# All Affirmative Cards- MQ Round 2

## 1AC

### Plan Text

#### US Congress should prohibit National Security Agency offensive cyber operations not authorized by a congressionally elected civilian head.

#### NSA overreach causes cyber attacks and backlash- Alexander is stepping down now and thus removing joint-command solves

Wheeler ’13 (PhD from Michigan, specialized in researching on politics, Writer for the Guardian, specializing in national security and civil liberties. She has written for blogs The Next Hurrah and Firedoglake, “After General Alexander, Obama should split the NSA to make us all safer”, <http://www.theguardian.com/commentisfree/2013/oct/21/general-alexander-obama-split-nsa>, October 21, 2013)

The NSA's aggressive pursuit of Big Data has not only invaded our privacy, but also left us more vulnerable to cyber attack. The NSA is one of its own biggest adversaries in its fight to keep America safe from cyber attacks. To fight this considerable adversary, the president should use the replacement of NSA Director Keith Alexander and his deputy, John Inglis, as an opportunity to split off NSA's defensive function and rebuild necessary trust. Commentators have long recognized the NSA had two conflicting missions: one to defend key American networks, and one to collect intelligence on our adversaries. As Wired explained three years ago: NSA headquarters … in Fort Meade, Maryland, is actually home to two different agencies under one roof. There's the signals intelligence directorate, the Big Brothers who, it is said, can tap into any electronic communication. And there's the information assurance directorate, the cyber security nerds who make sure our government's computers and telecommunications systems are hacker- and eavesdropper-free. The addition of US Cybercommand to this mix made things still worse: General Alexander has warned of attacks on the US's electrical grid that might rely on vulnerabilities similar to the ones the US exploited to attack Iran's nuclear program. Documents leaked by Edward Snowden have exposed more details about how the NSA's dual missions undermine each other. The agency uses court orders to oblige Google to turn over its users' data under the Prism program, while finding ways around Google's encryption when compiling contact lists of unsuspecting Google users in collection supervised by no court. While the NSA points to vulnerabilities of American business networks and communications, it works with companies to "insert vulnerabilities into commercial encryption systems" and "influence policies, standards and specification for commercial public key technology". Even as NSA and other national security leaders warn that cyberattacks (pdf) present the biggest threat to the country, NSA is leaving open or even creating vulnerabilities that our adversaries can exploit. As security expert Bruce Schneier described: Finding a vulnerability – or creating one – and keeping it secret to attack the bad guys necessarily leaves the good guys more vulnerable. The NSA is violating the trust needed to accomplish its goal of protecting America's networks. The NSA has exacerbated this trust problem in a slew of ways. Last year, Alexander donned a hacker costume and went to the computer security DefCon convention to schmooze hackers. While there, he made a series of misleading statements – denying the NSA collects data on millions of Americans – that set up James Clapper's more famous repetition of the same lie in March of this year. This year, Alexander attended Black Hat conference (this time, without a hacker costume) and warned of the "terrorist walk[ing] among us". That same day, another Snowden-leaked document revealed the NSA considered encryption – used by many computer security professionals – indication of a potential terrorist under Xkeyscore. More recently, an illustration on a slide (pdf) reviewing the NSA's efforts to crack Tor – a sophisticated encryption system used by many security experts – identifies Tor users as terrorists. In fact, the NSA's minimization procedures allow it (pdf) to keep all encrypted communication, effectively targeting those who try to protect themselves. Effectively, NSA treats hackers, who should be key allies, as terrorists. Corporations, too, appear to be growing wary of the NSA. Shane Harris reported that "many corporate participants" in an cyber security information-sharing effort say: General Alexander's primary motive has not been to share what the NSA knows about hackers. It's to get intelligence from the companies. Cloud storage and security firms worry about losing business to other countries or to private storage because of NSA's snooping. The NSA has also proven unworthy of the general public's trust for a key scheme it wants to use to catch hackers. Alexander has sought the authority for the NSA to "live on the networks", copying and analyzing data that travels within the US to find any malicious code that might indicate a cyber attack. They already conduct similar analysis (in search of cyber attacks, but also terrorists) with data presumed to be foreign that nevertheless traverses the United States. Only after three years of conducting such collection did the NSA explain what it was doing to the Fisa court. In response, in a 2011 opinion (pdf), the court not only determined the collection had been deliberate (not unintentional, as the NSA and its defenders still claim), but had also violated the fourth amendment. Yet, despite of being caught breaking the law protecting Americans, the NSA refuses to reveal the extent of this deliberate collection of Americans' data to either the Fisa court or Congress. The NSA did not provide such information in response to a request from the Fisa court, and the NSA has blown off Senator Ron Wyden's multiple requests by claiming that to do so would infringe on Americans' privacy and threaten its ability to conduct this collection. There are even hints that the NSA relies on a secret, fairly shocking DOJ opinion to conduct some of its cyber security collection. In short, because the NSA has prioritized collecting vast amounts of information – and getting it in bulk, rather than based on particularized suspicion – and even preparing offensive attacks, it has taken actions that increase our exposure to network attacks, all while insisting cyber attacks are the biggest threat to the country. And that has enabled it to demand new authorities to protect against the attacks it has made easier. Metaphorically, the NSA has pursued its search for intelligence by partly disabling the locks to all our front doors. Having thus left us exposed, it demands the authority to be able to enter our homes to look around and see if those disabled locks have allowed any nasty types to get in. Given the way the NSA's data retention procedures have gone beyond the letter of the law to allow them to keep Americans' data if it presents a threat to property (rather than just a threat of bodily harm), while the NSA is looking for nasty types, they might also make sure you don't have any music or movies for which you don't have a receipt. Thus it has happened that, in the name of preventing invaders, the NSA has itself invaded. President Obama has claimed he welcomes a debate about the proper balance between security and privacy – though it's not at all clear privacy and security present a real tradeoff. But there is a real tradeoff between security by defense and security by aggression – the latter as currently practised by the NSA. With all functions of the NSA and Cybercommand under "big data" enthusiast Keith Alexander, there was no debate. He inherited the Bush administration's dragnet approach, and has made it his own, claiming – despite evidence to the contrary – each dragnet program has been critical for defending against terrorism. And that approach demands access to as much data as possible with minimal technical challenge. But now, with the need to replace Alexander, Obama has an opportunity to consider defense over "big data". At the very least, Obama should consider breaking out the NSA's defensive and offensive functions to create competing champions, one fighting to create holes, and one fighting to plug them. The Department of Homeland Security – an agency far better prepared to defend against threats – might be a better home for such a defensive function. Preferably, the defensive function could operate transparently, with the ability and trust to share information about vulnerabilities. Sure, that might well result in the offensive fighters hoarding their data, even from those empowered to protect the country. But that, at least, would highlight the problem. So long as the NSA prioritizes exploiting data that should be shared for the defense of the country, the agency will be one of America's most formidable adversaries in the effort to keep the US safe from cyber attacks.

#### Civilian control best

Strobel and Hosenball ’13 (Warren Strobel (U.S. Foreign Policy and National Security Editor @ Reuters) and Mark Hosenball, Reuters, “U.S. nears decision to split leadership of NSA, Cyber Command: sources”, <http://www.reuters.com/article/2013/11/27/us-usa-security-nsa-idUSBRE9AQ1BG20131127?feedType=RSS&feedName=everything&virtualBrandChannel=11563>, November 27, 2013)

(Reuters) - The White House is nearing a decision on splitting up the eavesdropping National Security Agency and U.S. Cyber Command, which conducts cyber warfare, a proposed reform prompted in part by revelations of NSA's widespread snooping, individuals briefed on the matter said on Wednesday. As part of the emerging plan, the NSA likely would get a civilian director for the first time in its 61-year history, the individuals said. Both agencies are now headed by the same person, Army General Keith Alexander, who is retiring in March as NSA's longest-serving director. While Alexander is highly regarded in the intelligence community, critics have questioned the current arrangement. They say it concentrates too much power in one individual and that the two agencies have different missions. NSA monitors phone, email and other communications for national security threats. Cyber Command defends Pentagon and other U.S. computer networks, infiltrates adversary networks and conducts offensive cyberwarfare. Two administration officials confirmed that the discussions about the split are nearing a critical stage. They spoke on condition of anonymity because no announcement has been made. White House spokeswoman Caitlin Hayden said President Barack Obama has not made a final decision. "With General Alexander's planned departure next spring, this is a natural point to look at this question to ensure we are appropriately postured to address current and future security needs," Hayden said. "We have no new decisions to announce at this point." But one official said that it was possible a decision could come soon and could even be made public simultaneously with the results of White House reviews of NSA activities prompted by disclosures by former contractor Edward Snowden. An unclassified version of one of two reviews, conducted by a group of outside experts, is tentatively due to be released in mid-December. Snowden gave media organizations highly classified documents describing electronic snooping by the agency and its British counterpart, Government Communications Headquarters GCHQ, that was far more extensive than previously known. He is in Russia where he was granted temporary asylum. Since its inception in 1952, NSA has been led by a general or admiral, with a civilian deputy director. Under the emerging plan, the director would be a civilian and the head of Cyber Command, which is a U.S. military command, would be a military officer. Reuters reported last month that Vice Admiral Michael Rogers, commander of the U.S. Navy's 10th Fleet and the Navy's top cyberwarfare officer, was a leading candidate to be the next NSA director. Rogers is now more likely to take over U.S. Cyber Command, individuals familiar with the matter said. A senior administration official, speaking on condition of anonymity, said: "Given that we are still looking at the question of whether the position would be split, we are not yet considering preferred candidates."

### Advantage 1: ~~NSA Overreach~~

#### Cyber war causes nuclear lashout

Fritz ‘9 (Jason - former Captain of the U.S. Army, July, Hacking Nuclear Command and Control)

The US uses the two-man rule to achieve a higher level of security in nuclear affairs. Under this rule two authorized personnel must be present and in agreement during critical stages of nuclear command and control. The President must jointly issue a launch order with the Secretary of Defense; Minuteman missile operators must agree that the launch order is valid; and on a submarine, both the commanding officer and executive officer must agree that the order to launch is valid. In the US, in order to execute a nuclear launch, an Emergency Action Message (EAM) is needed. This is a preformatted message that directs nuclear forces to execute a specific attack. The contents of an EAM change daily and consist of a complex code read by a human voice. Regular monitoring by shortwave listeners and videos posted to YouTube provide insight into how these work. These are issued from the NMCC, or in the event of destruction, from the designated hierarchy of command and control centres. Once a command centre has confirmed the EAM, using the two-man rule, the Permissive Action Link (PAL) codes are entered to arm the weapons and the message is sent out. These messages are sent in digital format via the secure Automatic Digital Network and then relayed to aircraft via single-sideband radio transmitters of the High Frequency Global Communications System, and, at least in the past, sent to nuclear capable submarines via Very Low Frequency (Greenemeier 2008, Hardisty 1985). The technical details of VLF submarine communication methods can be found online, including PC-based VLF reception. Some reports have noted a Pentagon review, which showed a potential “electronic back door into the US Navy’s system for broadcasting nuclear launch orders to Trident submarines” (Peterson 2004). The investigation showed that cyber terrorists could potentially infiltrate this network and insert false orders for launch. The investigation led to “elaborate new instructions for validating launch orders” (Blair 2003). Adding further to the concern of cyber terrorists seizing control over submarine launched nuclear missiles; The Royal Navy announced in 2008 that it would be installing a Microsoft Windows operating system on its nuclear submarines (Page 2008). The choice of operating system, apparently based on Windows XP, is not as alarming as the advertising of such a system is. This may attract hackers and narrow the necessary reconnaissance to learning its details and potential exploits. It is unlikely that the operating system would play a direct role in the signal to launch, although this is far from certain. Knowledge of the operating system may lead to the insertion of malicious code, which could be used to gain accelerating privileges, tracking, valuable information, and deception that could subsequently be used to initiate a launch. Remember from Chapter 2 that the UK’s nuclear submarines have the authority to launch if they believe the central command has been destroyed. Attempts by cyber terrorists to create the illusion of a decapitating strike could also be used to engage fail-deadly systems. Open source knowledge is scarce as to whether Russia continues to operate such a system. However evidence suggests that they have in the past. Perimetr, also known as Dead Hand, was an automated system set to launch a mass scale nuclear attack in the event of a decapitation strike against Soviet leadership and military. In a crisis, military officials would send a coded message to the bunkers, switching on the dead hand. If nearby ground-level sensors detected a nuclear attack on Moscow, and if a break was detected in communications links with top military commanders, the system would send low-frequency signals over underground antennas to special rockets. Flying high over missile fields and other military sites, these rockets in turn would broadcast attack orders to missiles, bombers and, via radio relays, submarines at sea. Contrary to some Western beliefs, Dr. Blair says, many of Russia's nuclear-armed missiles in underground silos and on mobile launchers can be fired automatically. (Broad 1993) Assuming such a system is still active, cyber terrorists would need to create a crisis situation in order to activate Perimetr, and then fool it into believing a decapitating strike had taken place. While this is not an easy task, the information age makes it easier. Cyber reconnaissance could help locate the machine and learn its inner workings. This could be done by targeting the computers high of level official’s—anyone who has reportedly worked on such a project, or individuals involved in military operations at underground facilities, such as those reported to be located at Yamantau and Kosvinksy mountains in the central southern Urals (Rosenbaum 2007, Blair 2008) Indirect Control of Launch Cyber terrorists could cause incorrect information to be transmitted, received, or displayed at nuclear command and control centres, or shut down these centres’ computer networks completely. In 1995, a Norwegian scientific sounding rocket was mistaken by Russian early warning systems as a nuclear missile launched from a US submarine. A radar operator used Krokus to notify a general on duty who decided to alert the highest levels. Kavkaz was implemented, all three chegets activated, and the countdown for a nuclear decision began. It took eight minutes before the missile was properly identified—a considerable amount of time considering the speed with which a nuclear response must be decided upon (Aftergood 2000). Creating a false signal in these early warning systems would be relatively easy using computer network operations. The real difficulty would be gaining access to these systems as they are most likely on a closed network. However, if they are transmitting wirelessly, that may provide an entry point, and information gained through the internet may reveal the details, such as passwords and software, for gaining entrance to the closed network. If access was obtained, a false alarm could be followed by something like a DDoS attack, so the operators believe an attack may be imminent, yet they can no longer verify it. This could add pressure to the decision making process**,** and if coordinated precisely, could appear as a first round EMP burst. Terrorist groups could also attempt to launch a non-nuclear missile, such as the one used by Norway, in an attempt to fool the system. The number of states who possess such technology is far greater than the number of states who possess nuclear weapons. Obtaining them would be considerably easier, especially when enhancing operations through computer network operations. Combining traditional terrorist methods with cyber techniques opens opportunities neither could accomplish on their own. For example, radar stations might be more vulnerable to a computer attack, while satellites are more vulnerable to jamming from a laser beam, thus together they deny dual phenomenology. Mapping communications networks through cyber reconnaissance may expose weaknesses, and automated scanning devices created by more experienced hackers can be readily found on the internet. Intercepting or spoofing communications is a highly complex science. These systems are designed to protect against the world’s most powerful and well funded militaries. Yet, there are recurring gaffes, and the very nature of asymmetric warfare is to bypass complexities by finding simple loopholes. For example, commercially available software for voice-morphing could be used to capture voice commands within the command and control structure, cut these sound bytes into phonemes, and splice it back together in order to issue false voice commands (Andersen 2001, Chapter 16). Spoofing could also be used to escalate a volatile situation in the hopes of starting a nuclear war**.** “ “In June 1998, a group of international hackers calling themselves Milw0rm hacked the web site of India’s Bhabha Atomic Research Center (BARC) and put up a spoofed web page showing a mushroom cloud and the text “If a nuclear war does start, you will be the first to scream” (Denning 1999). Hacker web-page defacements like these are often derided by critics of cyber terrorism as simply being a nuisance which causes no significant harm. However, web-page defacements are becoming more common, and they point towards alarming possibilities in subversion. During the 2007 cyber attacks against Estonia, a counterfeit letter of apology from Prime Minister Andrus Ansip was planted on his political party website (Grant 2007). This took place amid the confusion of mass DDoS attacks, real world protests, and accusations between governments.

#### Escalates to global war

Lawson ‘9 (Sean, Assistant professor in the Department of Communication at the University of Utah, Cross-Domain Response to Cyber Attacks and the Threat of Conflict, p. <http://www.seanlawson.net/?p=477>, June 13, 2009)

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 resolveÃ¢â‚¬Â¦ Removing the capacity for rational action may result in completely unforeseen consequences, including longer and bloodier battles than may otherwise have been.” [4] Ã¯Â»Â¿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]

#### Cyberwarfare draws in space war

Coleman ‘10 (Kevin Coleman, Defense Tech Chief Cyber War Correspondent, Cyber War = Space War, <http://defensetech.org/2010/03/01/cyber-war-space-war/#ixzz1948Fvj1r>, March 1, 2010)

While the satellite broadband market slowed in 2009 because of the poor economy, it still increased. The market continues to expand after U.S. regulators outlined the national broadband plan that allows satellite operators to use their radio spectrum for Internet traffic. That is why cyber security professionals are so concerned about the convergence of cyber space and space. Its becoming increasingly evident that any future war between modern militaries would be both a space war and a cyber war, in fact, they would be one and the same. Russia, China, and the U.S. have all stated they don’t want a space war, but are all preparing for one if one occurs. That sounds so familiar – oh wait a minute, didn’t Russia, China and the U.S. say the same thing about cyber war? Yes, they did. Satellites in geostationary orbits provide broadband connectivity to businesses and customers. Those satellites and their computer control ground stations present a viable target for offensive cyber actions. A hacker could disrupt or interfere with satellite control communications and could disrupt the delivery of broadband services. In the absence of such command signals, a satellite would malfunction. Worldwide attention focused on China’s successful anti-satellite missile test. While military officials question the scale and progress of the Chinese anti-satellite program, one has to wonder if China has already tested their anti-satellite cyber weapon. Military leaders are all too aware of the convergence of space and cyber space. An increasing percentage of military operations occur in cyber space and are integrated with and dependent on communication satellite systems in outer space.

