managing privileged accounts and keeping PCs, databases and applications updated with the lastest security patches.¶ While details of how he did it aren't yet clear, **Snowden's escapades highlight a complex challenge all large organizations face in securing sprawling networks increasingly reliant on Internet cloud connections and use of mobile devices.**¶ "Digital assets are all plugged into an amazingly complex infrastructure," says Mike Lloyd, chief technology officer at network security firm Red Seal Networks. "**Even diligent defenders** struggle to keep up **with all the latest weaknesses, and the dizzying interactions between interdependent systems and layers. We cannot defend what we cannot understand."**¶ Snowden claims to have a long history of working as an IT specialist, including stints as a systems engineer, systems administrator, a senior adviser for the CIA, and a telecommunications systems information officer.¶ As Snowden told The Guardian in a videotaped interview: "**When you're in positions of privileged access,** like a systems administrator, for these sort of intelligence community agencies, **you're exposed to a lot more information on a broader scale than the average employee ...** Anybody **in the positions of access with the technical capabilities that I had could, you know, suck out secrets**."¶ "I'm no different from anybody else," he said. "I don't have special skills."¶ Snowden would have been well-aware of so-called privileged accounts, the logons that give administrative access to any device with a microprocessor, including PCs, servers, databases and copiers.¶ **By identifying and accessing privileged accounts, an unscrupulous insider can easily roam far and wide inside an organization's network. Such accounts function, in effect, as master keys to the deepest, most sensitive parts of an organization's digital assets.**¶ A recent survey by Cyber-Ark Software found that 86% **of large enterprise organizations** either do not know or underestimate the number of privileged accounts **incorporated into their networks.** Most have three or four times as many privileged accounts as actual employees.

**Attacks will become increasingly destructive in the SQUO—Advances outpace our defenses.**

**Business Insider 12**

Business Insider Jul. 10, 2012 Pentagon Says Bureaucracy Is Getting In The Way Of Cyber Defense http://www.businessinsider.com/pentagon-says-bureaucracy-is-getting-in-the-way-of-cyber-defense-2012-7#ixzz22hjyjtVU

The current head of the Pentagon's cyber attack response team told the American Enterprise Institute that war is coming, and that the United States remains unprepared for the worst. General Keith Alexander said he expects that cyberattacks will soon become legitimately destructive at the rate they're **outpacing the United States defenses**. There's one big problem holding all of this back, according to Alexander. The responsibility to defend and respond to cyber attacks lies variously with the FBI, Homeland Security, and the Department of Defense. Alexander said that unless Congress consolidates that sprawling cyber-defense infrastructure, the U.S. will not be able to fend off the **increasingly likely major successful attack**. What's the kicker from the speech is this: all that stands between the United States and the coordinated attacks on it is a sprawling, disorganized group of feds without a centralized command and each working for different goals.

#### Cyber-attacks are up 680%.

**FCW 12**

Advisory website on federal business and technology 2012: The year in cybersecurity

Dec 05, 201http://fcw.com/Articles/2012/12/05/2012-cybersecurity.aspx?Page=3

Cyberspace was more dangerous than ever in 2012. **With the emergence of highly sophisticated attacks, adversaries were pilfering information and generally wreaking havoc on the digital infrastructure. The cyber battlefield became a reality**, and federal agencies stepped up their efforts to fight an invisible enemy. FCW asked a variety of experts how 2012 will be remembered in the history of cybersecurity — and what those developments might mean for federal agencies in the years to come. 1. A change in attackers’ battle plans **Cyber experts and top government IT security officials have noted** a sharp increase in cyber assaults in the past half-decade. From 2006 to 2011, federal agencies experienced **a 680 percent spike in cyberattacks. The Department of Homeland Security alone was bombarded with 50,000 attacks in a five-month period. There are a growing variety of assault methods**, but **coordinated and high-precision attacks on infrastructure in particular increased in 2012**, said Keith Rhodes, chief technology officer in QinetiQ North America's Services and Solutions Group. He cited the **Stuxnet** worm as an example of particularly complex malware that targeted and knocked out individual pieces of equipment. That code, generally believed to be the work of the U.S. and Israeli governments, **is a preview of how attacks will likely evolve. Attackers** “basically got it down to the part number — this manufacturer, this piece of equipment, this part number,” he said. “It’s not the usual, ‘I’m going to go against a router or a switch.’ They’re **going after** programmable logic controllers, **the infrastructure pieces**.” The main purpose of such attacks is to interrupt whatever activity the targeted device is used for. Think of an assembly line, said Rhodes, who served as the Government Accountability Office’s first chief technologist. If hackers go after a programmable logic controller of a particular type, they can accelerate it or turn it off, and the system will stop or break. By contrast, previous attacks simply shut down the entire production, he said. “It’s a more sophisticated approach to a rather on/off brute-force approach, and that means...an adversary is trying to be more subtle,” Rhodes said. “**They are trying to have not just a bunch of arrows in their quiver but they want arrows of different length, size and weight.”** Those **infrastructure-based attacks are revealing the true nature of cyber weapons**, said W. Hord Tipton, executive director of (ISC)2 and former CIO at the Interior Department. “Now we see much more focused attacks with targets that are much more defined, and that makes them more stealthy,” he said. “When you’re scanning networks and looking around for vulnerabilities, you’re just banging on all the doors, and it makes it easier for our defensive teams to figure out where attacks are coming from. But now **if attackers can’t find a vulnerability, they stay hidden and keep looking behind the scenes to find a way in.”**

### Scenario 1: Military

**Cyber-attacks shut down our military—It’s all been transferred to the internet.**

**Samuelson 13**

Samuelson: Internet Armageddon? RobertSamuelson, Times Dispatch | Posted: Monday, July 1, 2013 12:00 amhttp://www.timesdispatch.com/opinion/their-opinion/columnists-blogs/robert-samuelson/samuelson-internet-armageddon/article\_34e6bb6a-e1cb-5d18-8db7-decf84abd790.html?mode=print