#### Space war causes extinction

Mitchell et al ‘1 (Dr. Gordon, Associate Professor of Communication and Director of Debate at the University of Pittsburgh, ISIS Briefing on Ballistic Missile Defence, “Missile Defence: Trans-Atlantic Diplomacy at a Crossroads”, No. 6 July, http://www.isisuk.demon.co.uk/0811/isis/uk/bmd/no6.html, July 2001)

The dizzying speed of space warfare would introduce intense ‘use or lose’ pressure into strategic calculations, with the spectre of split-second attacks creating incentives to rig orbiting. Death Start with automated ‘hair trigger’ devices. In theory, this automation would enhance survivability of vulnerable space weapon platforms. However, by taking the decision to commit violence out of human hands and endowing computers with authority to make war, military planners could sow insidious seeds of accidental conflict. Yale sociologist Charles Perrow has analyzed ‘complexlyinteractive, tightly coupled’ industrial systems such as space weapons, which have many sophisticated components that all depend on each other’s flawless performance. According to Perrow, this interlocking complexity makes it impossible to foresee all the different ways such systems could fail. As Perrow explains, ‘[t]he odd term “normal accident” is meant to signal that, given the system characteristics, multiple and unexpected interactions of failures are inevitable’.36 Deployment of space weapons with predelegated authority to fire death rays or unleash killer projectiles would likely make war itself inevitable, given the susceptibility of such systems to “normal accidents’. It is chilling to contemplate the possible effects of a space war. According to retired Lt. Col. Robert M. Bowman, ‘even a tiny projectile reentering from space strikes the earth with such high velocity that it can do enormous damage- even more than would be done by a nuclear weapon of the same size!’.37 In the same Star Wars technology touted as a quintessential tool of peace, defence analyst David Langford sees one of the most destabilizing offensive weapons ever conceived: ’One imagines dead cities of microwave-grilled people’. Given this unique potential for destruction, it is not hard to imagine that any nation subjected to space weapon attack would retaliate with maximum force, including use of nuclear biological, and/or chemical weapons. An accidental war sparked by a computer glitch in space could plunge the world into the most destructive military conflict ever seen.

#### A cyber attack has the same fallout as a nuclear weapon- economic and military ruin

Greenemeier ‘7 (Larry Greenemeier and Sharon Gaudin, “The Impact Of Cyberwarfare”, <http://www.informationweek.com/the-impact-of-cyberwarfare/199800131>, June 2, 2007)

It's a chilling prospect, too potentially devastating to ignore. 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. Distributed denial-of-service attacks are particularly difficult to prevent and require a lot of coordination to contain the damage when multiple sites are hit. In order to weather the 128 strikes launched against its cyberinfrastructure, Estonia sought help from not only its Computer Emergency Readiness Team, established late last year, but also the Trans-European Research and Education Networking Association and Computer Emergency Readiness Teams in other countries, including Finland and Germany, according to ENISA.

#### NSA overreach will trigger these wars through Tailored Access Operations

Nakashima ’13 (Ellen Nakashima, national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties. She previously served as a Southeast Asia correspondent for the paper. She wrote about the presidential candidacy of Al Gore and co-authored a biography of Gore, and has also covered federal agencies, Virginia state politics and local affairs. She joined the Post in 1995. “Dual-leadership role at NSA and Cyber Command stirs debate”, <http://www.washingtonpost.com/world/national-security/dual-leadership-role-at-nsa-and-cyber-command-stirs-debate/2013/10/06/ffb2ac40-2c59-11e3-97a3-ff2758228523_story.html>, October 6, 2013)

During suspected Iranian cyber­attacks on the Web sites of commercial banks last year, Gen. Keith B. Alexander, who simultaneously heads the country’s largest electronic spy agency and the military’s Cyber Command, proposed a simple solution: Shut off the attacks at their source. “We had the expertise and could have done something about it,” said one U.S. official, who like others interviewed for this store spoke on the condition of anonymity to describe sensitive discussions. “We’re sitting on their networks overseas. Why don’t we just turn it off?” But the proposal to send a simple computer “reset” command to the attacking servers was ultimately rejected by National Security Council officials this year because the attacks were not causing enough harm to warrant an offensive response. The episode shows the willingness — some say eagerness — of Alexander to use his authority to conduct offensive actions to fend off attacks against the private sector. If a similar proposal were on the table today, it would be the new cyber-teams that Alexander is creating to defend the nation that probably would do the job. As he builds out U.S. Cyber Command at Fort Meade, Md., and other installations to a fighting force of 6,000 over the next three years, there are fresh questions about the wisdom of so much power residing in one “dual-hatted” official. The debate has taken on greater significance in the wake of disclosures by former National Security Agency contractor Edward Snowden about the sweeping scope of the agency’s domestic surveillance to thwart terrorist attacks and gain foreign intelligence. “The mashing together of the NSA and Cyber Command has blurred the lines between a military command and a national spy agency,” said Peter Singer, a Brookings Institution expert on evolving modes of warfare. Alexander disagrees. “It’s one network,” he said in a recent interview. “We all operate on the same network. You create more problems by trying to separate them and have two people fighting over who’s in charge [of both missions] than putting it all together. I think our nation benefits from that.” He said that other countries “do similar things.” Britain’s GCHQ, the equivalent of the NSA, is able to conduct espionage and computer-network attacks. With Alexander expected to retire next year after eight years as the longest-serving NSA director, his successor will face the questions. Administration officials acknowledge that there are concerns with what they call the dual-hat assignment, which includes regularly briefing the president on counterterrorism. “It is an unusual arrangement,” said one senior administration official, speaking on the condition of anonymity. “I’m sure that debate will resurface when General Alexander leaves that position — whether that’s the right mixture to have.” When it comes to cyber­attacks, much of it is done by the NSA’s Tailored Access Operations unit, officials say. Many of the operators are uniformed military personnel who spy on overseas networks for national intelligence priorities, including targets such as Iran, Russia and North Korea, among other countries. According to interviews with U.S. officials, these same personnel, who operate under intelligence legal authorities, may switch to a military authority when they are ordered to conduct a computer attack under an execute order by the president and the defense secretary. The process is documented. “You can be doing intelligence-gathering one second and then pull the trigger on an offensive op the next,” a former intelligence official said. “We’re allowing the same military commander to tell us how bad the problem is and propose and implement suggestions to fix it,” said Jason Healey, director of the Atlantic Council’s Cyber Statecraft Initiative. “The concentration of power at Fort Meade risks further militarizing cyberspace.”

#### Tailored Access Operations is the medium for all OCO’s

Bishop ’13 (Bryan Bishop, Bryan is a reporter for the Verge, specializing in technology, entertainment, and patent trial theatrics, “New leaks reveal broad scope of US cyber offensive”, <http://www.theverge.com/2013/8/30/4678016/new-leaks-reveal-broad-scope-of-us-cyber-offensive>, August 30, 2013)

Yesterday, The Washington Post revealed that US spy agencies proposed a $52 billion "black budget" for 2013. What would they do with all that cash? Among other things, they could spend $1 billion on cyberwarfare, with two-thirds of that funding hundreds of digital preemptive strikes to turn foreign networks into the computer equivalent of sleeper agents for the US. That's precisely what happened in 2011, according to The Washington Post's latest scoop, when US intelligence agencies carried out 231 offensive cyber-ops, using a program called GENIE to place "covert implants" into what the publication reports are "tens of thousands of machines every year." STRIKING FROM AFAR WITH SOFTWARE According to the Post, nearly 75 percent of the operations carried out under the $652 million GENIE program were aimed at top-priority targets: countries like Iran, Russia, North Korea, and China. The documents also provide a clearer view of how many of these programs are carried out. There are reference to "field operations" — basically, sending agents out to a physical location to modify software or hardware at a given site — but the more common scenario is to use custom software tools put together by the NSA's Tailored Access Operations (TAO). The documents reveal that TAO has its own set of software templates that allow it to break into common brands of routers, firewalls, and switches, and that its implants are designed to be resistant to software updates and other upgrades. They can copy stored data, "harvest" communications, and work their way into any connected networks as well.

#### Military control over the NSA risk cyber warfare that escalates

Grubbs ’13 (Larry Grubbs, Senior Lecturer in the Department of History at Georgia State University. In U.S. history, he studies foreign relations, the Cold War, and the cultural history of the five human senses. His work has appeared in the journals Diplomatic History and Peace and Change, among other publications. His book, Secular Missionaries: Americans and African Development in the 1960s, was published by the University of Massachusetts Press in 2010, “I’d Tap That,” or Whither General Keith Alexander?”, <http://tropicsofmeta.wordpress.com/2013/09/09/id-tap-that-or-whither-general-keith-alexander/>, September 9, 2013)

On August 23 the Wall Street Journal reported that National Security Agency (NSA) analysts abused their extraordinary power to conduct surveillance on love interests – “LOVEINT,” as intelligence analysts call it. This had Twitter sizzling with such hashtags as #NSAPickuplines and #NSALovePoems and the popular parody @PRISM\_NSA (a reference to the PRISM surveillance program disclosed by Edward Snowden earlier this summer) where citizens poke a little fun at the shadowy officials who spy on them in the name of national security (with such suggestive adaptations of spy-speak as “I’d tap that,” “I’d like to violate your privacy,” “After all that metadata, I’m looking forward to some content”). Meantime, Snowden, the erstwhile hacker nerd for hire employed as a contractor for the NSA, has now become a global icon, complete with his own Wikileaks line of merchandise and the essential Che Guevara-inspired t-shirts. Though hounded by Washington for his leaking of classified secrets, Snowden is justly admired by most of the world for his disclosure of the extraordinary and deeply disturbing surveillance programs the NSA has pursued without any public debate or meaningful congressional oversight. It’s hard not to enjoy these expressions of a robust humor and commitment to transparency that have remained unscathed in this age of ultra-surveillance. Perhaps, however, we can agree that it is, ultimately, no laughing matter that Americans and citizens of the world now live under a high-tech NSA Leviathan with a fetish for hyper secrecy. If, as recent reports suggest, “the NSA has secretly worked to gain access to virtually all communications entering, leaving, or going through the country,” scrutiny is overdue. When the last drop of ribald fun has been wrung from our tweets and we’ve bought as many Snowden mugs as we can afford, it might be time to put into perspective the man whom Snowden has forced out of the shadows and who is singularly responsible for some of the most disturbing tendencies of our age. Have Snowden adorn the merchandise, but let it be four-star General Keith Alexander who endures the heat of the public glare. Despite his public obscurity (until Snowden’s leaks), Alexander is a stealthy but shrewd bureaucratic operator who has reshaped the national security state to serve his agenda. As head of NSA, Cyber Command and even more shadowy parts of the surveillance state, he has built an empire that threatens the basic privacy and civil liberties of all Americans and much of the population of the world, and threatens the peace of the world with the development and proliferation of dangerous cyberweapons. The NSA under Alexander has, in the words of one expert, “transformed itself into the largest, most covert, and most potentially intrusive intelligence agency ever created.” Alexander’s Cyber-Industrial Complex Snowden blew the whistle heard round the world before embarking on his own global tour, which currently has him marooned in Moscow. Snowden’s revelations came as a bombshell to many citizens in this country and abroad, but perhaps they should not have. For one thing, Snowden only disclosed a portion of the iceberg. There are more – and possibly more dangerous – NSA programs than those he has revealed. Second and more importantly, there is, in a certain sense, nothing completely new about the recent abuse of power emanating from Fort Meade, Maryland. Though government classification of documents, and the inherently arcane nature of espionage – and especially signals intelligence, the NSA’s specialty – limits how much of the terrain we can see, enough is known about the history of the U.S. intelligence community to feel a sense of expectation. In a way, the current mania of the NSA is a fitting conclusion to generations of paranoia, power hunger, incompetence and abuse by the entire U.S. intelligence community (and their foreign partners). Nevertheless, like many others, I found the steady outpouring of new details about the NSA’s surveillance and cyberwar programs – and the absurd secrecy and hypocrisy surrounding them – left me increasingly anxious and angry about the apotheosis of the surveillance state. It’s hard to keep up: from the Bush-era revelations about warrantless wiretapping to the Obama-era disclosures from Wikileaks and Snowden, the sheer range and scope of the intelligence community’s eavesdropping makes the subject daunting and, perhaps, has induced fatalism in many Americans. To make sense of it all, it is helpful to revisit the work of the most reliable guide to all things NSA, James Bamford, and to read his latest contributions. Bamford, author of four finely researched volumes on the history of the NSA and its pre-1952 signals intelligence predecessors dating back to the First World War, is THE expert on the agency. Since 1982, when he published The Puzzle Palace, Bamford has doggedly pursued as much information as possible about what the secretive agency – often referred to as No Such Agency – does, how, and why. Through Freedom of Information Act requests and interviews with current and former NSA officials, he follows the trail of an agency dedicated to concealment. The cover of The Puzzle Palace depicts an ear, the symbol of eavesdropping, and he often writes there and in subsequent books about the NSA turning its “ear” this way and that as it seeks to listen in on international – and, increasingly, domestic – communications. A thoughtful profile of Bamford earlier this summer by Alexander Nazaryan for The New Yorker notes that even his earliest writings warned of the NSA’s indifference to legal restraints and its voracious appetite for as much information as it could possibly get, even if it meant violating its charter by spying on Americans. By 2008, Bamford had published a scathing takedown of the agency’s exploitation of 9/11, The Shadow Factory. Written shortly after Alexander had succeeded General Michael Hayden, the book makes only a few brief references to the new director of the agency. However, in three articles published in 2012-13 – two for Wired and one for The New York Review of Books – Bamford has zeroed in on Alexander and the behemoth that his agency has become. Bamford, though described by Nazaryan as “a slightly mischievous character,” is ideally suited to offer this introduction to Alexander in his June 2013 contribution to Wired: …. Never before has anyone in America’s intelligence sphere come close to his degree of power, the number of people under his command, the expanse of his rule, the length of his reign, or the depth of his secrecy. A four-star Army general, his authority extends across three domains: He is director of the world’s largest intelligence service, the National Security Agency; chief of the Central Security Service; and commander of US Cyber Command. As such, he has his own secret military, presiding over the Navy’s 10th Fleet, the 24th Air Force, and the Second Army. The massive expansion of Alexander’s cyber warfare resources has been illustrated by one of Snowden’s latest revelations. At the end of August, we learned that in 2011 alone, the United States “carried out 231 offensive cyber-operations,” mostly aimed at such adversaries as Russia, China, Iran, and North Korea. Despite American claims that China is threatening the stability of the world with its hacking, the United States remains the most prolific in cyber warfare. Alexander has used the specter of a devastating cyberattack – what former CIA Director and Secretary of Defense Leon Panetta calls “a cyber Pearl Harbor” – on the United States as principal justification for amassing control over so much data and erecting such a formidable institutional edifice. One can only sigh, perhaps, at the inevitability that someone like Alexander would respond to the drop off of actual global terrorism against American interests by invoking a new, frightening-sounding if vague bogeyman. As a bureaucratic strategy, the use of cyber threats to justify ever-growing “cyberspace operations” budgets for both the NSA and the Department of Defense has been a signature success. At a time when sequestration has hit other intelligence agencies, Alexander has been able to spend more and more. The NSA’s massive expansion of the headquarters at Fort Meade and several facilities across the country and its enlistment of “cyberattack teams” has, in turn, been very good for certain businesses. “What’s good for Alexander,” writes Bamford, “is good for the fortunes of the cyber-industrial complex, a burgeoning sector made up of many of the same defense contractors who grew rich supplying the wars in Iraq and Afghanistan.” With $30 billion being spent annually on cybersecurity the bonanza shows no signs of slowing down, as companies build or expand vast facilities and hire armies of “attack and penetration consultants.” Snowdens abound. What Alexander has done is to persuade Washington that the best defense against this threat is a great offense. Established in 2009 by the Pentagon, US Cyber Command has become a key part of Alexander’s realm. As he explained recently during congressional testimony, “I would like to be clear that this team, this defend-the-nation team, is not a defensive team.” Cyber Command has over 14,000 personnel. The goal has been to “dominate cyberspace” the same way the United States armed forces “dominate air and space.” That dominance, of course, comes at the expense not only of other countries, but of American citizens who value even a modicum of privacy. For all his personal blandness (he “more closely resembles a head librarian than George Patton. His face is anemic, his lips a neutral horizontal line… Some combat types had a derisive nickname for him: Alexander the Geek”), Alexander embodies and is responsible for a number of disturbing tendencies that make apathy no longer an option. Bamford quotes a “senior intelligence official” familiar with the NSA’s recent success at code-breaking: “Everybody’s a target; everybody with communication is a target.” The NSA is getting better and better at reading even the encrypted information of both governments and individual citizens in the United States and abroad. To store all of the data the NSA is swiping, it has erected the Utah Data Center at a staggering cost of $2 billion. This heavily protected facility “will become, in effect, the NSA’s cloud.” It will take in data from American spy satellites, overseas listening posts and a series of perhaps ten to twenty NSA domestic listening posts, “secret monitoring rooms in telecom facilities throughout the US.” (Bamford notes that these secret rooms, called “switches,” have not been a secret for some time, as the practice dates back to the immediate aftermath of 9/11, but the NSA refuses to acknowledge their existence.) The data then becomes fodder for “NSA code breakers, data-miners, China analysts, counterterrorism specialists, and others” at Fort Meade and beyond. As ever, Bamford captures the drama: Flowing through its servers and routers and stored in near-bottomless databases will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails – parking receipts, travel itineraries, bookstore purchases, and other digital “pocket litter.” It is, in some measure, the realization of the “total information awareness” program created during the first term of the Bush administration – an effort that was killed by Congress in 2003 after it caused an outcry over its potential for invading Americans’ privacy. From James Bamford, “The NSA Is Building the Country’s Biggest Spy Center (Watch What You Say)” Menacing, all-encompassing systems of information gathering are unsettling, to be sure, but so, too, is the human failure. Bamford strongly doubts Alexander’s ambitious programs are protecting Americans. If the NSA is so much better as a result of its recent buildup, why did it fail to catch “the near-disastrous attempted attacks by the underwear bomber on a flight to Detroit in 2009 and by the car bomber in Times Square in 2010?” Congressional critics have argued the agency gives misleading statements that exaggerate the impact the programs have had in counterterrorism. Those who are familiar with the basics of how, historically, espionage works find it difficult to take NSA claims at face value. As Kenneth Roth, director of Human Rights Watch and a former prosecutor has argued, when U.S. intelligence has disrupted specific plots, the success has been “not because of the mass collection of our metadata but through more traditional surveillance of particular phone numbers or e-mail addresses – the kinds of targeted inquiries that easily would have justified a judicial order allowing review of records kept by communications companies.” Endgame? Fittingly, I’m writing this in downtown Atlanta, Georgia. Bamford has pointed to this city as the corporate home of “one of the most secretive” of the defense contractors to rise alongside Alexander’s empire. His Wired essay on Alexander singles out, as an extreme example of the “cyber-industrial complex,” Endgame Systems, which is located in Midtown at 817 West Peachtree Street. Such defense contractors, according to Bamford, sell the services Alexander’s conception of cyberwar requires, recruiting “cyberwarriors [who] play offense and defense,” “computer network attack specialists,” “attack and penetration consultants.” Endgame, a startup created in 2008, “is transparently antitransparent.” Wikileaks disclosed an internal email quoting the company’s desire to stay that way: “We don’t ever want to see our name in a press release.” Endgame is, however, too flush with capital and too important a player to go wholly unnoticed. Why? Endgame is developing ways to break into internet-connected devices through chinks in their antivirus armor. Like safecrackers listening to the click of tumblers through a stethoscope, the “vulnerability researchers” use an extensive array of digital tools to search for hidden weaknesses in commonly used programs and systems, such as Windows and Internet Explorer. And since no one else has ever discovered these unseen cracks, the manufacturers have never developed patches for them. Endgame also serves to NSA, Cyber Command, the CIA and British intelligence “a unique map showing them exactly where their targets are located. Dubbed Bonesaw, the map displays the geolocation and digital address of basically every device connected to the Internet around the world, providing what’s called network situational awareness.” For millions of dollars, Endgame can give its clients the capability of pinpointing seemingly complete information on foreign targets – such as government agencies in China – and to find in their defenses “the equivalent of a back door left open.” The high stakes this represents worries even intelligence officials, who debate the extent to which “the buying and selling of such a subscription by nation-states could be seen as an act of war.” Bamford quotes Mike Jacobs, a former top NSA official who thinks it is, indeed: “In my opinion, these activities constitute acts of war, or at least a prelude to future acts of war.” Jacobs, noting the complete lack of regulation or oversight of this development and sale of cyberweapons, says “It should be illegal. I knew about Endgame when I was in intelligence. The intelligence community didn’t like it, but they’re the largest consumer of that business.” Bamford concludes that by buying the services of a firm like Endgame, “the spy agencies are helping drive a lucrative, dangerous, and unregulated cyber arms race, one that has developed its own gray and black markets.” Endgame and its competitors could choose to sell their cyberweapons to anyone, including adversarial nations like Iran or to terrorists, a prospect Alexander himself has called his “greatest worry.” I would add that even if Endgame and others remain committed to selling only to the Americans and to American allies, the danger remains that the manic drive for offensive cyberweapons might well provoke a real war. That it would have begun shrouded in such secrecy and as a result of a corporate profit strategy would make the disaster all the greater. Endgame’s website (http://www.endgamesystems.com/) implores potential clients to “Visualize Risk, Create Opportunity.” It doesn’t offer much detail on what, exactly, Endgame does, or how to interact with its personnel. It does give us cyberwarfare with a human face on the “Meet the Team” page, which cutely mingles personal details (“Telvis is a lover of hard problems and loud music”) with a fairly conventional rundown of the executive management, albeit one stuffed with national security connections, capped by the membership on the Board of Directors, which includes former NSA Director Lt. General Kenneth A. Minihan. The retired Lt. General seems to have been swayed by the gusher of capital pouring into Endgame in the last several months. Chris Rouland, “co-founder and founding CEO,” is a Georgia Tech grad whose previous experience includes, reassuringly, a stint as Vice President at Lehman Brothers.[15] America’s economic recovery remains sluggish, the nation might yet default on its debt, but the times they are a-booming for firms such as Endgame that make themselves indispensable within the cyberwar complex. With a report this week listing sixteen firms (including Endgame) among those reaping “eight-figure venture capital deals directed at tech security firms in the past 20 months,” we seem to have a self-reinforcing mechanism at work. It is said that Snowden’s revelations have, ironically, increased the value of the services of these shadowy firms that offer “solutions” to corporate and national security planners worried about their cyber vulnerabilities. While it’s nice to see a bull market for at least one sector of the American economy, one might fail, however, to accept the Panglossian assurance from the chief marketing officer at one of these cash-rich security start-ups: “The cybersecurity market is in a renaissance period that should enable the good guys to leapfrog the bad guys in prevention and detection capabilities.” Such a claim belies not only the improbability that cash or technology alone will best “the bad guys” overseas, but also the enormous risks to American civil liberties posed by the wild west, anything goes lack of regulation and oversight that has created countless Snowdens, snooping on citizens without scrutiny at the behest of the NSA. Ultimately, where is all of this NSA growth – in numbers, money, facilities, and scope of reach in pursuit of American and foreign data – leading the nation? How, at this juncture, could the genie even be put back into the bottle as far as the restoration of constitutional protections for individuals? As a matter of national security, how much could General Alexander’s empire have helped, given the frustrations U.S. foreign policy has repeatedly faced over the last several years, such as America’s eroding influence, especially in the Middle East? What is to become of the empire when the emperor retires, as Alexander is expected to do next year? Answers are needed, but to get them requires openness to asking the questions, and that has been sorely lacking, not least due to Alexander’s personal contributions to the institutionally ingrained NSA secrecy fetish. It’s time, as Bamford suggests, for sustained congressional investigations of Snowden’s claims “or an independent body, like the 9/11 Commission.” What we do not need is someone like Alexander, inscrutable and unaccountable, amassing such power and wielding it under a cloak of secrecy.