By cyberwarfare, I mean **the capacity of groups** — whether **nations or not — to attack, disrupt and possibly destroy the institutions and networks that underpin everyday life**. These would be **power grids, pipelines, communication and financial systems, business record-keeping and supply-chain operations, railroads and airlines, databases** of all types (from hospitals to government agencies). The list runs on. So much depends on the Internet that its vulnerability to sabotage invites doomsday visions of the breakdown of order and trust. In a report, **the** Defense Science Board, an advisory group to the **Pentagon, acknowledged “staggering losses” of information** involving weapons design and combat methods **to hackers** (not identified, but probably Chinese). **Hackers might disarm military units. “U.S. guns, missiles and bombs may not fire, or may be directed against our own troops,”** the report said. It also painted a specter of **social chaos from a full-scale cyberassault.** There would be “no electricity, money, communications, TV, radio or fuel (electrically pumped). **In a short time**, food and medicine distribution systems **would be** ineffective.” I don’t know the odds of this **technological Armageddon.** I doubt anyone does. The fears may be wildly exaggerated, as Thomas Rid of Kings College London argues in his book “Cyber War Will Not Take Place” (already published in Britain, due out this fall in the United States). In living memory, there are many threats that, with hindsight, seemed hyped: the “missile gap” in 1960; the Y2K phenomenon in 2000 (the date change would allegedly disable many computer chips); and, so far, the prophecies of widespread terrorism after 9/11. Still, the Internet creates new avenues for conflict and mayhem. Until now, the motives for hacking — aside from political activists determined to make some point — have mostly involved larceny and business espionage. Among criminals, “the Internet is seen as the easiest, fastest way to make money,” says Richard Bejtlich, chief security officer for Mandiant, a cybersecurity firm. Recently, federal prosecutors alleged that a gang of cyberthieves had stolen $45 million by hacking into databases of prepaid debit cards and then draining cash from ATMs. Stealing trade secrets likely dwarfs ordinary crime. From its clients, Mandiant identifies four industries as receiving the bulk of attacks: aerospace and defense, 31 percent; energy, oil and gas, 17 percent; pharmaceuticals, 15 percent; and finance, 11 percent. Mandiant identified one unit of China’s People’s Liberation Army that allegedly has hacked 141 companies and organizations since 2006, removing “technology blueprints, propriety manufacturing processes, test results, business plans.” What’s unclear is how “**infrastructure” systems** (electricity grids and the like) have been penetrated and, on command, might be compromised. In the mid-1980s, most of these systems **were self-contained**. They relied on dedicated phone lines and private communications networks. They were hard to infiltrate**. Since then, many systems switched to the Internet**. “It’s cheaper,” says James Andrew Lewis, an Internet expert at the Center for Strategic and International Studies. The architects of **these conversions apparently underestimated the risk of sabotage.**

**We have three internal links. First is lash out**

**The US will retaliate to damaging attacks cyber-attacks.**

Nakashima 11

Pentagon: Cyber offense part of U.S. strategy

By Ellen Nakashima, November 15, 2011 http://articles.washingtonpost.com/2011-11-15/news/35284321\_1\_cyberspace-new-report-cyberwarfare

The report is more explicit than the Pentagon’s cyberstrategy released in July, which focused on the importance of deterring attacks by building defenses that would “deny” adversaries the benefits of success. In the latest report, the Pentagon states directly that it “has the capability to conduct offensive operations in cyberspace to defend our nation, allies and interests.” When defense-based deterrence fails to stop a hostile act, the report says, the Pentagon “maintains, and is further developing, the ability to respond militarily in cyberspace and in other domains.” James E. Cartwright, the recently retired vice chairman of the Joint Chiefs of Staff, said the report “is a good start at documenting how the U.S. will both defend our interests in this vital domain and deter those who would threaten those interests.” Cartwright had publicly stated in July that a strategy dominated by defense would fail. In May, the White House released an international cyberstrategy declaring that the United States reserves the right to use all necessary means — diplomatic, military and economic — to defend the nation against hostile acts in cyberspace. But it said that the United States will “exhaust all options prior to using force whenever we can” in response to a hostile act in cyberspace.

**Use of America cyber weapons escalates to full blown cyber warfare**

**Temple 12**

James Temple—San Francisco Chronicle Published 4:00 a.m., Sunday, June 10, 2012 http://www.sfgate.com/business/article/In-waging-cyber-war-battlefield-becomes-blurred-3622760.php

**An attack on another nation's centrifuges could prompt an assault on our power grids, water-treatment facilities or air traffic-control systems, putting human lives at stake.** These aren't entirely hypothetical risks. A 2011 report from the Center for a New American Security found **that U.S. military networks are "probed** or scanned" about **250,000 times every** hour, **foreign agents have infiltrated the nation's power grid**, and in one test, a hacker was able to wrest control of the equipment that added chemicals to the public's drinking water in Southern California. An estimated **85 percent of the nation's critical infrastructure** lies in private hands, and by most accounts, large portions **aren't adequately secured.** Eric Jensen, a former military lawyer and associate law professor at Brigham Young University, said Stuxnet could constitute an "armed attack" under U.N. rules, which would grant Iran the right to take proportional actions in self-defense. "If I was a legal adviser to **Iran,** I'd say there's enough (evidence) to respond," he said. In fact, he suspects the nation **will respond**. It probably lacks the technical sophistication to retaliate on its own, but Jensen said there are surely international crime syndicates happy to sell their cyber services. Kate Jastram, a lecturer in residence at UC Berkeley Law School, doesn't think the U.S. action qualifies as an armed attack. But she does think Stuxnet and similar efforts demand a re-evaluation of questions surrounding the traditional rules of war, such as: What level of damage from a cyber attack constitutes a use of force or armed attack? What's a proportional response, and how sure should we be of the source of an attack before we can respond? One problem with the United States and it allies conducting cyber warfare out of the public eye is that the battles are preceding the policy conversations. "Analysts are still not clear about the lessons of offense, defense, deterrence, escalation, norms, arms control, or how they fit together into a national strategy," Harvard's Joseph Nye wrote in his 2011 paper "Nuclear Lessons for Cyber Security?" Cyber terror next? It's high time to sort through these issues, since **all signs point to increasing cyber conflicts.**

#### Independently, US retaliation to cyber warfare goes nuclear.

Lawson, Professor of Communication at Utah, 09

(Cross-Domain Response to Cyber Attacks and the Threat of Conflict, 5/13, http://www.seanlawson.net/?p=477)