#### Congress electing a civilian head of NSA solves overreach- Congress key

Romm ’13 (Tony Romm, technology reporter for POLITICO Pro. He closely follows tech topics and debates on Capitol Hill and before agencies like the Federal Trade Commission, keeping a close eye on issues such as online privacy, antitrust and competitiveness, tech industry lobbying and PAC spending, intellectual property and cybersecurity, “Congress could see power to confirm NSA chief”, <http://www.politico.com/story/2013/11/congress-could-seek-nsa-confirmation-99650.html>, November 10, 2013)

Frustration with the National Security Agency’s spying and the impending departure of its longtime director have fueled a congressional push to put its future leaders through the potentially grueling process of Senate confirmation — a scenario the White House has warned in the past could harm intelligence efforts. The idea — backed by California Democratic Sen. Dianne Feinstein, the leader of the Intelligence Committee and one of the NSA’s top allies in Congress — is among the more prominent agency reforms percolating on Capitol Hill, where lawmakers are rethinking the agency’s expansive surveillance authorities in light of Edward Snowden’s leaks. Some believe Senate confirmation for the director could bring sweeping change and more accountability to the ultrasecretive NSA. But it also threatens to subject the agency to public political showdowns and delays — which the Obama administration has said it wants to avoid. “Given the enormous power of the NSA and its important mission, I certainly am open to the idea of having the director being a confirmed position,” Rep. Jim Langevin (D-R.I.) said, adding: “The more oversight we have, the better.” The confirmation concept is one of several NSA reforms under serious consideration on Capitol Hill. Administration officials also have weighed whether to split leadership of the NSA away from U.S. Cyber Command — both currently led by Gen. Keith Alexander, who’s slated to depart in 2014. Such a change could forge the way for a civilian to head the NSA for the first time. For his part, Alexander has had some vetting by Congress. The Senate approved his nomination to lead CyberCom, the Pentagon’s cyberwar forces, in 2010. And the chamber approved the general’s third star before he was tapped for the NSA post in 2005. But much has changed during his record-setting tenure of eight years at the NSA, including once-unthinkable leaks about the agency’s sprawling phone record and Internet surveillance programs. As he prepares to depart the government, some members of Congress see an opportunity to rethink the agency’s future — not to mention lawmakers’ role in overseeing it. Feinstein’s new surveillance reform bill — widely panned by civil-liberties advocates as weak — contains a provision ensuring that future NSA directors obtain the Senate’s so-called advice and consent. That requirement has even drawn the backing of her bill’s opponents, including Sen. Mark Udall (D-Colo.), whose spokesman told POLITICO that Senate confirmation of NSA directors is a “long overdue measure.” And another Senate proposal, which would authorize all of the intelligence community’s activities in 2014, includes a similar confirmation mandate. That cleared Feinstein’s committee last week. However, the idea long has left a sour taste at the White House. When Feinstein’s intelligence committee counterpart in the House — Rep. Mike Rogers (R-Mich.) — tried to advance a measure that included NSA confirmation in 2011, the White House said it “strongly objects” to the change. The reason: “The administration believes that if this provision were to become law, a critical national security position would likely remain unfilled for a significant period of time, adversely impacting the management and function of the National Security Agency.” The White House declined to comment on the issue. Such a move could mean more oversight for future directors of the NSA. The confirmation process would permit two key congressional panels — Feinstein’s intelligence committee and the Senate’s top defense committee — to get a crack at questioning the NSA nominee, one intelligence aide told POLITICO. In fact, the two committees already have worked out an initial plan to ensure they can share that crucial role, the aide added. And that’s all before a vote by the full Senate, which historically has held up federal candidates when lawmakers want documents or answers from the White House. Feinstein’s plan also might serve as a signal to the White House. One former senior intelligence official told POLITICO it’s designed to ensure that the Senate gets the chance to confirm a civilian nominee, should the administration choose to go that route. A civilian NSA director would make waves at the Pentagon, where Alexander always has worn “dual hats” leading both the NSA and CyberCom. The general himself told POLITICO in October he firmly believes one director should run both entities given their overlap in mission and close proximity, with the two based at Fort Meade in Maryland.

#### Only Congress reviewing NSA solves concentration of power- outside opinions key to check cyber groupthink

Healey ’13 (Jason Healey, Director of the Cyber Statecraft Initiative at the Atlantic Council of the United States and the editor of the first military history of cyberspace, A Fierce Domain: Cyber Conflict, 1986 to 2012, “Time to Split the Cyber 'Deep State' of NSA and Cyber Command”, <http://www.huffingtonpost.com/jason-healey/keith-alexander-nsa-cyber-command_b_4031368.html>, October 2, 2013)

Imagine if the commander of U.S. Pacific Command were the leading source of information on the Chinese military threat, had the ear of Congress on China policy, ran covert military operations against China, and could decide what information on China was classified. This perverse concentration of power is similar to where the United States has found itself on cyber policy. To restore balance, Congress and the president must ensure that new initiatives to control surveillance are more than just cosmetic by reforming America's current national security cyber organizations. The same military officer -- General Keith Alexander -- is the Director of the National Security Agency, the top intelligence officer plugging the cyber threat and leading cyber policy advocate, while also the head of U.S. Cyber Command, the cyber commander ready to combat those same threats. For this latter job, he was promoted to four-star general, a rank that gives his voice more punch than other intelligence officials. The General also has significant power to decide who is allowed access to what information, either as the original classification authority or as godfather for a system his direct predecessors have called "horribly overclassifed." This concentration of power has allowed one single view of America's cyber power to lead policymakers into a cul-de-sac. The official and public U.S. policies on cyberspace emphasize peace and security, but the cyber "deep state" led by NSA and Cyber Command have essentially overridden that policy by changing the facts on the ground, in the network, through aggressive collection and covert actions. Cyberspace makes it far easier to spy on others and attack them anonymously. When I first got involved in military cyber operations in the late 1990s, this was a bad thing. But no more; the combination of NSA and Cyber Command has seized on these characteristics for short-term gain and even apparently subverted many of the technologies that were supposed to make cyberspace more resilient and secure. It is very difficult for outsiders to have any influence on such policies because in the more than eight years General Alexander has held the position, discussion on cyber policy has become increasingly stifled and chilled, both inside and outside government. For example, fifteen years ago it was common to have unclassified discussions of U.S. offensive doctrine and options in cyberspace -- but now that NSA has the lead, any debates only take place behind secure vault doors. Few outside voices can temper an increasingly militarized policy that has led to the Stuxnet attacks on industrial control systems and surveillance programs so broad the president himself has had to very publicly backtrack. Congressmen who are supposed to question the program have felt NSA's classification has driven oversight to be "inadequate" while the CIA "jokingly referred to him as Emperor Alexander ... because whatever Keith wants, Keith gets." Forget Congress; if even the Central Intelligence Agency feels he has unstoppable power, what chance do the rest of us have to influence cyber policy? The President must continue to tear down the walls of classification that have stifled discussions, but to restore balance to US cyber policy, he must go further and reduce this concentration of power. NSA must be split from U.S. Cyber Command to create separate leadership with physically distinct headquarters. This will of course create tensions and increased costs, but cyberspace is too important to grant one person have a near-monopoly on threat intelligence while simultaneously conducting active espionage, directing military force, and advising on policy. General Alexander must step down earlier than his planned 2014. Regardless of whether his views and priorities have been right or wrong, he has become a distraction to U.S. cyber efforts and eight years is too long for any director of an intelligence collection agency. Yes, General Alexander is a cyber expert and an intelligence hero whose work has saved hundreds of American lives. But this does not make him irreplaceable. The U.S. military has had generals in charge of combined offensive and defensive joint cyber commands since 1998; fifteen years should be enough time to develop a sufficient bench. The president may find that just as he has to backtrack away from NSA's cyber espionage programs, he will soon have to do to the same for U.S. Cyber Command's cyber warfare programs as well. Cyberspace isn't primarily a domain for military operations but the most liberating technology since the printing press, driven by American companies, artists, and citizens and already responsible for 4.7 precent of our GDP. This is America's true cyber power, but it is under threat from the unprecedented concentration of military cyber and a culture of classification that smothers outside opinions. As Congress reviews NSA's surveillance programs this week, they should seize the chance to restore balance to American policy to ensure the cyberspace we hand to our children and grandchildren will be at least as free and open as that which we have today.

#### External congressional checks are key to reform NSA- presidential initiatives fail

ZEGART 2009 - co-director of the Center for International Security and Cooperation (CISAC), a senior fellow at the Hoover Institution, and professor of political economy at Stanford's Graduate School of Business (Zegart, Amy B. “Spying Blind: The CIA, the FBI, and the Origins of 9/11”)

For government agencies, bounded rationality, structural secrecy, and the liability of time are only the beginning. While all organizations have difficulty adapting to changing environmental demands, government agencies have the hardest time of all because they lack three key advantages that businesses enjoy. The first is the imperative of markets to adapt or suffer the consequences. In the private sector, organizational survival is never guaranteed and everyone knows it. As Enron, Tyco, Kmart, Global Crossing, WorldCom, Polaroid, and United Airlines executives can attest, even industry leaders can fairly rapidly go from profitability to insolvency. Markets create the ultimate incentive to adapt. There is nothing quite like the prospect of unemployment to focus the mind. Government agencies live in an altogether different world. Although congressional scholars have made much of Congress’s oversight powers, the fact is that government agencies almost never fear that poor performance will lead to their death and replacement by newer, fitter organizations.46 More than twentyfive million small businesses operate in the United States. There is only one Internal Revenue Service, it has been in business since the Civil War, and nobody is about to let it go under. The House Intelligence Committee’s Report authorizing the 2005 intelligence budget makes clear just how weak Congress’s oversight powers can be. The committee wrote: “After years of trying to convince, suggest, urge, entice, cajole, and pressure [the] CIA to make wide-reaching changes to the way it conducts its HUMINT [human intelligence] mission . . . [the] CIA, in the committee’s view, continues down a road leading over a proverbial cliff.”47 This sounds more like a plea for help than an ironfisted demand for change. The truth is that government agencies are not built to adapt. They are designed to be reliable and fair, performing tasks consistently and predictably and ensuring that all citizens receive the same level of service, regardless of their wealth or connections. Every state has a Department of Motor Vehicles and every neighborhood has a post office, no matter how small or remote. The mail may be slow, but everyone in the United States can get it. The lines at the DMV may be long, but detailed rules and procedures guarantee that everyone must stand in them. Reliability and fairness have their benefits. But these benefits come with a price: The more often things are done in the same way, the harder it is to alter them. The second advantage that firms possess in the adaptation struggle is that their creators and employees want them to succeed. No one foists a new company on reluctant owners. No employee cheers silently for the day when company profits tumble and layoffs are announced. Instead, businesses are filled with organizational well-wishers who have vested interests in the company’s continued success. Competitors may be plentiful and powerful, but they must do battle from the outside. By contrast, government agencies are created by many who want them to fail. In politics, new agencies are forged by winning political coalitions who must compromise to succeed. The important point is not that winners win but that losers have a say in the organization’s design and operation. The fragmented structure of the American political system ensures that political opponents have plenty of opportunities to sabotage the creation of any new agency at the outset—hobbling it with all sorts of rules and requirements—and possess the interests and capabilities to dog the agency forever after.48 Third and finally, business leaders have far more freedom to run their organizations than public sector managers do. Business executives can determine the organization’s mission; hire and fire personnel with relatively few restraints; institute the policies, procedures, and customs they believe necessary; and attract capital from a multitude of sources. Government officials can only dream about this kind of freedom.49 Any manager working for Coca Cola knows that his mission is to sell soda. But conflicting goals are built into the very mission of public sector agencies. The U.S. Forest Service, for example, is supposed to help harvest timber and protect national park lands at the same time. In addition, although intelligence agencies are technically exempt from a number of Civil Service regulations, the process of hiring and firing personnel is still riddled with bureaucratic red tape. As we shall see in chapter 4, managers in the CIA’s clandestine service found personnel procedures so cumbersome, they often retained and even promoted poor performers instead of firing them. As one intelligence official complained, the Intelligence Community “is the Commerce Department with secrets. Fifty percent of every manager’s time is spent managing the three percent of the people in the office who shouldn’t be there. . . . Up or out? Survival of the fittest? We can’t go there.”50 Finally, intelligence agency leaders must answer to many but have few places to turn to for help. The CEO of Intel can acquire needed resources from any number of financial institutions and investors around the world. The head of the U.S. Intelligence Community cannot. Together, these forces suggest that prospects for internal reforms are not promising. What is a difficult challenge for businesses is a Herculean feat for government agencies. To adapt, all organizations must contend with bounded rationality, structural secrecy, and the liability of time. But firms are relatively lucky. They are fueled by market competition (and its shadow of death), focused by a unified mission, filled with stakeholders seeking success, armed with broad managerial discretion to match resources against organizational needs, and built to adjust as conditions change. Government agencies lack all of these adaptation advantages from birth. Agencies that do not adapt on their own may be subjected to change from the outside, either through executive branch action or through legislation. In such cases, the rational self-interest of political actors and the fragmented structure of the federal government work to block success. Rational Self-Interest of Presidents, Legislators, and National Security Bureaucrats Government officials are constrained by the incentives and capabilities that come with their positions. Although individuals have their own ideas, skills, and policy preferences, institutional incentives and capabilities exert a powerful influence, making some courses of action easier and less costly than others. These incentives and capabilities explain why, before the September 11 attacks, no president championed intelligence reform, why legislators largely avoided and blocked it, and why national security agency bureaucrats opposed it. PRESIDENTS All presidents have strong incentives to improve organizational effectiveness. To make their mark on history, they must make the bureaucracy work well for them. Perhaps even more important, presidents are also driven to enhance organizational effectiveness by the electorate, which expects far more of them than they can possibly deliver. Held responsible for everything from inflation to Iraqi democratization, presidents have good reason to ensure that government agencies adapt to changing demands as much and as fast as possible.51 The problem is that presidents are weak.52 With little time, limited political capital, few formal powers, and packed political agendas, presidents lack the capabilities to make the changes they desire. Instead, they almost always prefer to focus their efforts on policy issues that directly concern (and benefit) voters rather than on the arcane details of organizational design and operation. And who can blame them? Tax cuts and social security lock boxes win votes, but no president ever won a landslide election by changing the CIA’s personnel system. Moreover, presidents are especially reluctant to push for agency reforms in the absence of a crisis or in the presence of anticipated resistance. Presidents are thus loath to reform existing agencies through executive action or legislation. Although dozens of investigations, commissions, and experts identified shortcomings in the U.S. Intelligence Community between 1947, when the CIA was created, and the September 11, 2001, terrorist attacks, no president attempted major intelligence reform.53 Rational self-interest explains why. LEGISLATORS Self-interest leads most legislators to avoid tackling intelligence reform altogether or seek to block it. Like presidents, legislators have little incentive to delve into the messy inner workings of intelligence agency design because doing so does not provide tangible benefits to voters back home.54 Indeed, the weak electoral connection is one of the reasons congressional intelligence oversight committees continued imposing term limits for their members throughout the 1990s, long after it became clear that these regulations severely weakened the development of congressional expertise and after numerous commissions recommended abolishing them.55 When crises do arise, intelligence committee members are rewarded more for airing dirty laundry than cleaning it. They frequently hold hearings but only rarely take corrective action. The Bay of Pigs, the congressional investigations into CIA abuses during the 1970s, the Iran-Contra scandal, and the Aldrich Ames spy case all triggered major investigations but none produced fundamental change in the Intelligence Community. In addition, members of Congress care about maintaining the power of the institution. Generally, this means that legislators prefer executive arrangements that diffuse authorities and capabilities; the more agencies in the executive branch, the more power bases can accrue in Congress to oversee them. NATIONAL SECURITY AGENCY BUREAUCRATS Finally, National Security Agency bureaucrats have their own interests at stake and powerful means to pursue them. Whereas most domestic policy agencies operate in relatively autonomous policy domains—the Environmental Protection Agency (EPA), for example, has no reason to think about the design or operation of the Social Security Administration—U.S. national security agencies are more tightly connected. Policymaking inevitably crosses bureaucratic boundaries, involving diplomacy, the use of force, economic policy, and intelligence. In such a complex web, national security bureaucrats see reform as a zero-sum battle for agency autonomy and power. EPA officials may not be conjuring up ways to gain advantage over another government agency, but national security bureaucrats are. In the interdependent world of national security affairs, no agency wants to yield authority or discretion to another.56 The Problems of Decentralized Democracy Rational self-interest makes reform difficult; self-interest coupled with the decentralized structure of the U.S. federal government makes it more so. Paradoxically, some of the cherished features of American democracy impede effective agency design and raise obstacles to reform. Separation of powers, the congressional committee system, and majority rule have created a system that invites compromise and makes legislation hard to pass. This has two consequences for government agencies. First, political compromise allows opponents to cripple any new agency from the start. As Terry Moe writes, “In the political system, public bureaucracies are designed . . . by participants who explicitly want them to fail.”57 Political compromise unavoidably leads to suboptimal initial agency design, even for critical national security agencies such as the Central Intelligence Agency.58 Indeed, critics who contend that the CIA is poorly suited to meeting the needs of the post–Cold War world are only partially right: the agency was not particularly well designed to meet the United States’ Cold War needs, either. In 1947, existing intelligence agencies in the FBI, State Department, and military services succeeded in stripping the CIA of any strong centralization powers. When the CIA was created, it was flawed by design.59 The decentralized structure of American democracy also means that the worst agency problems usually are the hardest to fix. Although agencies can make some changes on their own and can also be altered by unilateral presidential action, the most far-reaching reforms almost always require new legislation. But legislative success is difficult even under the best of circumstances because it demands multiple majorities in both houses of Congress. As Philip Zelikow, executive director of the 9/11 Commission put it, “the most powerful interest group in Washington is the status quo.”60 Taken together, these three enduring realities—the nature of organizations, rational self-interest, and the fragmented federal government—provide a basic model for understanding why U.S. intelligence agencies failed to adapt to the terrorist threat before September 11, why they have not done much better since then, and why they are unlikely to improve substantially in the future. Government agencies are not built to change with the times. Because reform does not generally arise from within, it must be imposed from the outside. But even this rarely happens because all organizational changes, even the best reforms, create winners and losers, and because the political system allows losers multiple opportunities to keep winners from winning completely. Indeed, the greater the proposed change, the stronger the resistance will be. As a result, organizational adaptation almost always meets with defeat, becomes watered down, or gets shelved for another day, when the next crisis erupts.

### Advantage 2: EU-Relations Advantage

#### NSA overreach kills US-EU relations and trade

Tuccille ’13 (J.D. Tuccille is managing editor of Reason 24/7 at Reason.com. Having started his online career in the days of proprietary online services, and seen them swept away by the Internet, he's a believer in the liberating and transformative power of new media, Tuccille has worked for ZDNet, the New York Daily News, and forgotten dot-coms and dot-orgs. For years, he edited the late, lamented Freedom News Daily for the equally mourned Free-Market.Net. His provocative and often witty (says he) columns on topics including civil liberties and government overreach have appeared in publications including the Arizona Republic, the Denver Post and the Washington Times. As a result, he's been quoted, and criticized, in the pages of such publications as the New York Times and Salon., “NSA Spying Torpedoes American Business Dealings in Europe”, <http://reason.com/blog/2013/11/01/nsa-spying-torpedoes-american-business-d>, November 1, 2013)

From the beginning of the NSA mass-surveillance scandal, revelations that the U.S. spy agency was not only scooping up international communications, but had conscripted American companies into the effort have opened doors for foreign firms. Tech companies in other countries are relatively shielded from pressure by U.S. spooks (whatever their relationships with spy agencies in their own countries) and some American entrepreneurs, like Ladar Levison of Lavabit, actively urge people to avoid U.S.-based services. Worse, though, the NSA's connection to some companies is giving European politicians cover to discriminate against American businesses. Never mind that Europeans do their own fair share of spying; they now have legitimate concerns to raise about the security of data in the hands of Apple, AT&T, Google, and other familiar names. BRUSSELS—The backlash in Europe over U.S. spying is threatening an agreement that generates tens of billions of dollars in trans-Atlantic business every year—and negotiations on another pact worth many times more. A growing number of European officials are calling for the suspension of the "Safe Harbor" agreement that lets U.S. companies process commercial and personal data—sales, emails, photos—from customers in Europe. This little-known but vital deal allows more than 4,200 American companies to do business in Europe, including Internet giants like Apple, Google, Facebook and Amazon. Revelations of the extent of U.S. spying on its European allies is also threatening to undermine one of President Barack Obama's top trans-Atlantic goals: a sweeping free-trade agreement that would add an estimated $138 billion (100 billion euros) a year to each economy's gross domestic product. The Safe Harbor agreement allows companies to move data around their networks as needed. In its absence, data from Europeans might have to be stored and processed only within the physical confines of Europe—a huge expense and possibly insurmountable hurdle for many companies. Many U.S. companies would effectively be unable to operate in Europe if they were reachable by European law. Some companies could explicitly be barred from expanding their presence in Europe out of fears that they operate as pipelines to the NSA. According to the Wall Street Journal's Anton Troianovski: AT&T Inc.'s ambitions to expand in Europe have run into unexpected hurdles amid the growing outcry across the region over surveillance by the National Security Agency. German and other European officials said any attempt by AT&T to acquire a major wireless operator would face intense scrutiny, given the company's work with the U.S. agency's data-collection programs. Resistance to such a deal, voiced by officials in interviews across Europe, suggests the impact of the NSA affair could extend beyond the diplomatic sphere and damage U.S. economic interests in key markets. AT&T Chief Executive Randall Stephenson has signaled repeatedly in recent months that he is interested in buying a mobile-network operator in Europe, highlighting the potential for growth on the continent at a time when the U.S. company faces headwinds at home. Some of this resistance to American companies is legitimate; Europeans are as outraged as Americans about the spying scandal—quite possibly more so, given that continent's long history with authoritarian regimes and secret police. And some of these moves are just opportunistic; the NSA has turned into a great excuse for European politicians to openly favor well-connected companie in their own countries at the expense of U.S. firms. In a recent report (PDF), the European Parliament called out Britain, France, Germany, and Sweden for tapping directly into communications networks—though it insisted "The capacities of Sweden, France and Germany (in terms of budget and human resources) are low compared to the magnitude of the operations launched by GCHQ and the NSA and cannot be considered on the same scale". Germany's BND worked closely with the NSA to facilitate spying, and France's DGSE needed no encouragement to hoover up communications data, though it apparently aided the NSA, as did a counterpart agency in Spain. Britain's GCHQ is reported to have burrowed its way into Begian telecommunications firms in the course of its extensive cooperation with the NSA. In other words, European government officials are shocked. Shocked! But, however cynical the response, by compromising the independence of American firms, U.S. officials created a hell of a justification for other countries to torpedo those companies and favor their own.

#### It encompasses drone backlash

Osborne ’13 (Louise is a British print journalist based in Berlin. Her work has appeared in USA Today, The Washington Times, The Guardian and Deutsche Welle. She has a background in regional news, working for the Woking News and Mail and Surrey Advertiser before moving to Berlin. She now specializes in international affairs, intellectual property and culture reporting. She holds a bachelors degree in English language and Spanish from Roehampton University in London, is fluent in Spanish and has intermediate German, “Germany denies phone data sent to NSA used in drone attacks”, <http://www.theguardian.com/world/2013/aug/12/germany-phone-data-nsa-drone>, August 12, 2013)

Germany's intelligence agency, the BND, has denied that mobile phone data it sends to the NSA could be used in drone attacks carried out in Afghanistan and Pakistan. Chancellery minister Ronald Pofalla told a closed parliamentary committee that GSM data, which the BND has admitted sending to other foreign secret services, was not specific enough to pinpoint exact locations, according to Left Party politician and committee member, Steffen Bockhahn. Germany's intelligence agency, the BND, has denied that mobile phone data it sends to the NSA could be used in drone attacks carried out in Afghanistan and Pakistan. Following the meeting on Monday, Pofalla, who is responsible for the BND, told reporters the NSA and the British intelligence services, GCHQ, had sent written assurances they were abiding by German law. The BND has faced widespread criticism in Germany since it was revealed it had collaborated with the NSA and GCHQ by sending hundreds of millions of pieces of metadata every month. Over the weekend, it was reported that mobile phone information sent to the NSA could have been used in the targeting of a terrorist group, which also resulted in the death of a German citizen as part of a drone attack in Waziristan on the border of Afghanistan and Pakistan in October 2010. Germany's federal state prosecutor ruled in July that the death of 20-year-old Bünyamin E. was legal under international law because he was "not a civilian protected by international human rights law, but a member of an organised armed group". The BND has denied it sent Bünyamin E.'s phone data to the NSA, but said any information sent to foreign intelligence agencies was done so with the condition that the data must not be used as a "basis or reason for unreasonable measures", such as torture or for the "passing of a death sentence". However, Bockhahn, said it is impossible to know what foreign agencies are doing with data passed on by the BND. "You can't control [other intelligence agencies] if they take the information and use it with their own intelligence…and then use drones," he said. "Intelligence agencies are impossible to control and it is impossible to know if they accept foreign law and my feeling is they don't. Indirectly, Germany is responsible for the drones." Human rights lawyer Eberhard Schultz said if Germany's intelligence agency was responsible for sending information used in drone attacks resulting in deaths, it would violate Germany's international criminal law and the German criminal code. "That is an aid to war crimes and to murder and the murder is not justified because there was no trial and there is no chance to defend oneself," he said. Experts disputed that the information could not be used in the targeting of terrorism suspects by intelligence agencies, at least in some cases. "They are right that in a lot of cases that data is not enough to localise and target someone, but in some cases it is enough to locate a person within the cell of the mobile network and that's the problem," said Hannes Federrath, a professor of information technology and security at Hamburg University. "Even if in 90% of the cases it's not possible, and in 10% of the cases it is possible someone can be targeted, then it is an illegal situation, if data is transmitted to another secret service." Meanwhile, anti-drone campaigners said if data collected by German authorities was used to target people using drones, it could "not be accepted". "If data from Germans, no matter from who, the foreign state secret services or any other services from Germany, was used for such an aim, this is something that has to be brought to court and cleared up," said Michael Ebeling, a coordinator at the German Drone Campaign, an umbrella organisation for groups fighting against the use of drones.

#### Worse than Iraq for relations- specifically kills US-German relations

Barkin 1/16 (Noah Barkin, Bureau Chief for Germany, Austria, and Switzerland, Reuters, “Spying plunges U.S.-German ties lower than Iraq war - Merkel ally”, <http://uk.reuters.com/article/2014/01/16/uk-germany-usa-spying-idUKBREA0F0UC20140116>, January 16, 2014)

(Reuters) - Relations between Germany and the United States are worse now than during the U.S.-led invasion of Iraq a decade ago, a leading ally of Chancellor Angela Merkel said on Thursday, in a sign of mounting anger in Berlin over American spying tactics. Philipp Missfelder, foreign policy spokesman for Merkel's Christian Democrats (CDU) in parliament, said Berlin should bar U.S. access to a database of international financial transactions unless Washington promises to stop spying in Germany. The lawmaker is expected to be confirmed soon as the government coordinator for U.S. ties. Reports this week have suggested talks on a "no spying" deal, launched after revelations last year that the U.S. National Security Agency (NSA) had monitored Merkel's mobile phone, are near collapse because Washington refuses to rule out eavesdropping on one of its closest post-war allies. "2003 is generally seen as a lowpoint in German-American relations," Missfelder said, referring to the clash over former U.S. President George W. Bush's invasion of Iraq. "But if you look at the current situation the loss of trust is not smaller than it was then. Indeed it's probably bigger because this issue is preoccupying people longer and more intensively than the invasion of Iraq." The comments, among the strongest from a senior German figure since leaks of a massive U.S. spying programme first emerged last year, come a day before U.S. President Barack Obama is expected to unveil reforms of the NSA. Reuters reported last week that Obama is unlikely to announce major changes to a programme which has collected masses of raw data on the telephone calls of Americans and bugged foreign leaders including Merkel, who in 2011 received the Presidential Medal of Freedom from Obama, America's highest civilian honour. "We can see that we are not seen as loyal friends anymore, rather we are confronted with a great deal of mistrust," Missfelder said. "I am not saying we are on a level with countries that are outside of NATO, but there has been a qualitative change, at least from the American side." If talks on the "no spying" agreement fail, Berlin should support suspending a deal clinched in the aftermath of the September 11, 2001 attacks that gives the United States access to SWIFT, a global financial database, he said. The European Parliament voted last year to suspend the SWIFT agreement over concerns the U.S. was snooping on the database for financial gain, but the vote was symbolic and not binding. Missfelder listed three main German demands for the United States: an agreement not to spy on each other; the end to targeted bugging of politicians; and general agreement on how the U.S. handles the bulk "metadata" it is collecting. He said he opposed holding a transatlantic free trade deal hostage to the spying talks, and described the United States as a "friend". But he added that there were "huge expectations" tied to an upcoming visit by Merkel to the United States and spoke of disillusionment with Obama, feted in Berlin last June on the 50th anniversary of John F. Kennedy's "Ich bin ein Berliner" speech. "A lot of people had big hopes. The hopes have been disappointed," Missfelder said.

#### Two impacts-

#### First- Specifically kills TTIP

Traynor et al. ’13 (Ian Traynor in Brussels is Guardian's European editor, Louise Osborne in Berlin and Jamie Doward, The Guardian, “Key US-EU trade pact under threat after more NSA spying allegations”, <http://www.theguardian.com/world/2013/jun/30/nsa-spying-europe-claims-us-eu-trade>, June 2013)

The prospects for a new trade pact between the US and the European Union worth hundreds of billions have suffered a severe setback following allegations that Washington bugged key EU offices and intercepted phonecalls and emails from top officials. The latest reports of NSA snooping on Europe – and on Germany in particular – went well beyond previous revelations of electronic spying said to be focused on identifying suspected terrorists, extremists and organised criminals. The German publication Der Spiegel reported that it had seen documents and slides from the NSA whistleblower Edward Snowden indicating that US agencies bugged the offices of the EU in Washington and at the United Nations in New York. They are also accused of directing an operation from Nato headquarters in Brussels to infiltrate the telephone and email networks at the EU's Justus Lipsius building in the Belgian capital, the venue for EU summits and home of the European council. Without citing sources, the magazine reported that more than five years ago security officers at the EU had noticed several missed calls apparently targeting the remote maintenance system in the building that were traced to NSA offices within the Nato compound in Brussels. The impact of the Der Spiegel allegations may be felt more keenly in Germany than in Brussels. The magazine said Germany was the foremost target for the US surveillance programmes, categorising Washington's key European ally alongside China, Iraq or Saudi Arabia in the intensity of the electronic snooping. Germany's justice minister, Sabine Leutheusser-Schnarrenberger, called for an explanation from the US authorities. "If the media reports are true, it is reminiscent of the actions of enemies during the cold war," she was quoted as saying in the German newspaper Bild. "It is beyond imagination that our friends in the US view Europeans as the enemy." France later also asked the US authorities for an explanation. France's foreign minister, Laurent Fabius, said: "These acts, if confirmed, would be completely unacceptable. "We expect the American authorities to answer the legitimate concerns raised by these press revelations as quickly as possible.". Washington and Brussels are scheduled to open ambitious free trade talks next week following years of arduous preparation. Senior officials in Brussels are worried that the talks would be overshadowed by the latest disclosures of US spying on its closest allies. "Obviously we will need to see what is the impact on the trade talks," said a senior official in Brussels. A second senior official said the allegations would cause a furore in the European parliament and could then hamper relations with the US. Robert Madelin, one of Britain's most senior officials in the European commission, tweeted that EU trade negotiators always operated on the assumption that their communications were listened to. A spokesman for the European commission said: "We have immediately been in contact with the US authorities in Washington and in Brussels and have confronted them with the press reports. They have told us they are checking on the accuracy of the information released yesterday and will come back to us." There were calls from MEPs for Herman Van Rompuy, the president of the European council – who has his office in the building allegedly targeted by the US – and José Manuel Barroso, the president of the European commission, to urgently appear before the chamber to explain what steps they were taking in response to the growing body of evidence of US and British electronic surveillance of Europe through the Prism and Tempora operations. Guy Verhofstadt, the former Belgian prime minister and leader of the liberals in the European parliament, said: "This is absolutely unacceptable and must be stopped immediately. The American data collection mania has achieved another quality by spying on EU officials and their meetings. Our trust is at stake." Luxembourg's foreign minister, Jean Asselborn, told Der Spiegel: "If these reports are true, it's disgusting." Asselborn called for guarantees from the very highest level of the US government that the snooping and spying is immediately halted. Martin Schulz, the head of the European parliament, said: "I am deeply worried and shocked about the allegations of US authorities spying on EU offices. If the allegations prove to be true, it would be an extremely serious matter which will have a severe impact on EU-US relations. "On behalf of the European parliament, I demand full clarification and require further information speedily from the US authorities with regard to these allegations." There were also calls for John Kerry, the US secretary of state, to make a detour to Brussels on his way from his current trip to the Middle East, to explain US activities. "We need to get clarifications and transparency at the highest level," said Marietje Schaake, a Dutch liberal MEP. "Kerry should come to Brussels on his way back from the Middle East. This is essential for the transatlantic alliance. The US can only lead by example, and should uphold the freedoms it claims to protect against attacks from the outside. Instead we see erosion of freedoms, checks and balances, from within."