At a time when it seems impossible to avoid the seemingly growing hysteria over the threat of cyber war,[1] network security expert Marcus Ranum delivered a refreshing talk recently, “The Problem with Cyber War,” that took a critical look at a number of the assumptions underlying contemporary cybersecurity discourse in the United States. He addressed one issue in partiuclar that I would like to riff on here, the issue of conflict escalation–i.e. the possibility that offensive use of cyber attacks could escalate to the use of physical force. As I will show, his concerns are entirely legitimate as current U.S. military cyber doctrine assumes the possibility of what I call “cross-domain responses” to cyberattacks. Backing Your Adversary (Mentally) into a Corner Based on the premise that completely blinding a potential adversary is a good indicator to that adversary that an attack is iminent, Ranum has argued that “The best thing that you could possibly do if you want to start World War III is launch a cyber attack. [...] When people talk about cyber war like it’s a practical thing, what they’re really doing is messing with the OK button for starting World War III. We need to get them to sit the f-k down and shut the f-k up.” [2] He is making a point similar to one that I have made in the past: Taking away an adversary’s ability to make rational decisions could backfire. [3] For example, Gregory Witol cautions that “attacking the decision maker’s ability to perform rational calculations may cause more problems than it hopes to resolve.. Removing the capacity for rational action may result in completely unforeseen consequences, including longer and bloodier battles than may otherwise have been.” [4] Cross-Domain Response So, from a theoretical standpoint, I think his concerns are well founded. But the current state of U.S. policy may be cause for even greater concern. It’s not just worrisome that a hypothetical blinding attack via cyberspace could send a signal of imminent attack and therefore trigger an irrational response from the adversary. What is also cause for concern is that current U.S. policy indicates that “kinetic attacks” (i.e. physical use of force) are seen as potentially legitimate responses to cyber attacks. Most worrisome is that current U.S. policy implies that a nuclear response is possible, something that policy makers have not denied in recent press reports. The reason, in part, is that the U.S. defense community has increasingly come to see cyberspace as a “domain of warfare” equivalent to air, land, sea, and space. The definition of cyberspace as its own domain of warfare helps in its own right to blur the online/offline, physical-space/cyberspace boundary. But thinking logically about the potential consequences of this framing leads to some disconcerting conclusions. If cyberspace is a domain of warfare, then it becomes possible to define “cyber attacks” (whatever those may be said to entail) as acts of war. But what happens if the U.S. is attacked in any of the other domains? It retaliates. But it usually does not respond only within the domain in which it was attacked. Rather, responses are typically “cross-domain responses”–i.e. a massive bombing on U.S. soil or vital U.S. interests abroad (e.g. think 9/11 or Pearl Harbor) might lead to air strikes against the attacker. Even more likely given a U.S. military “way of warfare” that emphasizes multidimensional, “joint” operations is a massive conventional (i.e. non-nuclear) response against the attacker in all domains (air, land, sea, space), simultaneously. The possibility of “kinetic action” in response to cyber attack, or as part of offensive U.S. cyber operations, is part of the current (2006) National Military Strategy for Cyberspace Operations [5]: (U) Kinetic Actions. DOD will conduct kinetic missions to preserve freedom of action and strategic advantage in cyberspace. Kinetic actions can be either offensive or defensive and used in conjunction with other mission areas to achieve optimal military effects. Of course, the possibility that a cyber attack on the U.S. could lead to a U.S. nuclear reply constitutes possibly the ultimate in “cross-domain response.” And while this may seem far fetched, it has not been ruled out by U.S. defense policy makers and is, in fact, implied in current U.S. defense policy documents. From the National Military Strategy of the United States (2004): “The term WMD/E relates to a broad range of adversary capabilities that pose potentially devastating impacts. WMD/E includes chemical, biological, radiological, nuclear, and enhanced high explosive weapons as well as other, more asymmetrical ‘weapons’. They may rely more on disruptive impact than destructive kinetic effects. For example, cyber attacks on US commercial information systems or attacks against transportation networks may have a greater economic or psychological effect than a relatively small release of a lethal agent.” [6] The authors of a 2009 National Academies of Science report on cyberwarfare respond to this by saying, “Coupled with the declaratory policy on nuclear weapons described earlier, this statement implies that the United States will regard certain kinds of cyberattacks against the United States as being in the same category as nuclear, biological, and chemical weapons, and thus that a nuclear response to certain kinds of cyberattacks (namely, cyberattacks with devastating impacts) may be possible. It also sets a relevant scale–a cyberattack that has an impact larger than that associated with a relatively small release of a lethal agent is regarded with the same or greater seriousness.” [7]

Second, Miscalc—Vulnerabilities **and tensions get exploited to start nuclear war.**

**Fritz 09**

Fritz ‘09, Jason, Researcher for International Commission on Nuclear Nonproliferation and Disarmament, Former Army Officer and Consultant, Master of Internation Relations at Bond University, “Hacking Nuclear Command and Control,” 2009.

(http://icnnd.org/Documents/Jason\_Fritz\_Hacking\_NC2.pdf.)