#### TTIP key to prevent US and Euro economic collapse

Rines ’13 (Samuel Rines, Samuel Rines is an economist with Chilton Capital Management in Houston, TX,   
“Can TTIP Save the West?”, <http://nationalinterest.org/commentary/can-ttip-save-the-west-9325>, October 29, 2013)

After watching their economies stagnate and sputter forward, two economic titans are sitting down to talk about a trade agreement. Currently in the early stages of negotiation between the US and European Union, the Transatlantic Trade and Investment Partnership (TTIP) could be critically important (and positive) for the future of both economies. Already critical markets for one another, the EU and US trade relationship accounts for about 30 percent of global trade, and $1.5 trillion in current-account transactions. This relationship may become much cozier soon. Normally, free-trade agreements (FTAs) would break down the barriers to trade by lowering and removing tariffs, but tariffs are already low between the world’s two largest economies. Lowering nontariff barriers to trade (NTBs) is the true prize here. NTBs make up most of the actual impediments to trade between the US and EU, and include everything from technical requirements on goods to health and agricultural standards. Mutual recognition of standards—the EU recognizing the FDA stamp of approval in drug development, for example—is an area in which agreement could create a meaningful positive feedback to both economies. For the TTIP to have a pronounced economic impact, regulatory standards will need to be integrated significantly. With the US and EU together constituting 50 percent of the world’s economy, setting firm, mutually recognized standards could spur a de facto global standards regime. Because they are imperative, NTBs also run the risk of sidelining the TTIP as lobbies and interest groups apply political pressure. Externalities are already disturbing the trade talks. The recent U.S. government shutdown caused U.S. Trade Representative Michael Froman to cancel the second round of negotiations which had been scheduled for October 7—not the best way to begin an already delicate process. The recent NSA spying fiasco is stoking concerns over data privacy and lessening already tenuous trust in US institutions. Needless to say, there is a skeptical undertone to the intellectual-property portion of the talks. The French recently summoned the US ambassador with questions about the NSA’s activities, and President Obama was forced to call Angela Merkel to tell her the US was not tapping her phone. But while these may be embarrassing instances, the rewards for removing even a portion of the NTBs are too great to ignore. The EU will fight for the inclusion of language surrounding the protection of geographical indications (GIs). GIs—designations on goods indicating a specific geographical origin or a certain quality—are potentially very valuable. The US would argue that words like Parmesan and Pilsner indicate broad product categories, not specific places. A strengthening of GIs would benefit Europe, and some global marketing by US firms with certain products would have to change. Thus far, the US has not supported GIs as a global standard, but this may change if the EU concedes some controversial point(s) on their side. Genetically modified organisms (GMOs) are a potential flashpoint. Opposition to GMOs is strong in the EU, where all GMOs must be labeled. Part of the EU’s distrust of a potential settlement around GMOs is a broader threat to their perceived high level of consumer-protection standards. The EU’s “precautionary principle” requires the producer to prove that a product is not harmful to consumers, but the US adheres to a “science-based approach” where the product must be shown to be detrimental to health before its removal. The GMO issue is important for both sides. Europeans want to know about their food, and majorities of key US crops are genetically engineered. The EU already imports more agricultural goods from the US than any other country except Brazil, and the US is the largest importer of EU agricultural products. The US and EU need the TTIP, not only to compete more favorably with the emerging world, but to spur growth in a time of stagnation on both sides of the Atlantic. The OECD has estimated that the TTIP could boost the EU economy 3-3.5 percent. More than a million jobs could be created in the US. Spain and Italy could see 140,000, and the UK more than 400,000. And per capita income could rise more than 6 percent in Spain, 10 percent in the UK, and 13 percent in the US. Not everyone will be so thrilled. A successful TTIP would erode the value of trade agreements already in place. Some countries that have long been trade partners with the US and EU will suffer. The US’s NAFTA neighbors, Mexico and Canada, will suffer relative trade losses as their trade treatment loses its exclusivity. (This likely explains the recent push by Mexico’s ambassador to the United States, Eduardo Medina Mora, for Mexico’s inclusion in TTIP.) The BRICs (Brazil, Russia, India, China and South Africa) will find their long-standing advantages of low-cost labor and production slipping. In the case of a comprehensive agreement between the US and EU that includes the removal of at least some NTBs, the Bertelsmann Foundation estimates the BRICs loss of export and import trade at more than 30% to the US and EU. The TTIP is not the only FTA currently being negotiated by the EU or the US. The EU currently has 11 such negotiations underway. And they are set to discuss an investment agreement with China (though not an FTA). The EU estimates that if all their agreements were concluded and effected today, then 2.2 million jobs could be created and 2.2 percent added to the EU’s GDP. The US is involved in the Trans-Pacific Partnership (TPP) which completed its 19th round of talks and includes a host of countries from Asia and the Americas. Again, no BRIC countries are involved, and it would be the second largest FTA to the TTIP. The nations involved in the TTP comprise 38 percent of the world’s GDP, but US participation in the discussions is mainly political—a piece of the “Asian pivot”. However, the success of the TTIP is not guaranteed. France, which has little to gain from the TTIP and therefore little incentive to bargain, has already managed to exclude “cultural exceptions” from the talks. Meanwhile Germany and the UK, which have the most to gain, are looking for the most comprehensive TTIP possible. The TTIP could, in fact, be a reason the UK has stayed in the EU. The TTIP is not a silver bullet. Its potential economic benefits should be met with at least some skepticism. The predicted gains are almost too good to be true. Consider this: If the US were to gain the entirety of its 1.1 million potential jobs today, it would reduce the unemployment rate to the Fed’s target of about 6.5 percent from 7.2 (assuming all else equal). It is probable the expectations for the negotiation will prove to be somewhat optimistic, and leave many NTBs untouched and mutual regulatory standards undetermined. The US and EU are in desperate need of growth and job generators at the moment. A bold TTIP alters the global playing field, tipping the trading field in favor of the developed world. While politically difficult, its ultimate outcome has significant ramifications for the future of global trade and regulatory standards. The economic benefits, sorely sought by both sides of the Atlantic, outweigh some of the differences in regulatory thought. With the prospect for meaningful GDP and job gains in the US, maybe the TTIP is just the push the U.S. economy needs to attain escape velocity and for the EU to begin to reduce unemployment and reaccelerate growth. It is time for the West to regain its place of leadership and prominence in the global economy.

#### Prevents EU Collapse from Euro-zone

Vilpišauskas ’13 (Ramūnas Vilpišauskas, Director of the Institute of International Relations and Political Science at Vilnius University examines the TTIP's implications for the EU’s neighborhood policies, arguing that a successfully concluded agreement could help boost the Union’s image and increase its attractiveness in Europe’s Eastern approaches, “TTIP: A Test for the European Union?”, <http://www.cepa.org/content/ttip-test-european-union>, August 6, 2013)

The Euro-zone crisis has done a great deal to damage the EU’s appeal, even though the origin of the crisis has less to do with the EU than with its members’ national policies. Quick progress on the TTIP negotiations could improve the EU’s image, making it more attractive to its neighbors, and could help revitalize the reform process in the East. Of course, even if a deal on the TTIP is reached, it will not apply directly to other countries that have or might be negotiating preferential trade agreements with the EU or the United States. There are also fears that the TTIP would result in some trade diversion due to its discriminatory provisions against third countries that are not part of the deal but trade heavily with either the United States or the EU. However, if the partnership is negotiated in line with the WTO principles designed to reduce regulatory burdens, it could become a stepping stone rather than a stumbling block on the way to broader trade liberalization.3 In such a way, it would improve trade conditions for those outside the transatlantic market as well as make closer economic relations with the EU more attractive. As negotiations on the TTIP proceed, these corollary implications for the EU’s foreign and neighborhood policies should not be lost out of sight.

#### Eurozone collapse causes World War III

Gommes, 11 -- former Columbia Law Review senior editor

(Thomas, publisher of Periscope Post, former corporate lawyer, "Eurozone in crisis: The death of the euro could trigger World War III," 12-9-11, www.periscopepost.com/2011/12/eurozone-in-crisis-the-death-of-the-euro-could-trigger-world-war-iii/, accessed 10-23-12, mss)

Eurozone in crisis: The **death of the euro could trigger** World War III The slow-motion demise of the euro isn’t just financial Armageddon – it could just be one step down the slippery path to World War III. At the risk of being accused of scaremongering, I’ll state my point simply and up front: Things in Europe are not as bad as they seem – they’re worse. And though the commentariat is queuing up to predict the imminent demise of the euro currency and to lament the ongoing recession, that’s not even the half of it: We’re looking at World War III. As major corporations start drawing up contingency plans for a world without the euro and as weaknesses in government finances become ever more glaring, the end of the euro currency becomes an increasingly realistic prospect. Related, the total absence of business growth, or trading among European nations raises the question of what benefits a unified trading block offers. The driving motive behind the original Coal and Steel alliance that ultimately became today’s European Union was a desire among nations, traumatised by the worst war in their collective history, to provide a deterrent against another war. My concern is that that trauma has faded, and that the fear of war has been replaced by the fear of recession. As anyone with even a fleeting familiarity with **European history** can confirm, ours **is not** exactly **a history of** love and **peace**. In fact, the period since the end of World War II has been probably the longest period of relative peace the region has ever known. Arguably, it’s no coincidence that that period of peace has coincided exactly with the ever strengthening ties that have been forged between European nations over these past 60 years. If the bonds that tie European nations together are weakened, the **incentives to avoid** total war **dwindle.** And its not as dramatic or far fetched a theory as it may at first sound. The end of the euro currency and a reversion to national currencies could quite possibly provide the impetus for a further dissolution of the union. The unraveling of painstakingly negotiated ties becomes easier and easier as each strand frays and breaks. Combine this unraveling with an ongoing or even deepening recession, and it all makes for a **combustible atmosphere**. Unfortunately, it is human nature to blame others for our woes. In an environment of unemployment, austerity, and general resentment, it is not difficult to imagine nations starting to point the finger at their neighbours. And **without the unifying effect** of a common currency, thriving trading relations, free movement of peoples, and common interests, **Europe would find itself** increasingly susceptible to war. Moreover, as so few Europeans in my generation, let alone subsequent generations, have even the slightest inkling about how horrific war is, it may be tempting to consider it as a solution to problems, or at minimum an acceptable response to perceived slights.

#### Strong EU key to solve extinction

Bruton, 2 -- former prime minister of Ireland

(John, former ambassador of the EU to the US, European Commission Delegation ambassador, "The Future of the European Union," The Irish Times, 1-31-2002, 195.7.33.33/newspaper/special/2002/europe/index.htm)

As the Laeken Declaration put it, "Europe needs to shoulder its responsibilities in the governance of globalisation" adding that Europe must exercise its power in order "to set globalisation within a moral framework, in other words to anchor it in solidarity and sustainable development". Only a strong European Union is big enough to create a space, and a stable set of rules, within which all Europeans can live securely, move freely, and provide for themselves, for their families and for their old age. Individual states are too small to do that on their own. Only a strong European Union is big enough to deal with the globalised human diseases, such as AIDS and tuberculosis. Only a strong European Union is big enough to deal with globalised criminal conspiracies, like the Mafia, that threaten the security of all Europeans. Only a strong European Union is big enough to deal with globalised environmental threats, such as global warming, which threaten our continent and generations of its future inhabitants. Only a strong European Union is big enough to deal with globalised economic forces, which could spread recession from one country to another and destroy millions of jobs. Only a strong European Union is big enough to regulate, in the interests of society as a whole, the activities of profit seeking private corporations, some of which now have more spending power than many individual states. These tasks are too large for individual states. Only by coming together in the European Union can we ensure that humanity, and the values which make us, as individuals, truly human, prevail over blind global forces that will otherwise **overwhelm us.**

#### Eurozone collapse spurs massive global depression and protectionism

Wright, 12 -- Brookings Managing Global Order fellow

(Thomas, Ph.D. from Georgetown University, former executive director of studies at the Chicago Council on Global Affairs, a lecturer at the Harris School of Public Policy at the University of Chicago, and senior researcher for the Princeton Project on National Security, "What if Europe Fails?" The Washington Quarterly, Summer 2012, 35:3, 23-41, csis.org/files/publication/twq12SummerWright.pdf, accessed 10-21-12, mss)

The most immediate and obvious impact would be on the European and global economy. The two scenarios under consideration are bad, but one is much worse than the other. It is the overwhelming view of senior economists, financial institutions, and international organizations that the disorderly collapse of the Eurozone, resulting in a return to national currencies, has a high probability of causing a new depression **and** ending the period of economic integration which has characterized world politics since the Cold War. For instance, the OECD’s Economic Outlook in November 2011 warned: The establishment and likely large exchange rate changes of the new national currencies could imply large losses for debt and asset holders, including banks that could become insolvent. Such turbulence in Europe, with the massive wealth destruction, bankruptcies and a collapse in confidence in European integration and cooperation, would most likely result in a deep depression in both the exiting and remaining euro area countries as well as in the world economy. 7 In the private sector, Citi’s chief economist William Buiter wrote that disorderly defaults and eurozone exits by the five periphery statesGreece, Ireland, Portugal, Spain, and Italywould drag down not just the European banking system but also the north Atlantic financial system and the internationally exposed parts of the rest of the global banking system. **The resulting financial crisis would trigger a** global depression **that would** last for years**,** with GDP likely falling by more than 10 per cent and unemployment in the West reaching 20 per cent or more. Emerging markets would be dragged down too. 8 Other analysts have reached similar conclusions about the consequences of a Euro break up. HSBC predicted, ‘‘A euro break-up would be a disaster, threatening another Great Depression;’’ UBS estimated that a **breakup would cost each peripheral economy** up to **40 percent of** their **GDP** in year one; ING estimated that the Eurozone as a whole (including Germany) could see a 9 percent drop in the first year following break up, while inflation in the periphery would soar to double digits; IMF chief Christine Lagarde warned that **the global economy faces the prospect of ‘‘**economic retraction, rising **protectionism, isolation and** . . . **what happened in the 30s.**’’ 9 Following a disorderly breakup, it is highly likely that it would be every state for itself as governments sought to do everything possible to insulate their countries against the greatest economic shock in the West since World War II. A return to national currencies would result in tremendous fluctuations, uncertainty, and volatility following redenomination, including a redenomination of complex international contracts. 10 It would also mean that countries with a weak currency would immediately be bankrupt, as their assets would have depreciated while their debts would be denominated in the currency of the creditor state. These states would introduce capital controls to prevent capital flight and the collapse in value of the new currencies. Strong states would introduce tariffs to protect against competitive devaluations and cheap imports. The European single market would not likely survive. Globally, governments would try to save what they could and would likely replicate some of the protectionist measures introduced in Europe. **The** net **effect could** jeopardize global economic integration **and open the door to neo-mercantilism and protectionism**.

#### And economic collapse causes nuclear war

Kemp ’10 [Geoffrey Kemp, Director of Regional Strategic Programs at The Nixon Center, served in the White House under Ronald Reagan, special assistant to the president for national security affairs and senior director for Near East and South Asian affairs on the National Security Council Staff, Former Director, Middle East Arms Control Project at the Carnegie Endowment for International Peace, 2010, “The East Moves West: India, China, and Asia’s Growing Presence in the Middle East”, p. 233-4]

The second scenario, called Mayhem and Chaos, is the opposite of the first scenario; everything that can go wrong does go wrong. The world economic situation weakens rather than strengthens, and India, China, and Japan suffer a major reduction in their growth rates, further weakening the global economy. As a result, energy demand falls and the price of fossil fuels plummets, leading to a financial crisis for the energy-producing states, which are forced to cut back dramatically on expansion programs and social welfare. That in turn leads to political unrest: and nurtures different radical groups, including, but not limited to, Islamic extremists. The internal stability of some countries is challenged, and there are more “failed states.” Most serious is the collapse of the democratic government in Pakistan and its takeover by Muslim extremists, who then take possession of a large number of nuclear weapons. The danger of war between India and Pakistan increases significantly. Iran, always worried about an extremist Pakistan, expands and weaponizes its nuclear program. That further enhances nuclear proliferation in the Middle East, with Saudi Arabia, Turkey, and Egypt joining Israel and Iran as nuclear states. Under these circumstances, the potential for nuclear terrorism increases, and the possibility of a nuclear terrorist attack in either the Western world or in the oil-producing states may lead to a further devastating collapseof the world economic market, with a tsunami-like impact on stability. In this scenario, major disruptions can be expected**,** with dire consequences for two-thirds of the planet’s population.

#### Second is relations-

#### US-EU relations prevent Eurasian global nuclear war

Brzezinski ‘3 (Zbigniew Brzezinski, former national security advisor to the president, “Hegemonic quicksand,” National Interest Winter, 2003)

FOR THE next several decades, the most volatile and dangerous region of the world--with the explosive potential to plunge the world into chaos--will be the crucial swathe of Eurasia between Europe and the Far East. Heavily inhabited by Muslims, we might term this crucial subregion of Eurasia the new "Global Balkans." (1) It is here that America could slide into a collision with the world of Islam while American-European policy differences could even cause the Atlantic Alliance to come unhinged. The two eventualities together could then put the prevailing American global hegemony at risk. At the outset, it is essential to recognize that the ferment within the Muslim world must be viewed primarily in a regional rather than a global perspective, and through a geopolitical rather than a theological prism. The world of Islam is disunited, both politically and religiously. It is politically unstable and militarily weak, and likely to remain so for some time. Hostility toward the United States, while pervasive in some Muslim countries, originates more from specific political grievances--such as Iranian nationalist resentment over the U.S. backing of the Shah, Arab animus stimulated by U.S. support for Israel or Pakistani feelings that the United States has been partial to India-than from a generalized religious bias. The complexity of the challenge America now confronts dwarfs what it faced half a century ago in Western Europe. At that time, Europe's dividing line on the Elbe River was the strategically critical frontline of maximum danger, with the daily possibility that a clash in Berlin could unleash a nuclear war with the Soviet Union. Nevertheless, the United States recognized the stakes involved and committed itself to the defense, pacification, reconstruction and revitalization of a viable European community. In doing so, America gained natural allies with shared values. Following the end of the Cold War, the United States led the transformation of NATO from a defense alliance into an enlarging security alliance--gaining an enthusiastic new ally, Poland--and it has supported the expansion of the European Union (EU). For at least a generation, the major task facing the United States in the effort to promote global security will be the pacification and then the cooperative organization of a region that contains the world's greatest concentration of political injustice, social deprivation, demographic congestion and potential for high-intensity violence. But the region also contains most of the world's oil and natural gas. In 2002, the area designated as the Global Balkans contained 68 percent of the world's proven oil reserves and 41 percent of the world's proven natural gas reserves; it accounted for 32 percent of world oil production and 15 percent of world natural gas production. In 2020, the area is projected to produce roughly 42 million barrels of oil per day--39 percent of the global production total (107.8 million barrels per day). Three key regions-Europe, the United States and the Far East--collectively are projected to consume 60 percent of that global production (16 percent, 25 percent and 19 percent, respectively). The combination of oil and volatility gives the United States no choice. America faces an awesome challenge in helping to sustain some degree of stability among precarious states inhabited by increasingly politically restless, socially aroused and religiously inflamed peoples. It must undertake an even more daunting enterprise than it did in Europe more than half a century ago, given a terrain that is culturally alien, politically turbulent and ethnically complex. In the past, this remote region could have been left to its own devices. Until the middle of the last century, most of it was dominated by imperial and colonial powers. Today, to ignore its problems and underestimate its potential for global disruption would be tantamount to declaring an open season for intensifying regional violence, region-wide contamination by terrorist groups and the competitive proliferation of weaponry of mass destruction. The United States thus faces a task of monumental scope and complexity. There are no self-evident answers to such basic questions as how and with whom America should be engaged in helping to stabilize the area, pacify it and eventually cooperatively organize it. Past remedies tested in Europe--like the Marshall Plan or NATO, both of which exploited an underlying transatlantic political-cultural solidarity--do not quite fit a region still rent by historical hatreds and cultural diversity. Nationalism in the region is still at an earlier and more emotional stage than it was in war-weary Europe (exhausted by two massive European civil wars fought within just three decades), and it is fueled by religious passions reminiscent of Europe's Catholic-Protestant forty-year war of almost four centuries ago. Furthermore, the area contains no natural allies bonded to America by history and culture, such as existed in Europe with Great Britain, France, Germany and, lately, even Poland. In essence, America has to navigate in uncertain and badly charted waters, setting its own course, making differentiated accommodations while not letting any one regional power dictate its direction and priorities. To Whom Can America Turn? TO BE SURE, several states in the area are often mentioned as America's potential key partners in reshaping the Global Balkans: Turkey, Israel, India and--on the region's periphery--Russia. Unfortunately, every one of them suffers serious handicaps in its capability to contribute to regional stability or has goals of its own that collide with America's wider interests in the region. Turkey has been America's ally for half a century. It earned America's trust and gratitude by its direct participation in the Korean War. It has proven to be NATO's solid and reliable southern anchor. With the fall of the Soviet Union, it became active in helping both Georgia and Azerbaijan consolidate their new independence, and it energetically promoted itself as a relevant model of political development and social modernization for those Central Asian states whose people largely fall within the radius of the Turkic cultural and linguistic traditions. In that respect, Turkey's significant strategic role has been complementary to America's policy of reinforcing the new independence of the region's post-Soviet states. Turkey's regional role, however, is limited by two major offsetting considerations stemming from its internal problems. The first pertains to the still uncertain status of Ataturk's legacy: Will Turkey succeed in transforming itself into a secular European state even though its population is overwhelmingly Muslim? That has been its goal since Ataturk set his reforms in motion in the early 1920s. Turkey has made remarkable progress since then, but to this day its future membership in the European Union (which it actively seeks) remains in doubt. If the EU were to close its doors to Turkey, the potential for an Islamic political-religious revival and consequently for Turkey's dramatic (and probably turbulent) international reorientation should not be underestimated. The Europeans have reluctantly favored Turkey's inclusion in the European Union, largely in order to avoid a serious regression in the country's political development. European leaders recognize that the transformation of Turkey from a state guided by Ataturk's vision of a European-type society into an increasingly theocratic Islamic one would adversely affect Europe's security. That consideration, however, is contested by the view, shared by many Europeans, that the construction of Europe should be based on its common Christian heritage. It is likely, therefore, that the European Union will delay for as long as it can a clear-cut commitment to open its doors to Turkey--but that prospect in turn will breed Turkish resentments, increasing the risks that Turkey might evolve into a resentful Islamic state, with potentially dire consequences for southeastern Europe. (2) The other major liability limiting Turkey's role is the Kurdistan issue. A significant proportion of Turkey's population of 70 million is composed of Kurds. The actual number is contested, as is the nature of the Turkish Kurds' national identity. The official Turkish view is that the Kurds in Turkey number no more than 10 million, and that they are essentially Turks. Kurdish nationalists claim a population of 20 million, which they say aspires to live in an independent Kurdistan that would unite all the Kurds (claimed to number 25-35 million) currently living under Turkish, Syrian, Iraqi and Iranian domination. Whatever the actual facts, the Kurdish ethnic problem and the potential Islamic religious issue tend to make Turkey-- notwithstanding its constructive role as a regional model--also very much a part of the region's basic dilemmas. Israel is another seemingly obvious candidate for the status of a pre-eminent regional ally. As a democracy as well as a cultural kin, it enjoys America's automatic affinity, not to mention intense political and financial support from the Jewish community in America. Initially a haven for the victims of the Holocaust, it enjoys American sympathy. As the object of Arab hostility, it triggered American preference for the underdog. It has been America's favorite client state since approximately the mid-1960s and has been the recipient of unprecedented American financial assistance ($80 billion since 1974). It has benefited from almost solitary American protection against UN disapprobation or sanctions. As the dominant military power in the Middle East, Israel has the potential, in the event of a major regional crisis, not only to be America's military base but also to make a significant contribution to any required U.S. military engagement. Yet American and Israeli interests in the region are not entirely congruent. America has major strategic and economic interests in the Middle East that are dictated by the region's vast energy supplies. Not only does America benefit economically from the relatively low costs of Middle Eastern oil, but America's security role in the region gives it indirect but politically critical leverage on the European and Asian economies that are also dependent on energy exports from the region. Hence good relations with Saudi Arabia and the United Arab Emirates--and their continued security reliance on America--is in the U.S. national interest. From Israel's standpoint, however, the resulting American-Arab ties are disadvantageous: they not only limit the degree to which the United States is prepared to back Israel's territorial aspirations, they also stimulate American sensitivity to Arab grievances against Israel. Among those grievances, the Palestinian issue is foremost. That the final status of the Palestinian people remains unresolved more than 35 years after Israel occupied the Gaza Strip and the West Bank--irrespective of whose fault that actually may be--intensifies and, in Arab eyes, legitimates the widespread Muslim hostility toward Israel. (3) It also perpetuates in the Arab mind the notion that Israel is an alien and temporary colonial imposition on the region. To the extent that the Arabs perceive America as sponsoring Israeli repression of the Palestinians, America's ability to pacify anti-American passions in the region is constrained. That impedes any joint and constructive American-Israeli initiative to promote multilateral political or economic cooperation in the region, and it limits any significant U.S. regional reliance on Israel's military potential. Since September 11, the notion of India as America's strategic regional partner has come to the forefront. India's credentials seem at least as credible as Turkey's or Israel's. Its sheer size and power make it regionally influential, while its democratic credentials make it ideologically attractive. It has managed to preserve its democracy since its inception as an independent state more than half a century ago. It has done so despite widespread poverty and social inequality, and despite considerable ethnic and religious diversity in a predominantly Hindu but formally secular state. India's prolonged conflict with its Islamic neighbor, Pakistan, involving violent confrontations with guerrillas and terrorist actions in Kashmir by Muslim extremists benefiting from Pakistan's benevolence, made India particularly eager to declare itself after September 11 as co-engaged with the United States in the war on terrorism. Nonetheless, any U.S.-Indian alliance in the region is likely to be limited in scope. Two major obstacles stand in the way. The first pertains to India's religious, ethnic and linguistic mosaic. Although India has striven to make its 1 billion culturally diverse people into a unified nation, it remains basically a Hindu state semi-encircled by Muslim neighbors while containing within its borders a large and potentially alienated Muslim minority of somewhere between 120-140 million. Here, religion and nationalism could inflame each other on a grand scale. So far, India has been remarkably successful in maintaining a common state structure and a democratic system--but much of its population has been essentially politically passive and (especially in the rural areas) illiterate. The risk is that a progressive rise in political consciousness and activism could be expressed through intensified ethnic and religious collisions. The recent rise in the political consciousness of both India's Hindu majority and its Muslim minority could jeopardize India's communal coexistence. Internal strains and frictions could become particularly difficult to contain if the war on terrorism were defined as primarily a struggle against Islam, which is how the more radical of the Hindu politicians tend to present it. Secondly, India's external concerns are focused on its neighbors, Pakistan and China. The former is seen not only as the main source of the continued conflict in Kashmir but ultimately--with Pakistan's national identity rooted in religious affirmation--as the very negation of India's self-definition. Pakistan's close ties to China intensify this sense of threat, given that India and China are unavoidable rivals for geopolitical primacy in Asia. Indian sensitivities are still rankled by the military defeat inflicted upon it by China in 1962, in the short but intense border clash that left China in possession of the disputed Aksai Chin territory. The United States cannot back India against either Pakistan or China without paying a prohibitive strategic price elsewhere: in Afghanistan if it were to opt against Pakistan, and in the Far East if it allied itself against China. These internal as well as external factors constrain the degree to which the United States can rely on India as an ally in any longer-term effort to foster--let alone impose--greater stability in the Global Balkans. Finally, there is the question of the degree to which Russia can become America's major strategic partner in coping with Eurasian regional turmoil. Russia clearly has the means and experience to be of help in such an effort. Although Russia, unlike the other contenders, is no longer truly part of the region--Russian colonial domination of Central Asia being a thing of the past--Moscow nevertheless exercises considerable influence on all of the countries to its immediate south, has close ties to India and Iran and contains some 15-20 million Muslims within its own territory. At the same time, Russia has come to see its Muslim neighbors as the source of a potentially explosive political and demographic threat, and the Russian political elite are increasingly susceptible to anti-Islamic religious and racist appeals. In these circumstances, the Kremlin eagerly seized upon the events of September 11 as an opportunity to engage America against Islam in the name of the "war on terrorism." Yet, as a potential partner, Russia is also handicapped by its past, even its very recent past. Afghanistan was devastated by a decade-long war waged by Russia, Chechnya is on the brink of genocidal extinction, and the newly independent Central Asian states increasingly define their modern history as a struggle for emancipation from Russian colonialism. With such historical resentments still vibrant in the region, and with increasingly frequent signals that Russia's current priority is to link itself with the West, Russia is being perceived in the region more and more as a former European colonial power and less and less as a Eurasian kin. Russia's present inability to offer much in the way of a social example also limits its role in any American-led international partnership for the purpose of stabilizing, developing and eventually democratizing the region. Ultimately, America can look to only one genuine partner in coping with the Global Balkans: Europe. Although it will need the help of leading East Asian states like Japan and China--and Japan will provide some, though limited, material assistance and some peacekeeping forces--neither is likely at this stage to become heavily engaged. Only Europe, increasingly organized as the European Union and militarily integrated through NATO, has the potential capability in the political, military and economic realms to pursue jointly with America the task of engaging the various Eurasian peoples--on a differentiated and flexible basis--in the promotion of regional stability and of progressively widening trans-Eurasian cooperation. And a supranational European Union linked to America would be less suspect in the region as a returning colonialist bent on consolidating or regaining its special economic interests.

#### Strong alliance key to global war

O'Sullivan, 4 -- National Interest editor

(John, Nixon Center for Peace and Freedom Distinguished Fellow in International Relations, "Europe and the Establishment," The National Interest, 7-31-2004, nationalinterest.org/article/europe-and-the-establishment-2608]

The report's starting point -- that U.S.-European relations are extremely important -- is undeniable. A united Western alliance would shape world institutions in line with values and practices rooted in liberty and democracy and coax rising powers such as India and China into going along with this international status quo for the foreseeable future. Indeed, this is already happening as China accepts liberal economic rules at home in order to enter institutions such as the G7 and the World Trade Organization. By contrast, a disunited West would tempt such powers to play off Europe and America against each other and foster a global jockeying for power not unlike the maneuvering between a half-dozen great powers that led to 1914.

#### Relations key to effective EU Navy- solves laundry list of hotspot escalation

Seidler ’14 ( Journalist for the Institute for Security Studies Kiel, Member of the German Council on Foreign Relations , the German Atlantic Association , Berlin Working Group Security Policy and the Center for International Maritime Security, “What Should be in EU's New Maritime Security Strategy”, <http://www.seidlers-sicherheitspolitik.net/2014/01/emss.html>, January 7, 2014)