This paper will analyse the threat of cyber terrorism in regard to nuclear weapons. Specifically, this research will use open source knowledge to identify the structure of nuclear command and control centres, how those structures might be compromised through computer network operations, and how doing so would fit within established cyber terrorists’ capabilities, strategies, and tactics. **If access to command and control centres is obtained, terrorists could** fake or actually **cause one nuclear-armed state to attack another, thus provoking a nuclear response** from another nuclear power. **This may be an easier alternative for terrorist groups than building or acquiring a nuclear weapon** or dirty bomb themselves. **This would** also **act as a force equaliser, and provide terrorists with the asymmetric benefits of high speed, removal of geographical distance, and a relatively low cost.** **Continuing difficulties in developing computer tracking technologies which could trace the identity of intruders, and difficulties in establishing an internationally agreed upon legal framework to guide responses to computer network operations, point towards an inherent weakness in using computer networks to manage nuclear weaponry. This is particularly relevant to reducing the hair trigger posture of existing nuclear arsenals**. All computers which are connected to the internet are susceptible to infiltration and remote control. Computers which operate on a closed network may also be compromised by various hacker methods, such as privilege escalation, roaming notebooks, wireless access points, embedded exploits in software and hardware, **and** maintenance entry points. For example, e-mail spoofing targeted at individuals who have access to a closed network, could lead to the installation of a virus on an open network. This virus could then be carelessly transported on removable data storage between the open and closed network. Information found on **the internet may also reveal how to access these closed networks** directly. **Efforts by militaries to place increasing reliance on computer networks**, including experimental technology such as autonomous systems, and their desire to have multiple launch options, such as nuclear triad capability, **enables multiple entry points for terrorists**. For example, if a terrestrial command centre is impenetrable, perhaps isolating one nuclear armed submarine would prove an easier task. **There is evidence to suggest multiple attempts have been made by hackers to compromise the extremely low radio frequency once used by the US Navy to send nuclear launch approval to submerged submarines**. Additionally, the alleged Soviet system known as Perimetr was designed to automatically launch nuclear weapons if it was unable to establish communications with Soviet leadership. This was intended as a retaliatory response in the event that nuclear weapons had decapitated Soviet leadership; however it did not account for the possibility of cyber terrorists blocking communications through computer network operations in an attempt to engage the system. Should a warhead be launched, damage could be further enhanced through additional computer network operations. **By using proxies, multi-layered attacks could be engineered. Terrorists could remotely commandeer computers in China and use them to launch a US nuclear attack against Russia. Thus Russia would believe it was under attack from the US and the US would believe China was responsible.** Further, **emergency response communications could be disrupted, transportation could be shut down, and disinformation, such as misdirection, could be planted, thereby hindering the disaster relief effort and maximizing destruction**. Disruptions in communication and the use of disinformation could also be used to provoke uninformed responses. For example, a nuclear strike between India and Pakistan could be coordinated with Distributed Denial of Service attacks against key networks, so they would have further difficulty in identifying what happened and be forced to respond quickly. **Terrorists could also knock out communications between these states so they cannot discuss the situation. Alternatively, amidst the confusion of a traditional large-scale terrorist attack, claims of responsibility and declarations of war could be falsified in an attempt to instigate a hasty military response.** These false claims could be posted directly on Presidential, military, and government websites. E-mails could also be sent to the media and foreign governments using the IP addresses and e-mail accounts of government officials**. A sophisticated and all encompassing combination of traditional terrorism and cyber terrorism could be enough to launch nuclear weapons on its own**, without the need for compromising command and control centres directly.

**Extinction—Consensus of scientists.**

**Hogan 94** Michael Hogan, American scholar and president of the University Illinois at Urbana-Champaign,The Nuclear Freeze Campaign, 1994, p. 52

In the fall of 1983, a group of scientists led by Carl Sagan introduced a new strain of apocalyptic discourse into the freeze debate: the rhetoric of nuclear winter. Simply stated, the theory of nuclear winter held that **even a small exchange of nuclear weapons**—on the order, perhaps, of 500 of the world’s 18,000 nuclear weapons—**would throw so much dirt**, soot, and smoke **into the atmosphere that the earth would be plunged** **into darkness and subfreezing temperatures, a “winter” lasting long enough to create** “a real possibility of **the extinction of the human species”** Unlike doomsday scenarios that preceded it, **the theory** of nuclear winter **was based upon “extensive scientific studies.” and it had been “endorsed by a large number of scientists.”**

#### Third is decapitation

**Bad Cyber Defenses enable decapitation of the government from the military.**

Paul **Stockton 11**, assistant secretary of defense for Homeland Defense and Americas’ Security Affairs, “Ten Years After 9/11: Challenges for the Decade to Come”, <http://www.hsaj.org/?fullarticle=7.2.11>

The cyber threat to the DIB is only part of a much larger challenge to DoD. Potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities, by targeting the critical civilian and defense supporting assets (within the United States and abroad) on which our forces depend. This challenge is not limited to man-made threats; DoD must also execute its mission-essential functions in the face of disruptions caused by naturally occurring hazards.20 Threats and hazards to DoD mission execution include incidents such as earthquakes, naturally occurring pandemics, solar weather events, and industrial accidents, as well as kinetic or virtual attacks by state or non-state actors. Threats can also emanate from insiders with ties to foreign counterintelligence organizations, homegrown terrorists, or individuals with a malicious agenda. From a DoD perspective, this global convergence of unprecedented threats and hazards, and vulnerabilities and consequences, is a particularly problematic reality of the post-Cold War world. Successfully deploying and sustaining our military forces are increasingly a function of interdependent supply chains and privately owned infrastructure within the United States and abroad, including transportation networks, cyber systems, commercial corridors, communications pathways, and energy grids. This infrastructure largely falls outside DoD direct control. Adversary actions to destroy, disrupt, or manipulate this highly vulnerable homeland- and foreign-based infrastructure may be relatively easy to achieve and extremely tough to counter. Attacking such “soft,” diffuse infrastructure systems could significantly affect our military forces globally – potentially blinding them, neutering their command and control, degrading their mobility, and isolating them from their principal sources of logistics support. The Defense Critical Infrastructure Program (DCIP) under Mission Assurance seeks to improve execution of DoD assigned missions to make them more resilient. This is accomplished through the assessment of the supporting commercial infrastructure relied upon by key nodes during execution. By building resilience into the system and ensuring this support is well maintained, DoD aims to ensure it can "take a punch as well as deliver one."21 It also provides the department the means to prioritize investments across all DoD components and assigned missions to the most critical issues faced by the department through the use of risk decision packages (RDP).22 The commercial power supply on which DoD depends exemplifies both the novel challenges we face and the great progress we are making with other federal agencies and the private sector. Today’s commercial electric power grid has a great deal of resilience against the sort of disruptive events that have traditionally been factored into the grid’s design. Yet, the grid will increasingly confront threats beyond that traditional design basis. This complex risk environment includes: disruptive or deliberate attacks, either physical or cyber in nature; severe natural hazards such as geomagnetic storms and natural disasters with cascading regional and national impacts (as in NLE 11); long supply chain lead times for key replacement electric power equipment; transition to automated control systems and other smart grid technologies without robust security; and more frequent interruptions in fuel supplies to electricity-generating plants. These risks are magnified by globalization, urbanization, and the highly interconnected nature of people, economies, information, and infrastructure systems. The department is highly dependent on commercial power grids and energy sources. As the largest consumer of energy in the United States, DoD is dependent on commercial electricity sources outside its ownership and control for secure, uninterrupted power to support critical missions. In fact, approximately 99 percent of the electricity consumed by DoD facilities originates offsite, while approximately 85 percent of critical electricity infrastructure itself is commercially owned. This situation only underscores the importance of our partnership with DHS and its work to protect the nation’s critical infrastructure – a mission that serves not only the national defense but also the larger national purpose of sustaining our economic health and competitiveness. DoD has traditionally assumed that the commercial grid will be subject only to infrequent, weather-related, and short-term disruptions, and that available backup power is sufficient to meet critical mission needs. As noted in the February 2008 Report of the Defense Science Board Task Force on DoD Energy Strategy, “In most cases, neither the grid nor on-base backup power provides sufficient reliability to ensure continuity of critical national priority functions and oversight of strategic missions in the face of a long term (several months) outage.”23 Similarly, a 2009 GAO Report on Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DoD Critical Assets stated that DoD mission-critical assets rely primarily on commercial electric power and are vulnerable to disruptions in electric power supplies.24 Moreover, these vulnerabilities may cascade into other critical infrastructure that uses the grid – communications, water, transportation, and pipelines – that, in turn, is needed for the normal operation of the grid, as well as its quick recovery in emergency situations. To remedy this situation, the Defense Science Board (DSB) Task Force recommended that DoD take a broad-based approach, including a focused analysis of critical functions and supporting assets, a more realistic assessment of electricity outage cause and duration, and an integrated approach to risk management that includes greater efficiency, renewable resources, distributed generation, and increased reliability. DoD Mission Assurance is designed to carry forward the DSB recommendations. Yet, for a variety of reasons – technical, financial, regulatory, and legal – DoD has limited ability to manage electrical power demand and supply on its installations. As noted above, DHS is the lead agency for critical infrastructure protection by law and pursuant to Homeland Security Presidential Directive 7. The Department of Energy (DOE) is the lead agency on energy matters. And within DoD, energy and energy security roles and responsibilities are distributed and shared, with different entities managing security against physical, nuclear, and cyber threats; cost and regulatory compliance; and the response to natural disasters. And of course, production and delivery of electric power to most DoD installations are controlled by commercial entities that are regulated by state and local utility commissions. The resulting paradox: DoD is dependent on a commercial power system over which it does not – and never will – exercise control.