What Should be in EU's New Maritime Security Strategy Maritime great power politics is back and here to stay. Hence, EU needs to adapt and rediscover geopolitics. Although hard power matters most, Europe's naval decline is likely to continue: Less money, less navies. To be nevertheless a serious player, EU has to adapt a smart power approach. Most important is that EU says what it does and does what it says. Time to leave strategic no man's land The European Council's December session on security policy offers only one remarkable result: In June 2014, EU will endorse a new Maritime Security Strategy (EMSS). After years of economic crisis, geopolitical decline and military constraints, an EMSS could give EU a new push to adapt to the evolving security environment. Such a push is more than necessary. Ten years after the European Security Strategy (ESS), Europe drifted from large ambitious into the strategic no man's land: Soft power becomes more and more irrelevant, harsh great power competitions and geopolitics are back on the stage - just look at the Middle East and East Asia. In consequence, neither is anybody talking about a more secure Europe nor about EU building a better world. However, in the maritime domain Europe could come back on track. Therefore, EMSS must address three key points. First, it has to define Europe's strategic-maritime aims and set out the means to implement them. Second, due to the capabilities, there has to be a clear work-sharing with NATO, because the Alliance is much stronger in maritime security than EU. Third, EMSS must outline how EU wants to adapt to a geopolitical/-strategic environment that will not only develop to Europe's disadvantage, but also to the advantage of other powers. In the EMSS' development, there is no need for a long debate about security challenges, risks and threats, because the problems are well known: Terrorism, piracy, proliferation, organized crime, energy security, choke points, critical infrastructure, disaster relief and so forth. Not war-fighting or deterrence, but rather MOOTW are likely to dominate the operational agenda. What changed, in contrast to ESS 2003, are not the security challenges, risks and threats, but rather the players and theaters. Relevant heaters: Arctic, Med', Indo-Pacific Source: EUISS Report No. 16, p. 17 As the EMSS is about "security", the Baltic and the North Sea do not matter (when Russia tries to provoke, so what?). These are NATO/EU inland-seas and, therefore, only subject to regular politics and not to military considerations. What should concern Europe, are the Arctic, the Indo-Pacific and primarily the Mediterranean (Med'). The Gulf of Guinea is an area of operational, but not of strategic concern. Present piracy can be tackled by regional actors with international support. The Arctic's emerging geopolitical relevance is stressed by the relatively high number of applicants for observer status in the Arctic Council. In May 2013, EU suffered a serious defeat, as Brussels' application was rejected, while China, India, Italy, Japan, South Korea and even Singapore became observers. For EMSS it has therefore to be said, that there is no military role for EU in the High North. Sweden and Finland are Arctic Council members, but without direct access to the Arctic waters. What matters for EU are trade routes and resources. Thus, an EMSS should define how EU can contribute to safe and secure Arctic shipping lanes and how Europe's resource interests can be preserved. After the rejection, however, it is clear that EU will not be one of the major players in the High North. Instead, other theaters should receive more attention. Indian Navy show its two carriers (Source: WiB) The Indo-Pacific should be of great concern for EU. Due to China's and India's naval rise along with the growing seaborne trade, Indian and Pacific Ocean have to be seen as one theater. Moreover, there is an Emerging Asian Power Web made by bi-, tri- and multilateral maritime security partnerships among Indo-Pacific states. EU's interests in Indo-Pacific security are primarily motivated by economics. In 2012, the total value of goods shipped from Europe to Asia was 816 billion Euros. While EU can and should play a role in the Indian Ocean, the Union will hardly become relevant East of Malacca Strait. EU has been rejected three times as an observer at the East Asia Summit. Thus, an EMSS has to put a strong emphasis on the Indian Ocean and the Persian Gulf, but it also has to accept that EU will remain irrelevant between Singapore and Vladivostok. Only France and Britain could make themselves relevant in maritime East Asia. However, while budgetary under constraints, they will only choose to go there in case of a major incident. During its disaster relief operation on the Philippines, the Royal Navy demonstrated that the UK is still capable of acting East of Malacca. However, the British posture also showed the Royal Navy's limits. Moreover, it can be ruled out that Paris and London develop some kind of EU maritime security altruism and make an expeditionary EU presence a national priority. Instead, both will allocate their expensive warships to operations concerning their national interests, but not to EU (or NATO and UN) tasks. Hence, EMSS has to outline what European states want to do together in the Indo-Pacific and what not. It does not make any sense to write high expeditionary ambitions into a strategy, when it is clear from the beginning that those who have the means for implementing have no interest in doing so. Less can be more. This means the EMSS should contain realistic and credible ambitions in the Indo-Pacific, making the EU an actor who says what it does, and does what it says. Otherwise, EU is doomed to irrelevance East of Suez. In addition, EU has to withstand the seduction of a new free-riding with maritime stability and security provided by Asian powers. There is no guarantee that those powers will remain friendly to European interests. Most important for EU is the Med'. Not only by the refugee issue, but also by the new great power plays in the Eastern Med'. Russia has returned as a serious naval actor with its largest expeditionary operation since 1991. New conflicts about offshore gas will emerge. Moreover, the growing instability in North Africa from Tunisia to the Suez-Canal calls for EU action. Therefore, Brussels' main challenge will be to define in the EMSS, how EU wants to cooperate further will its Med' partners. In addition, EMSS has to say how EU aims to contribute from the maritime domain to stability ashore. Although terrorism, proliferation, human trafficking, illegal migration and organized crime are subject to EU's maritime agenda, the solutions are to be found on land, not on the waters. Dealing with new maritime powers After the USSR's collapse, only the United States and EU countries, in particular Britain and France, possessed the monopoly on long-range power projection. Until present, there is no other country, which is be able to go for Falklands-War-Style missions. This is going to change. While France and Britain are struggling to keep their capabilities alive, especially China, Russia and India are preparing themselves for expeditionary missions. In 2013, we have seen Russia's largest expeditionary deployment in the Med' since 1991. In terms of expeditionary power projection, Australia, Brazil, Japan and South Korea could become more capable players, if their governments decide to pursue that track. Rather than focusing on security challenges, EMSS has to address how Europe wants to deal with emerging naval powers. Of course, cooperation for promoting common interests, like safe and secure sea-lanes or mutual trust-building, should be a top priority. However, Brussels tends to see the world too much through pink glasses, where the world becomes good by itself as long as there are talks about multilateralism and global governance. Instead, the maritime environment can remain friendly to EU interest, but due to great power politics this cannot be taken for granted. Therefore, EMSS has to address how EU will react (it will not take the initiative) in case of fundamental state-driven changes to a maritime environment, which is hostile to European interests. Thus, advancing partnerships with like-minded democracies like India, Japan, Australia and South Korea has to be an EMSS priority. Potential partners are also Singapore, Indonesia and New Zealand. Cooperation with China is likely to become much more difficult, because recent Chinese actions (ADIZ) showed that Beijing's approach continues to become much more assertive. EU's aims Defining realistic and achievable aims for EU is that simple: Stability, security, safety and prosperity. Stability is the most important of all aims. It enables the flow of trade and the opportunities of doing non-hard power related politics. However, stability requires security and safety. Those three lead to the fourth aim: Prosperity by the maritime domain as an area, which provides trade lanes and resources. For EU, it does not matter who owns what. However, Europe's interest is the absence of conflict. Hence, an EMSS has to outline an increased portfolio of cooperation and trust-building programs. Defining Europe's means Europe's soft- and hard-power continue to suffer seriously from the monetary and economic crisis. To be effective and efficient, EU has to follow an approach of smart power. The latter means the combination of civilian and military means. However, as navies are costly, EU's focus should generally be on civilian capabilities, where necessary accompanied by military assets. In case of hard power, there will be no European comeback. Recent celebrations about countries leaving the rescue mechanisms ignore, that ESM and EFSF became irrelevant, because there is a new unofficial rescue mechanism called ECB (which does not include any submission to Troika obligations). The crisis has been managed, but it has not been solved. As the debt track is not left, Europe's armed forces will face further cuts. However, naval hard power matters most, because that is what you need to pursue your interests on the high seas. There is no soft power equivalent. Hence, it is important for Europe that the Royal Navy commissions both new carriers and that France, Italy and Spain preserve their flattops. Moreover, with an eye on Med' and Indo-Pacific theaters, LHD and LPD will be needed for MOOTW. Of course, this requires a balanced fleet with destroyers, frigates and submarines. For long-range power projection, the British and French SSN remain very relevant. Moreover, although extremely unpopular, Europe has to maintain a credible sea-based nuclear deterrent. That is also, why Britain should throw all alternatives in the bin and build four new SSBN. For implementing maritime smart power, coast guard vessels and patrol aircraft are needed, along with partnership teams on land. Especially in the Med', police enforcement capabilities are necessary. Challenges like migration and organized crime are not military issues. Moreover, research ships and new policies for fishing and energy are of great concern. NATO vs. EU? How to deal with the US? Much has been said here about emerging naval powers, while the world's largest seapower - still the US - has not been discussed, yet. Whatever happens, America will remain Europe's most important naval partner, based on common interests and capabilities. That is why NATO has a great maritime relevance, because it links the US Navy to Europe. As the EU does not have any naval links with US yet, EMSS has to clarify the relationship between EU, NATO and the US. What we do not need is a beauty contest, but what we do need is a clearly defined and coordinated work-sharing. Standing NATO Maritime Group 1 (Source) There was never a real reason why both, NATO and EU, had to have maritime operations in the Gulf of Aden. Both organizations wanted to be part of the international maritime beauty contest. In the future, however, Europe cannot afford two organizations doing the same. Therefore, the work-sharing between EU and NATO should look like this: While EU is good at civilian missions and smart power, NATO has decades-old naval hard power experience. Hence, the modus vivendi should be that EU is doing the softer and civilian tasks, while NATO does the hard power jobs; Europe becomes less capable in hard power anyway and only NATO provides access to the needed US assets (and maybe British assets, too, if the UK leaves EU). Moreover, it could be elaborated, if EU could get access to NATO's Standing Maritime Groups. However, NATO's real maritime worth is that the alliance links Britain, Canada, Turkey and Norway to European security. The UK is drifting apart from EU, but the Royal Navy will remain the most capable of all European navies. Turkey in the Med', Canada and Norway in Arctic are indispensable partners. All four countries continue to in their naval capabilities. In the US, NATO and EU triangle, EMSS has to address who does what and where. While US will carry most of the maritime burdens in the Indo-Pacific, also relying on coalitions of the willing, NATO's concern should be hard power missions in the Med' and Indian Ocean. In such a work-sharing, EU's job would be to tackle the civilian and softer issues in the Med' and the Indian Ocean; maybe in the South Atlantic, too. Dealing with decline Chinese frigate Yangcheng in Limassol, Cyprus (Source) To secure the destruction of Syria's chemical weapons, China's navy is now operating from Cyprus, an EU member state, in the Eastern Med'. Yes, it is only access to a port for supplies and it is only on a tactical level. Nevertheless, it is remarkable, while EU is not taken serious in Asia, China shows the flag in European homewaters. Never before has Non-Western power operated from an EU member state. In addition, in 2012, Japan's premier minister Shinzo Abe invited Britain and France to come back to the Asian maritime security theater. Nine years after the ESS' endorsement, it was quite humiliating for EU that not the Union herself, but rather two nation states have been addressed in such a way. Obviously, EU was not taken for serious in terms of hard power. Five megatrends will define the decades to come: (1) digitalization; (2) competition for resources; (3) demographic changes; (4) economic globalization; (5) economic power shifts. Due Europe's economic and demographic problems, European (maritime) decline is real and it is likely to remain so. Until 2030, competition for resources and economic growth will have increased the global sea-lanes' importance, foremost in the Indo-Pacific. Emerging relevance of navies will go along with that. Moreover, 2030 is a point of time, where China, India and Russia (and maybe others) will operate navies capable of medium and long-range power projection. China then could posses the capabilities to fight (and win) Falklands-Style-Wars. Economically, China will have surpassed the US the world's largest economy and European economies will have dropped back in the global economic hierarchy. The consequence will be that Europe will not able anymore to conduct operations like Libya 2011. Moreover, European power projection will be balanced by the emerging naval power of others. Thus, it essential that EU enhances its partnerships with the US and NATO and, moreover, creates new partnerships with like-minded democracies, in particular India. Digitalization and robotics will lead to the fact that coming generations of naval systems can do even more than today, however, will be even more complex and therefore more expensive in procurement and maintenance. Europe's budgetary situation will make the joint development, procurement and operation of new naval system a necessity. If this does not happen, Europe will simple disappear from the maritime domain as a serious, capable actor. In addition, it is likely that emerging navies, in particular China, will have the financial means to effort new high-end warfare assets, which will negatively affect Europe's power. With France on the march into an even worse economic mess, EU's maritime power projection will largely depend on Britain - though the UK remains an EU member. Britain's coming carriers and other high-end warfare capabilties (SSN, SSBN, Type 26 frigates) will be critical for Europe to be capable and taken serious in international maritime power politics. In this regard, the worst that could happen is that London decides to sell the second carrier to an emerging navy (e.g. Brazil). For the maritime balance of power, the second carrier must remain British (or European in some way) or, if it is sold, it has to be given to a like-minded country (e.g. Japan or Australia). After 2030, China likely and India maybe could reach the naval power status of the Soviet Union in the 1980s. This means the capability of global power projection and the ability to conduct at least one high-intensity operation. We will see scenarios where emerging navies conduct expeditionary power projection operations, while Europe will be incapable of doing anything, though there is no reversal of current trends. EU as a capable global, geostrategic and maritime security player is hardly imaginable for the decades to come. Hence, even not a popular idea, Europeans will have to re-discover the transatlantic partnership and NATO - a maritime alliance by nature. No matter how far Asian navies rise, the US Navy will remain the most capable of all and it will further dominate, although more and more challenged, the international maritime order. Europe in decline is well advised to seek close cooperation with the US, because America is likely to recover through the Shale Gas boom. What to do? For EMSS' implementation, preserving and renewing capabilities is essential. Countries like Germany, Denmark, the Netherlands and Poland in the North and Portugal, Spain and Italy in the South have to elaborate new mechanisms to integrate their navies. Jointly operated LPDs or submarines could be a start. Joint task groups out of coast guards, police services, technical and environmental experts (and others) are a necessity. Whatever is agreed in EMSS: As much as decisions matter, it matters that words are followed by actions. In a time of new maritime great power politics, Europe must say what it does and do what it says. Otherwise, EU will not be taken serious and the EMSS can just be dumped in the bin.

#### Relations key to solve the environment

Vig and Faure ‘4 (Norman J. Vig and Michael G. Faure, professor of science, technology and society at Carleton College, Minnesota and professor of comparative and international environmental law at Maastricht U, the Netherlands, Green Giants? Environmental Policies of the United States and the European Union, 2004)

This book stems from our concern that the US and the EU—representing the world’s two largest and most developed economic markets— seem increasingly incapable of resolving differences over the priority of environmental problems and methods of addressing them, thus preventing them from taking the kind of joint leadership role that will be necessary to halt environmental degradation on a global scale. The US and EU together account for at least half of the world’s gross domestic product and consume a disproportionate share of the world’s resources. They also generate about 40 percent of global greenhouse gas emissions and most of the planet’s toxic waste. At the same time, they are the source of much of the world’s advanced technology needed to reduce pollution and provide alternative sources of energy in the future. Without their support, it is unlikely that the 170 other nations of the world will be willing or able to pursue sustainable development policies in the future.

#### Ecosystem collapse risks extinction

Coyne and Hoekstra ‘7 (Jerry and Hopi, \*professor in the Department of Ecology and Evolution at the University of Chicago AND Associate Professor in the Department of Organismic and Evolutionary Biology at Harvard University, New Republic, “The Greatest Dying,” 9/24, <http://www.truthout.org/article/jerry-coyne-and-hopi-e-hoekstra-the-greatest-dying>, September 24, 2007)

But it isn't just the destruction of the rainforests that should trouble us. Healthy ecosystems the world over provide hidden services like waste disposal, nutrient cycling, soil formation, water purification, and oxygen production. Such services are best rendered by ecosystems that are diverse. Yet, through both intention and accident, humans have introduced exotic species that turn biodiversity into monoculture. Fast-growing zebra mussels, for example, have outcompeted more than 15 species of native mussels in North America's Great Lakes and have damaged harbors and water-treatment plants. Native prairies are becoming dominated by single species (often genetically homogenous) of corn or wheat. Thanks to these developments, soils will erode and become unproductive - which, along with temperature change, will diminish agricultural yields. Meanwhile, with increased pollution and runoff, as well as reduced forest cover, ecosystems will no longer be able to purify water; and a shortage of clean water spells disaster. In many ways, oceans are the most vulnerable areas of all. As overfishing eliminates major predators, while polluted and warming waters kill off phytoplankton, the intricate aquatic food web could collapse from both sides. Fish, on which so many humans depend, will be a fond memory. As phytoplankton vanish, so does the ability of the oceans to absorb carbon dioxide and produce oxygen. (Half of the oxygen we breathe is made by phytoplankton, with the rest coming from land plants.) Species extinction is also imperiling coral reefs - a major problem since these reefs have far more than recreational value: They provide tremendous amounts of food for human populations and buffer coastlines against erosion. In fact, the global value of "hidden" services provided by ecosystems - those services, like waste disposal, that aren't bought and sold in the marketplace - has been estimated to be as much as $50 trillion per year, roughly equal to the gross domestic product of all countries combined. And that doesn't include tangible goods like fish and timber. Life as we know it would be impossible if ecosystems collapsed. Yet that is where we're heading if species extinction continues at its current pace. Extinction also has a huge impact on medicine. Who really cares if, say, a worm in the remote swamps of French Guiana goes extinct? Well, those who suffer from cardiovascular disease. The recent discovery of a rare South American leech has led to the isolation of a powerful enzyme that, unlike other anticoagulants, not only prevents blood from clotting but also dissolves existing clots. And it's not just this one species of worm: Its wriggly relatives have evolved other biomedically valuable proteins, including antistatin (a potential anticancer agent), decorsin and ornatin (platelet aggregation inhibitors), and hirudin (another anticoagulant). Plants, too, are pharmaceutical gold mines. The bark of trees, for example, has given us quinine (the first cure for malaria), taxol (a drug highly effective against ovarian and breast cancer), and aspirin. More than a quarter of the medicines on our pharmacy shelves were originally derived from plants. The sap of the Madagascar periwinkle contains more than 70 useful alkaloids, including vincristine, a powerful anticancer drug that saved the life of one of our friends. Of the roughly 250,000 plant species on Earth, fewer than 5 percent have been screened for pharmaceutical properties. Who knows what life-saving drugs remain to be discovered? Given current extinction rates, it's estimated that we're losing one valuable drug every two years. Our arguments so far have tacitly assumed that species are worth saving only in proportion to their economic value and their effects on our quality of life, an attitude that is strongly ingrained, especially in Americans. That is why conservationists always base their case on an economic calculus. But we biologists know in our hearts that there are deeper and equally compelling reasons to worry about the loss of biodiversity: namely, simple morality and intellectual values that transcend pecuniary interests. What, for example, gives us the right to destroy other creatures? And what could be more thrilling than looking around us, seeing that we are surrounded by our evolutionary cousins, and realizing that we all got here by the same simple process of natural selection? To biologists, and potentially everyone else, apprehending the genetic kinship and common origin of all species is a spiritual experience - not necessarily religious, but spiritual nonetheless, for it stirs the soul. But, whether or not one is moved by such concerns, it is certain that our future is bleak if we do nothing to stem this sixth extinction. We are creating a world in which exotic diseases flourish but natural medicinal cures are lost; a world in which carbon waste accumulates while food sources dwindle; a world of sweltering heat, failing crops, and impure water. In the end, we must accept the possibility that we ourselves are not immune to extinction. Or, if we survive, perhaps only a few of us will remain, scratching out a grubby existence on a devastated planet. Global warming will seem like a secondary problem when humanity finally faces the consequences of what we have done to nature: not just another Great Dying, but perhaps the greatest dying of them all.

## 2AC

### Circumvention

#### Obama will follow through- aligns himself with Congress

Bellinger ’13 (John B. Bellinger III, Adjunct Senior Fellow for International and National Security Law, “Seeking Daylight on U.S. Drone Policy”, <http://www.cfr.org/drones/seeking-daylight-us-drone-policy/p30348>, March 29, 2013)

The president also has additional constitutional authority anytime to use force to protect the Unites States, either in self-defense or because he believes that it's in our national security interest. So if President Obama concludes that it's necessary to carry out a drone strike against a terror suspect, but that individual does not fall into the categories covered by the AUMF, he would have additional constitutional authority. But this administration has taken great pains to emphasize that it has been relying on congressional grant of authority rather than the president's own constitutional authority to conduct most of its counterterrorism operations. It has wanted to do that to contrast itself with the Bush administration, which had, at least early in its tenure, relied heavily on the president's constitutional authority. It's not clear though, at this point, given how old and somewhat limited the AUMF is, if the Obama administration has now been forced to rely on constitutional powers for certain drone strikes. It appears to many observers that the administration may be stretching the limits of the AUMF by targeting people who were not responsible for 9/11 or who were not affiliated or associated co-belligerents with those who carried out 9/11. In theory, could the president always claim constitutional authority with regard to these strikes? Although, as you pointed out, the administration is obviously loath to do that. This administration is already finding that 95 percent of its counterterrorism policies, and the legal basis therefore, are the same as the Bush administration's. Absolutely. I think the issue is, in this administration, political. This administration is already finding that 95 percent of its counterterrorism policies, and the legal basis therefore, are the same as the Bush administration's. It came into office with both domestic and international supporters expecting that it would change all of those policies. So one area where it really has been loath to act like the Bush administration is to rely heavily on the president's constitutional authority. We simply don't know whether they are doing it, but politically I'm sure that administration officials would be very reluctant to have to acknowledge that they are acting outside of the grant given to them by Congress.

#### Obama doesn’t act alone- Syria proves

Wehner ’13 (Peter Wehner, Peter Wehner is a senior fellow at the Ethics and Public Policy Center. Previously he worked in the administrations of Ronald Reagan, George H.W. Bush, and George W. Bush. In the last of which, he served as deputy assistant to the president, “Barack Obama’s Staggering Incompetence”, <http://www.commentarymagazine.com/2013/09/02/barack-obamas-staggering-incompetence/>, September 2, 2013)

It’s reported that President Obama was ready to order a military strike against Syria, with or without Congress’s blessing, but “on Friday night, he suddenly changed his mind.” According to the Huffington Post: Senior administration officials describing Obama’s about-face Saturday offered a portrait of a president who began to wrestle with his own decision – at first internally, then confiding his views to his chief of staff, and finally summoning his aides for an evening session in the Oval Office to say he’d had a change of heart. In light of all this, it’s worth posing a few questions: 1. Why didn’t the president seek congressional authority before the administration began to beat the war drums this past week? Did the idea not occur to him? It’s not as if this is an obscure issue. When you’re in the White House and preparing to launch military force against a sovereign nation, whether or not to seek the approval of Congress is usually somewhere near the top of the to-do list. And why has the urgency to act that we saw from the administration during the last week–when Assad’s use of chemical weapons was referred to by the secretary of state as a “moral obscenity”–given way to an air of casualness, with Obama not even calling Congress back into session to debate his military strike against Syria? 2. The president didn’t seek congressional approval for his military strike in Libya. Why does he believe he needs it in Syria? 3. Mr. Obama, in his Rose Garden statement on Saturday, still insisted he has the authority to strike Syria without congressional approval. So what happens if Congress votes down a use-of-force resolution? Does the president strike Syria anyway? If so, will it be an evanescent bombing, intended to be limited in scope and duration, while doing nothing to change the war’s balance of power? Or does the president completely back down? Does he even know? Has he thought through in advance anything related to Syria? Or is this a case of Obama simply making it up as he goes along? This latest volte-face by the president is evidence of a man who is completely overmatched by events, weak and confused, and deeply ambivalent about using force. Yet he’s also desperate to get out of the corner he painted himself into by declaring that the use of chemical weapons by the Assad regime would constitute a “red line.” As a result he’s gone all Hamlet on us. Not surprisingly, Obama’s actions are being mocked by America’s enemies and sowing doubt among our allies. (Read this New York Times story for more.) What explains this debacle? It’s impossible for us to know all the reasons, but one explanation appears to be a CYA operation. According to Politico, “At the very least, Obama clearly wants lawmakers to co-own a decision that he can’t back away from after having declared last year that Assad would cross a ‘red line’ if he used chemical weapons against his own people.” And the Washington Post reports: Obama’s proposal to invite Congress dominated the Friday discussion in the Oval Office. He had consulted almost no one about his idea. In the end, the president made clear he wanted Congress to share in the responsibility for what happens in Syria. As one aide put it, “We don’t want them to have their cake and eat it, too.” Get it? The president of the United States is preparing in advance to shift the blame if his strike on Syria proves to be unpopular and ineffective. He’s furious about the box he’s placed himself in, he hates the ridicule he’s (rightly) incurring, but he doesn’t see any way out. What he does see is a political (and geopolitical) disaster in the making. And so what is emerging is what comes most naturally to Mr. Obama: Blame shifting and blame sharing. Remember: the president doesn’t believe he needs congressional authorization to act. He’s ignored it before. He wants it now. For reasons of political survival. To put it another way: He wants the fingerprints of others on the failure in Syria. Rarely has an American president joined so much cynicism with so much ineptitude.