**Nuclear War**

**Andres and Breetz 11**

Richard Andres, Professor of National Security Strategy at the National War College and a Senior Fellow and Energy and Environmental Security and Policy Chair in the Center for Strategic Research, Institute for National Strategic Studies, at the National Defense University, and Hanna Breetz, doctoral candidate in the Department of Political Science at The Massachusetts Institute of Technology, Small Nuclear Reactorsfor Military Installations:Capabilities, Costs, andTechnological Implications, [www.ndu.edu/press/lib/pdf/StrForum/SF-262.pdf](http://www.ndu.edu/press/lib/pdf/StrForum/SF-262.pdf)

The DOD interest in small reactors derives largely from problems with base and logistics vulnerability. Over the last few years, the Services have begun to reexamine virtually every aspect of how they generate and use energy with an eye toward cutting costs, decreasing carbon emissions, and reducing energy-related vulnerabilities. These actions have resulted in programs that have significantly reduced DOD energy consumption and greenhouse gas emissions at domestic bases. Despite strong efforts, however, two critical security issues have thus far proven resistant to existing solutions: bases’ vulnerability to civilian power outages, and the need to transport large quantities of fuel via convoys through hostile territory to forward locations. Each of these is explored below. Grid Vulnerability. DOD is unable to provide its bases with electricity when the civilian electrical grid is offline for an extended period of time. Currently, domestic military installations receive 99 percent of their electricity from the civilian power grid. As explained in a recent study from the Defense Science Board: DOD’s key problem with electricity is that **critical missions, such as national strategic awareness and national command authorities, are** almost **entirely dependent on the national transmission grid** . . . [which] is fragile, vulnerable, near its capacity limit, and outside of DOD control. In most cases, neither the grid nor on-base backup power provides sufficient reliability to ensure continuity of critical national priority functions and oversight of strategic missions in the face of a long term (several months) outage.7 The grid’s fragility was demonstrated during the 2003 Northeast blackout in which 50 million people in the United States and Canada lost power, some for up to a week, when one Ohio utility failed to properly trim trees. The blackout created cascading disruptions in sewage systems, gas station pumping, cellular communications, border check systems, and so forth, and demonstrated the interdependence of modern infrastructural systems.8 More recently, awareness has been growing that the grid is also vulnerable to purposive attacks. A report sponsored by the Department of Homeland Security suggests that a coordinated cyberattack on the grid could result in a third of the country losing power for a period of weeks or months.9 Cyberattacks on critical infrastructure are not well understood. It is not clear, for instance, whether existing terrorist groups might be able to develop the capability to conduct this type of attack. It is likely, however, that some nation-states either have or are working on developing the ability to take down the U.S. grid. In the event of a war with one of these states, it is possible, if not likely, that parts of the civilian grid would cease to function, taking with them military bases located in affected regions. Government and private organizations are currently working to secure the grid against attacks; however, it is not clear that they will be successful. Most military bases currently have backup power that allows them to function for a period of hours or, at most, a few days on their own. If power were not restored after this amount of time, the results could be disastrous. First, military assets taken offline by the crisis would not be available to help with disaster relief. Second, **during an extended blackout, global military operations could be seriously compromised; this disruption would be particularly serious if the blackout was induced during major combat operations**. During the Cold War, this type of event was far less likely because the United States and Soviet Union shared the common understanding that **blinding an opponent with a grid blackout** **could escalate to nuclear war**. America’s current **opponents**, however, **may not share this fear or be deterred by this possibility**. In 2008, the Defense Science Board stressed that DOD should mitigate the electrical grid’s vulnerabilities by turning military installations into “**islands**” of energy self-sufficiency. The department has made efforts to do so by promoting efficiency programs that lower power consumption on bases and by constructing renewable power generation facilities on selected bases. **Unfortunately, these programs will not come close to reaching the goal of islanding the vast majority of bases**. Even with massive investment in efficiency and renewables, most bases would not be able to function for more than a few days after the civilian grid went offline Unlike other alternative sources of energy, **small reactors have the potential to solve DOD’s vulnerability to grid outages**. Most bases have relatively light power demands when compared to civilian towns or cities. Small reactors could easily support bases’ power demands separate from the civilian grid during crises. In some cases, the reactors could be designed to produce enough power not only to supply the base, but also to provide critical services in surrounding towns during long-term outages. Strategically, islanding bases with small reactors has another benefit. One of the main reasons an enemy might be willing to risk reprisals by taking down the U.S. grid during a period of military hostilities would be to affect ongoing military operations. Without the lifeline of intelligence, communication, and logistics provided by U.S. domestic bases, American military operations would be compromised in almost any conceivable contingency. Making bases more resilient to civilian power outages would reduce the incentive for an opponent to attack the grid. An opponent might still attempt to take down the grid for the sake of disrupting civilian systems, but the powerful incentive to do so in order to win an ongoing battle or war would be greatly reduced.

#### Collapse of America from external factors causes global transition wars.

Brzezinski ’05Zbigniew was the National Security Advisor for the Carter Administration and former Professor of Foreign Policy at Johns Hopkins University, 2005, “The Choice: Global Domination or Global Leadership”

History is a record of change, a reminder that nothing endures indefinitely. It can also remind us, however. That some things endure for a long time, and when they disappear, the status quo ante does not reappear. So it will be with the current **American global preponderance**. It, too, **will fade at some point**, probably later than some wish and earlier than many Americans take for granted. The key question is: What will replace it? **An abrupt termination of American hegemony would without doubt precipitate global chaos, in which international anarchy would be punctuated by eruptions of truly massive destructiveness. An unguided progressive decline would have a similar effect, spread out over a long time**. But a gradual and controlled devolution of power could lead to an increasingly formalized global community of shared interest, with supranational arrangements increasingly assuming some of the special security roles of traditional nation-states. In any case **the eventual end of American Hegemony** will not involve a restoration of multipolarityamong the familiar major powers that dominated world affairs for the last two centuries. Nor will it yield to another dominant hegemony that would displace the United States by assuming a similar political, military, economic, technological, and sociocultural worldwide preeminence. The familiar powers of the last century are too fatigued or too weak to assume the role the United States now plays. It is noteworthy that since 1880, in a comparative ranking of world powers (cumulatively based on their economic strength, military budgets and assets, populations, etc.), the top five slots at sequential twenty-year intervals have been shared by just seven states: the United States, the United Kingdom, Germany, France, Russia, Japan, and China. Only in the United States, however, unambiguously earned inclusion among the top five in every one of the twenty-year intervals, and the gap in the year 200 between the top-ranked United States and the rest was vastly wider than ever before. The former majorEuropean powers––Great Britain, Germany and France––are too weak to step into the breach**.** In the next two decades, it is quite unlikely that the European Union will become sufficiently united politically to muster the popular will to compete with the United States in the politico––military arena**.** Russia is no longer an imperial power, and its central challenge is to recover socioeconomically lest it lose its far eastern territories to China.Japan’s population is aging and its economy has slowed; the conventional wisdom of the 1980s that Japan is destined to be the next “superstate” now has the ring of historical irony. China, even if it succeeds in maintaining high rates of economic growth and retains its internal political stability (both are far from certain), will at best be a regional power still constrained by an impoverished population, antiquated infrastructure, and limited appeal worldwide. The same is true of India, which additionally faces uncertainties regarding its long-term national unity. Even a coalition among the above––a most unlikely prospect, given their historical conflicts and clashing territorial claims–would lack the cohesion, muscle, and energy needed to push both America off its pedestal and sustain global stability. Some leading states, in any case, would side with America if push came to shove. Indeed, any evident American decline might precipitate efforts to reinforce America’s leadership. Most important, the shared resentment of American hegemony would not dampen the clashes of interest among states. **The more intense collisions––in the event of America’s decline––could** spark a wildfire of regional violence**, rendered all the more dangerous by the dissemination of w**eapons of **m**ass **d**estruction. The bottom line is twofold**: For the next two decades, the steadying effect of American power will be indispensable to global stability,** while the principal challenge to American power can come only from within––either from the repudiation of power by the American democracy itself, or from America’s global misuse of its own power.

### Scenario 2: Econ

**Economic incentives are at the root of escalating attacks.**

**Clabough 12**

]Writer at The New American, Adjunct Professor at [Hillsborough Community College](http://www.linkedin.com/company/hillsborough-community-college?trk=ppro_cprof), studied at the State University of New York at Albany (Raven, “Senate to Consider Cybersecurity Act of 2012”, The New American, 7/25/12, <http://www.thenewamerican.com/usnews/politics/item/12211-senate-to-consider-cybersecurity-act-of-2012>)//GP

"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." Citing remarks made by Secretary of Defense Leon Panetta and National Security Agency head General Keith Alexander on the imminence of a cyber attack and the destruction it would cause, Lieberman said, “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.” “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." Meanwhile, Republicans have threatened to delay consideration on the cyber security bill until the Senate takes up legislation on defense authorization. Senate Majority Leader Harry Reid responded to such a threat by asserting, “Failing to act on cyber security legislation not only puts our national security at risk,” but also “recklessly endangers members of our armed forces and missions around the world.”

#### Cyber-attacks threaten our entire financial system.

**Tsai 12**

Staff writer for Stars and Stripes.com Military among victims of SC revenue department cyberattackBy JOYCE TSAI Stars and Stripes Published: December 5, 2012www.stripes.com/news/military-among-victims-of-sc-revenue-department-cyberattack-1.199456

WASHINGTON – **Military members** and their families **are among the victims of** what is being called **the largest cyberattack of its kind against a state government agency. The cyberattack on South Carolina’s Department of Revenue, led to the pilfering of Social Security numbers and a wealth of other personal financial data from millions** who filed South Carolina tax returns since 1998. **In addition to raiding** the **tax records** of 3.8 million taxpayers, **international hackers** in August and September also **stole** the **Social Security numbers** of about 1.9 million dependents – **as well as information from nearly 700,000 businesses, 3.3 million bank accounts and 5,000 credit cards**. Sen. Lindsey Graham, R-S.C., sent a letter to the Defense Department leadership urging them to notify all military members and their families of the security breach. Since 1998, many military members have rotated through the state’s numerous bases and may now be living overseas. Samantha Cheek, a Department of Revenue spokeswoman, said **the state recognized that this cyberattack was “a significant issue” for military members, “in light of the uniquely mobile natures of their service.”** All affected taxpayers should receive letters of notification from the state, she said. But anyone who filed a tax return since 1998 in the state should take the following steps to protect themselves: Defense personnel should visit ProtectMyID.com/SCDOR and use the activation code SCDOR123 or call Experian’s national consumer assistance center at (866) 578-5422 by Jan. 31 to determine whether their information is at risk. If so, enroll in identity theft protection, which is being offered free for one year by the state, along with $1 million in identity theft insurance. Also current and former South Carolina business owners should contact Dun & Bradstreet Credibility Corp. at dandb.com/sc/ or (800) 279-9881 to sign up for free credit monitoring services for a year. Graham said in a Nov. 28 press conference that the data breach served as an example of the type of threat that could lead someday to “**a major cyberattack against our national security infrastructure: our power plants, our aviation systems, our financial systems**.” He and other Congressional members have been pushing for the passage of **cybersecurity legislation** that **would** ensure that businesses do more to **protect** customers **from cyberattack.**

**This outweighs nuclear war.**

**Information Week 7**

Information Week June 02, 2007 The Impact Of Cyberwarfare http://www.informationweek.com/the-impact-of-cyberwarfare/199800131

Cyberwarfare: What will it look like, how will we defend against it? Those questions have taken on new urgency, as the possibility becomes more real. Recently, the Baltic nation of **Estonia suffered several weeks of distributed denial-of-service attacks against both government and private-sector Web sites**. And late last month, a report from the Department of Defense said the People's Liberation Army of China is building up its cyberwarfare capabilities, even creating malware that could be used against enemy computer systems in first-strike attacks. To date, there have been no proven, documented cases of one nation attacking another via cyberspace. Yet **cyberwarfare is a chilling prospect that's treated among most nations with much the same reverence as** Cold War players treated **the idea of nuclear winter, mainly because of the potential large-scale economic disruption that would follow, says** Howard Schmidt, **a former White House cybersecurity adviser and former chief security officer** **at eBay and Microsoft**. **This would include shortages of supplies that could affect both citizens and the military**, he says. The **cyberattacks against Estonia primarily targeted the government, banking, media, and police sites, and they "affected the functioning of the rest of the network infrastructure** in Estonia," the European Network and Information Security Agency, or ENISA, reported on its Web site. As a result, targeted sites were inaccessible outside of Estonia for extended periods in order to ride out the attacks and to try and maintain services within the country.

#### Four internal links

#### 1) Power Grid

**WSJ 12** – President of the United States (Barack, “Taking the Cyberattack Threat Seriously”, 7/20/12, Wall Street Journal, [http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html)//GP](http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html)/GP)

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. 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.** 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.

#### 2) Trade Wars

The Hill 13

Snowden leaks unlikely to sway cyber theft negotiations with China, expert says¶ By Amrita Khalid - 07/09/13 02:44 PM ET¶ http://thehill.com/blogs/hillicon-valley/technology/309905-snowden-leaks-unlikely-to-sway-cyber-theft-negotiations-with-china-expert-says#ixzz2c9zuYIJ8

“My experience with China is that they will steal and reverse-engineer anything they can get their hands on,” said Larry M. Wortzel of the U.S. China Economic and Security Review Commission. Wortzel suggested that the president declare the issue of cyber-intellectual property theft “an extraordinary threat to national security ... or the economy of the United States,” which under current law would allow him greater powers.¶ “Under this declaration, the president, in consultation with Congress, may investigate, regulate, and freeze transactions and assets, as well as block imports and exports in order to address the threat of cyber theft and espionage,” said Wortzel.

**3) Banks—Kills Biz Con**

**Ostrer 12**

Cyber-Attacks focus on banks: As cyber-warfare evolves, countries and companies must evolve with it

By Joshua Ostrer in Sci/Tech | October 4, 2012 | Views: 133 Staff writer for Union College http://www.concordy.com/article/science-and-technology/october-4-2012/cyber-attacks-focus-on-banks-as-cyber-warfare-evolves-countries-and-companies-must-evolve-with-it/5245/

For a week, **cyber-attacks plagued the websites of major American banks**. The banks included Wells Fargo, U.S. Bank, PNC Bank, Bank of America, and J.P. Morgan Chase. At the start of the attacks, the identity of the attackers was completely unknown. However, since then groups have claimed responsibility. One such group is the “Izz ad-Din al-Qassam Cyber Fighters,” claiming to be angry over the incendiary movie trailers for ‘Innocence of Muslims’,” a movie negatively depicting Muhammad. However, some analysts doubt the claim, as **the attack contained an entirely new level of sophistication.** “**Only a handful of companies around the world could survive** a hit of 70 Gbps (Gigabytes per second) **in conjunction with the complex blend of attack vectors** we have witnessed,” said Prolexic Chief Executive Officer Scott Hammack. **The attack came in the form of** a distributed denial of service attack or **DDoS.** A DDoS attack functions by launching an overload of requests for a website until the website’s server is overwhelmed and either loses functionality, or is forced to be shut down completely. Basically imagine thousands of people trying to get through the same door at once, and then trying to squeeze through while they do it. The attack, named itsoknoproblembro, immediately attracted the attention of Prolexic technologies, “the global leader in DDoS protection services” and its Security Engineering & Response team (PLXsert). Even security companies were worried about itsoknoproblembro. “The size and sophistication of this threat has created a high-alert within various industries and with good reason…I’m proud to say we’ve successfully mitigated multiple itsoknoproblembro campaigns throughout the year, even when attack vectors have continuously modulated during the course of the assault,” said Scott Hammack. DDoS attacks also commonly use “spoofed” IP addresses. However, part of what made itsoknoproblembro so effective was that it had legitimate, non-spoofed IP addresses, enabling it to bypass protective mechanisms against “spoofed” IP addresses. While the attacks didn’t directly affect funds or personal information of the banks or their customers, many customers were unable to check their bank information for a day or more. Some analysts still believe **the attack can lead to** a loss in consumer confidence**, which could greatly impact the affected banks going forward.** Some worry that **the attack is a sign of further mayhem to come**. “These are significant attacks…they should be considered a warning of the cyber cold war,” commented Lt. General Harry D. Raduege. Raduege, who used to work for cyber divisions within the U.S., says that this attack can be classified in the latter of cyber-warfare—“**operational” attacks**, where the goal is to **disrupt infrastructure, causing a political uproar** (which there most definitely has been). Raduege ranks the attack below the “strategic” level which includes destruction of infrastructure, citizens or financial institutions, and military confrontation. Chairman of the Senate Homeland Security Committee, Senator Joe Lieberman believes the Iranian special forces are behind the attack.

**4) Oil Prices**

**Parfomak 12**

["Keeping America’s Pipelines Safe and Secure:Key Issues for Congress", Paul W. Parfomak, Specialist in Energy and Infrastructure Policy, March 13, 2012 http://www.fas.org/sgp/crs/homesec/R41536.pdf]

In addition to their vulnerability to accidents, pipelines may also be intentionally damaged by vandals and terrorists. Some pipelines may also be vulnerable to “cyber-attacks” on computer control systems or attacks on electricity grids and telecommunications networks**.** 11 Oil and gas pipelines, globally, have been a favored target of terrorists, militant groups, and organized crime. In Colombia, for example, rebels have bombed the Caño Limón oil pipeline and other pipelines over 950 times since 1993. 12 In 1996, London police foiled a plot by the Irish Republican Army to bomb gas pipelines and other utilities across the city. 13 Militants in Nigeria have repeatedly attacked pipelines and related facilities, including the simultaneous bombing of three oil pipelines in May 2007. 14 A Mexican rebel group similarly detonated bombs along Mexican oil and natural gas pipelines in July and September 2007. 15 In June 2007, the U.S. Department of Justice arrested members of a terrorist group planning to attack jet fuel pipelines and storage tanks at the John F. Kennedy (JFK) International Airport in New York. 16 Natural gas pipelines in British Columbia, Canada, were bombed six times between October 2008 and July 2009 by unknown perpetrators. 17

**Collapses the economy—Inflationary Spiral**

**Tepperman 4**

[Jonathan Tepperman, senior editor at Foreign Affairs, 5/1/2004, Charleston Daily Mail]

A surge in oil prices would hurt everyone: consumers, by making transportation and heating far more expensive; and producers, by increasing the cost of their energy and other raw materials. This would raise the price of finished goods, decreasing sales and hitting consumers yet again. Worse, as we saw in the 1970s, a sudden jump in oil prices could also cause interest rates to skyrocket, setting off a dangerous inflationary spiral.

#### Extinction

**Royal 10** (Jedediah, Director of Cooperative Threat Reduction at the U.S. Department of Defense, 2010, Economic Integration, Economic Signaling and the Problem of Economic Crises, in Economics of War and Peace: Economic, Legal and Political Perspectives, ed. Goldsmith and Brauer, p. 213-215)

Less intuitive is how periods of economic decline may increase the likelihood of external conflict. Political science literature has contributed a moderate degree of attention to the impact of economic decline and the security and defence behaviour of interdependent stales. Research in this vein has been considered at systemic, dyadic and national levels. Several notable contributions follow. First, on the systemic level. Pollins (20081 advances Modclski and Thompson's (1996) work on leadership cycle theory, finding that rhythms in the global economy are associated with the rise and fall of a pre-eminent power and the often bloody transition from one pre-eminent leader to the next. As such, exogenous shocks such as economic crises could usher in a redistribution of relative power (see also Gilpin. 19SJ) that leads to uncertainty about power balances, increasing the risk of miscalculation (Fcaron. 1995). Alternatively, even a relatively certain redistribution of power could lead to a permissive environment for conflict as a rising power may seek to challenge a declining power (Werner. 1999). Separately. Pollins (1996) also shows that global economic cycles combined with parallel leadership cycles impact the likelihood of conflict among major, medium and small powers, although he suggests that the causes and connections between global economic conditions and security conditions remain unknown. Second, on a dyadic level. Copeland's (1996. 2000) theory of trade expectations suggests that 'future expectation of trade' is a significant variable in understanding economic conditions and security behaviour of states. He argues that interdependent states arc likely to gain pacific benefits from trade so long as they have an optimistic view of future trade relations. However, if the expectations of future trade decline, particularly for difficult to replace items such as energy resources, the likelihood for conflict increases, as states will be inclined to use force to gain access to those resources. Crises could potentially be the trigger for decreased trade expectations either on its own or because it triggers protectionist moves by interdependent states.4 Third, others have considered the link between economic decline and external armed conflict at a national level. Momberg and Hess (2002) find a strong correlation between internal conflict and external conflict, particularly during periods of economic downturn. They write. The linkage, between internal and external conflict and prosperity are strong and mutually reinforcing. Economic conflict lends to spawn internal conflict, which in turn returns the favour. Moreover, the presence of a recession tends to amplify the extent to which international and external conflicts self-reinforce each other (Hlomhen? & Hess. 2(102. p. X9> Economic decline has also been linked with an increase in the likelihood of terrorism (Blombcrg. Hess. & Wee ra pan a, 2004). which has the capacity to spill across borders and lead to external tensions. Furthermore, crises generally reduce the popularity of a sitting government. "Diversionary theory" suggests that, when facing unpopularity arising from economic decline, sitting governments have increased incentives to fabricate external military conflicts to create a 'rally around the flag' effect. Wang (1996), DcRoucn (1995), and Blombcrg. Hess, and Thacker (2006) find supporting evidence showing that economic decline and use of force arc at least indirecti) correlated. Gelpi (1997). Miller (1999). and Kisangani and Pickering (2009) suggest that Ihe tendency towards diversionary tactics arc greater for democratic states than autocratic states, due to the fact that democratic leaders are generally more susceptible to being removed from office due to lack of domestic support. DeRouen (2000) has provided evidence showing that periods of weak economic performance in the United States, and thus weak Presidential popularity, are statistically linked lo an increase in the use of force. In summary, rcccni economic scholarship positively correlates economic integration with an increase in the frequency of economic crises, whereas political science scholarship links economic decline with external conflict al systemic, dyadic and national levels.' This implied connection between integration, crises and armed conflict has not featured prominently in the economic-security debate and deserves more attention.