### 2AC- Topicality

#### Splitting NSA and US Cyber is a restriction on war powers independently-

#### We meet- plan ends OCO’s performed by NSA

#### NSA performing Offensive Cyber Operations

McKalin ’13 (Vamien McKalin, Journalist for dotTech an online tech news agency, “New leaked documents show NSA’s cyber offensive against Russia, Iran, China, and North Korea”, <http://dottech.org/124872/new-leaked-documents-show-nsas-cyber-offensive-russia-iran-china-north-korea/>, September 1, 2013)

In 2011, the U.S. National Security Agency (NSA) carried out 231 offensive cyber operations using a computer program called GENIE. According to a leaked document revealed by the Washington Post, the NSA — and other agencies — use this program to plant covert implants into tens of thousands of machines every year. These implants then give these agencies some sort of access to the devices in question. What’s interesting is that the top priority targets for GENIE are in no other than North Korea, China, Iran, and Russia. Furthermore, the documents claim America sends agents out into the field to modify hardware and software at undisclosed locations. However, we understand the most common situation is to use a custom software gears composed by the NSA’s Tailored Access Operations (TAO). TAO has the ability to gain access to any kind of switches, firewalls, and routers anywhere in the world. In addition, TAO is resistive to any form of software update or upgrades, which should give you an idea of how powerful this GENIE program is. The documents went on to further reveal how TAO will soon have the ability to identify voice communications and secretly send out information whenever it sees fit. Washington Post claims the GENIE program aims to control over 85,000 secret implants by the end of 2013 — that’s up from 21,252 in 2008. Just recently, the NSA proposed a $52.6 billion budget, and we’re certain a large portion will go directly into funding the GENIE program. Seeing the likes of Russia, China, Iran, and North Korea on the list of high level targets, it would be very interesting to see how those countries react. The American government must quickly realize it is walking on a thin line here… especially seeing as the US is quick to point the finger at China for any and all cyber attacks.

#### Splitting head of command ends NSA offensive attacks

Masnick ’13 (Mike Masnick, Mike is the founder and CEO of Floor64 and editor of the Techdirt blog, “NSA Claims It Doesn't Do Online Attacks; That's A Different Organization... Run By The NSA”, <http://www.techdirt.com/articles/20131012/01195424849/nsa-claims-it-doesnt-do-online-attacks-thats-different-organization-run-nsa.shtml>, October 14, 2013)

There are times you just shake your head and wonder who the NSA top officials think they're kidding with their statements. Take, for example, some recent comments from the NSA's number two guy in charge, Chris Inglis, the Deputy Director, who gave an interview to the BBC where he tried to paint the NSA as not being quite as bad as everyone says, but admitted that there could be more transparency. That's all the usual stuff, but the following tidbit caught my eye: The job of the NSA, Mr Inglis said, was to exploit networks to collect intelligence in cyberspace and to defend certain networks - but not carry out destructive acts. "NSA had a responsibility from way back, from our earliest days, to both break codes and make codes," he said. "We have a responsibility to do intelligence in a space we once called the telecommunications arena - now cyberspace - and the responsibility to make codes or to defend signals communications of interest. "That's different than what most people conceive as offence or attack in this space." That task of destructive cyber attack, if ordered, lies with the US military's rapidly expanding Cyber Command. Except, as we've noted more than a few times, US Cyber Command is the NSA. It's run by Keith Alexander, the director of the NSA, and it's housed in the same place as the NSA. For all intents and purposes, US Cyber Command is the NSA, and Alexander has no problem at all swapping hats depending on what's most convenient. He regularly tries to talk about "protecting the network" when it suits him, ignoring that the same efforts he's looking at (greater access to corporate networks) would also make it much easier for the NSA and US Cyber Command to launch offensive attacks -- which Snowden's leaks proved the NSA did hundreds of times. Pretending the two are different, and that the NSA only focuses on "breaking codes and making codes" is yet another bogus claim from an NSA official, adding to a very long list.

#### And meet War Powers

Sasso ’13 (Brendan Sasso, Technology policy reporter for National Journal and The Hill, “NSA director to retain cyber war powers”, <http://thehill.com/blogs/hillicon-valley/193088-nsa-director-to-retain-cyber-war-powers>, December 13, 2013)

The White House has decided to preserve the cyber war powers held by the director of the National Security Agency (NSA). The decision to maintain NSA control over U.S. Cyber Command, a team of military hackers, means that the agency's next director will be a military officer and not a civilian, as privacy advocates had hoped.

#### NSA is an extension of presidential war powers authority

Levy ‘6 (Robert A. Levy, senior fellow in constitutional studies at the Cato Institute, “Wartime Executive Power and the NSA’s Surveillance Authority II”, <http://www.cato.org/publications/congressional-testimony/wartime-executive-power-nsas-surveillance-authority-ii>, February 28, 2006)

President Bush has authorized the NSA to eavesdrop, without obtaining a warrant, on telephone calls, emails, and other communications between U.S. persons in the United States and persons outside of the United States. For understandable reasons, the operational details of the NSA program are secret, as are the details of the executive order that authorized the program. But Attorney General Gonzales has stated that surveillance can be triggered if an executive branch official has reasonable grounds to believe that a communication involves a person “affiliated with al-Qaeda or part of an organization or group that is supportive of al-Qaeda.” 1 The attorney general has declared that the president’s authority rests on the post-9/11 Authorization for Use of Military Force [AUMF] and the president’s inherent wartime powers under Article II of the U.S. Constitution, which includes authority to gather “signals intelligence” on the enemy. 2 The NSA program, and its defense by the administration, raise these questions, which I propose to address below: (1) Does NSA warrantless surveillance violate the Fourth Amendment’s protection against unreasonable searches? (2) Does the program violate the Foreign Intelligence Surveillance Act [FISA]? (3) Does the AUMF authorize warrantless surveillance by the NSA? (4) Do the president’s inherent powers allow him to ignore FISA? (5) What should be done if the executive branch has acted unlawfully? My conclusions, as elaborated in the following sections, are: First, the president has some latitude under the “executive Power” and “Commander-in-Chief” Clauses of Article II, even lacking explicit congressional approval, to authorize NSA warrantless surveillance without violating the “reasonableness” requirement of the Fourth Amendment. But second, if Congress has expressly prohibited such surveillance (as it has under FISA), then the statute binds the president unless there are grounds to conclude that the statute does not apply. Third, in the case at hand, there are no grounds for such a conclusion — that is, neither the AUMF nor the president’s inherent powers trump the express prohibition in the FISA statute. My testimony today addresses only the legality of the NSA program, not the policy question whether the program is necessary and desirable from a national security perspective. If the program is both essential and illegal, then the obvious choices are to change the program so that it complies with the law, or change the law so that it authorizes the program. Nor do I address, other than to mention in this paragraph, three other constitutional arguments that might be advanced in opposition to warrantless surveillance by the NSA. First, in contravention of the First Amendment, the program may deprive innocent persons of the right to engage freely in phone and email speech. Second, the president may have violated his constitutional obligation to “take Care that the Laws be faithfully executed.” 3 Among the laws to be faithfully executed is FISA. No doubt, the president has some discretion in enforcing the law, but not leeway to take actions that the law expressly prohibits. Third, in contravention of the Fifth Amendment, the NSA surveillance program may represent a deprivation of liberty without due process. Liberty, as we know from the Supreme Court’s recent decision in Lawrence v. Texas4, encompasses selected aspects of privacy that are separate from the question whether particular intrusions are reasonable in terms of the Fourth Amendment. Those concerns are legitimate, but they have not been central to the debate over NSA surveillance, and they are not the focus of the Committee’s deliberations or, therefore, of my testimony. II. Does NSA Warrantless Surveillance Violate the Fourth Amendment? The president has contended that NSA warrantless surveillance does not offend Fourth Amendment protections against “unreasonable” searches. That contention is correct as far as it goes; but it does not go far enough. To begin, the Fourth Amendment requires probable cause in order to obtain a warrant, but it does not require a warrant for all searches. There are numerous instances of permissible warrantless searches — e.g., hot pursuit,5 evanescent evidence,6 search incident to arrest,7 stop and frisk,8 automobile searches,9 plain view searches,10 consent searches,11 and administrative searches.12 In fact, federal courts have recognized a border search exception 13 and, within the border search exception, an exception for monitoring certain international postal mail. 14 As for a national security exception for foreign intelligence surveillance, that remains an open issue. The so-called Keith case in 1972 said there would be no exception if a domestic organization were involved; but there might be an exception if a foreign power were involved. 15 Thus, the administration can credibly argue that it may conduct some types of warrantless surveillance without violating the Fourth Amendment. And because the president’s Article II powers are elevated during time of war — assuming the AUMF to be the functional, if not legal, equivalent of a declaration of war — his post-9/11 authorization of NSA warrantless surveillance might be justifiable if the Congress had not expressly disapproved. But the Congress did expressly disapprove, in the FISA statute. Therefore, the president’s assertion of a national security exception that encompasses the NSA program misses the point. The proper question is not whether the president has inherent authority to relax the “reasonableness” standard of the Fourth Amendment in order to direct warrantless surveillance, even if not approved by Congress. The answer to that question is “yes, in some cases.” But the narrower issue in the NSA case is whether the president, in the face of an express statutory prohibition, can direct that same surveillance. The answer is “no,” and I am not aware of any case law to support an argument to the contrary. Put somewhat differently, Article II establishes that the president has inherent powers, especially during wartime. And those powers might be sufficient to support his authorization of warrantless surveillance, notwithstanding the warrant provisions of the Fourth Amendment. But Article II does not delineate the scope of the president’s wartime powers. And because Congress has concurrent authority in this area,16 an express prohibition by Congress is persuasive when deciding whether the president has overreached. The distinction between concurrent and exclusive powers is important. For example, the president’s “Power to grant Reprieves and Pardons”17 is exclusive; there is no stated power for Congress to modify it by legislation — e.g., by declaring certain offenses unpardonable. By contrast, the president’s wartime powers are shared with Congress (see note 16). That suggests the president must comply with duly enacted statutes unless he can show that Congress has exceeded its authority. In this instance, President Bush has made no such showing. III. Does NSA Warrantless Surveillance Comply with FISA? Accordingly, even if the administration establishes that NSA warrantless surveillance during wartime is reasonable in the context of the Fourth Amendment, the question remains whether the NSA program violates the express terms of FISA. It does. The text of FISA is unambiguous: “A person is guilty of an offense if he intentionally engages in electronic surveillance … except as authorized by statute.” 18 That provision covers communications from or to U.S. citizens or permanent resident aliens in the United States. Moreover, the Wiretap Act provides that its procedures and FISA “shall be the exclusive means by which electronic surveillance … may be conducted.” 19 From the early 1960s until 1973, the NSA, without approval of Congress, used a “watch list” of U.S. citizens and organizations in sorting through intercepted foreign communications. That was known as Project Minaret.20 From 1945 to 1975, telegraph companies gave the NSA copies of most telegrams sent from the United States to overseas. That was known as Project Shamrock, “probably the largest governmental interception program affecting Americans ever undertaken.” 21 Of course, there were also domestic spying abuses by the Federal Bureau of Investigation under J. Edgar Hoover against suspected communists, Black Panthers, civil rights leaders and others. That’s why FISA was enacted in 1978. It had a dual purpose: to curb abuses while facilitating domestic surveillance for foreign intelligence purposes. To be sure, the FISA statute was drafted to deal with peacetime intelligence. But that does not mean the statute can be ignored when applied to the post-9/11 war on terror. First, the FISA text makes no distinction between wartime and peacetime. To conduct surveillance without statutory authorization, in wartime or peacetime, is a crime, punishable by up to five years in prison.22 Second, in passing FISA, Congress expressly contemplated warrantless surveillance during wartime, but limited it to the first 15 days after war is declared. The statute reads: “Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.”23 Third, FISA warrant requirements and electronic surveillance provisions were amended by the USA PATRIOT Act,24 which was passed in response to 9/11 and signed by President Bush. If 9/11 triggered “wartime,” as the administration has repeatedly and convincingly argued, then the amended FISA is clearly a wartime statute. Some administration supporters have argued that FISA and the PATRIOT Act provide tools that the president had anyway, except he could not use the acquired evidence in a criminal prosecution.25 Yet there is no support for the notion that members of Congress, in passing the two statutes, thought they were simply debating the rules of evidence. Moreover, warrant requirements are triggered even if the government declines to prosecute. Imagine police secretly entering a private home without a warrant, installing bugs on phones and tracer software on computers, searching every room and closet, then leaving, never to be heard from again — no arrest, no indictment, no notice to the target. Clearly, the Fourth Amendment’s warrant provisions have been violated, even if the target is unaware and no fruits of the search are used as evidence in a criminal prosecution. A key purpose of the Amendment is to ensure privacy in those situations in which an expectation of privacy is reasonable. That said, there may be some international satellite or radio communications that do not come under FISA’s prohibition because the communicating parties could not reasonably expect privacy. But I know of no court case that has denied there is a reasonable expectation of privacy by U.S. citizens and permanent resident aliens in their phone calls and emails. Moreover, the Justice Department, in a December 2005 letter to Congress, acknowledged that the president’s October 2001 NSA eavesdropping order did not comply with the “procedures” of the FISA statute.26 The Department offers two justifications — the first of which I examine next. IV. Does the AUMF Authorize Warrantless Surveillance by the NSA? The Justice Department asserts that Congress’s post-9/11 AUMF provides the statutory authorization that FISA requires. Under the AUMF, “the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons” who may have been connected to 9/11.27 But that cannot reasonably mean the AUMF authorizes warrantless surveillance by the NSA in the face of an express provision in FISA that limits such surveillance to the first 15 days after a declaration of war. A settled canon of statutory interpretation directs that specific provisions in a statute supersede general provisions — lex specialis derogat legi generali. When FISA forbids “electronic surveillance without a court order” while the AUMF permits “necessary and appropriate force,” it is bizarre to conclude that electronic surveillance without a court order is authorized. In voting for the AUMF, members of Congress surely did not intend to make compliance with FISA optional. In fact, Congress was simultaneously relaxing selected provisions of FISA via the PATRIOT Act. Here’s how the Washington Post put it: “Clearheaded members of Congress voting for the [AUMF] certainly understood themselves to be authorizing the capture of al-Qaeda and Taliban fighters. We doubt any members even dreamed they were changing domestic wiretapping rules — particularly because they were focused on that very issue in passing the USA PATRIOT Act.” 28 Also in the Washington Post, former Senate minority leader Tom Daschle (D-SD) wrote that Congress rejected proposed language from the White House that the broader purpose of the AUMF was to “deter and pre-empt any future acts of terrorism or aggression.” And Congress also refused a last-minute administration proposal to change “appropriate force against those nations” to read “appropriate force in the United States and against those nations.”29 Notably, not one of the 518 members of Congress who voted for the AUMF has now come forth to dispute Sen. Daschle’s account, or claim that his or her vote was intended to approve NSA warrantless surveillance. Still, proponents of the NSA surveillance program argue that (a) the intent of members of Congress in signing the AUMF is trumped by the text of the AUMF itself, (b) “necessary and appropriate force,” as permitted under the AUMF, surely includes the gathering of battlefield intelligence, and (c) the war on terror, and the events of 9/11 in particular, have expanded the notion of “battlefield” to encompass places in the United States.30 Those assertions, insofar as they are posited as justification for NSA warrantless surveillance, are mistaken for three principal reasons: First, communications from the actual battlefield — e.g., Afghanistan — or from anywhere else outside the United States, can be monitored without violating FISA as long as the target of the surveillance is not a U.S. person in the United States. Second, a call from, say, France or the United Kingdom cannot reasonably be construed as battlefield-related unless the term battlefield has no geographic limits. The courts have rejected that idea in comparing the arrests of two U.S. citizens, Yaser Hamdi and Jose Padilla. In Hamdi v. Rumsfeld, federal appellate judge J. Harvie Wilkinson pointedly noted that Yaser Hamdi’s battlefield capture was like “apples and oranges” compared to Jose Padilla’s arrest in Chicago.31 And in Padilla v. Rumsfeld, the U.S. Court of Appeals for the Second Circuit rejected the argument that all the world is a battlefield in the war on terror.32 Third, if Naples, Italy is part of the battlefield, why not Naples, Florida? The same logic that argues for warrantless surveillance of foreign-to-domestic and domestic-to-foreign communications would permit warrantless surveillance of all-domestic communications as well. Of course, the administration denies the existence of an all-domestic surveillance program, but so too would the administration have denied the NSA’s current program but for the leak in the New York Times. As law professor Richard Epstein has noted:33 A current battlefield, where there is armed combat, is vastly different from a potential battlefield that could erupt if the enemy were to launch a terrorist act. To argue that we are living in a “war zone” would be news to most Americans jogging in Central Park or watching television in Los Angeles. There is, after all, a distinction to be made between suburban Chicago and suburban Baghdad. Nor did the events of 9/11 transform the United States into a battlefield in the Afghan war — any more than did the attack on Pearl Harbor or the invasion by eight Nazis in the Ex parte Quirin case34 transform the United States into a World War II battlefield. What, then, does the preamble of the AUMF mean when it refers to terrorist acts that “render it both necessary and appropriate that the United States exercise the right to self-defense and to protect U.S. citizens both at home and abroad” (emphasis added)? Here, too, Professor Epstein has correctly interpreted the text:35 The AUMF preamble sets out the purpose of the resolution but does not address the legitimacy of means undertaken to carry out that purpose. No one doubts that the president has the right to use force in self-defense to protect citizens at home and abroad. But a preamble containing a broad statement of goals is not an affirmative grant of power to violate the law. Finally, did the Supreme Court in Hamdi v. Rumsfeld36 interpret the AUMF so broadly as to buttress the administration’s claim that the AUMF justifies the NSA surveillance program? At issue in Hamdi was whether the AUMF satisfied the Non-Detention Act,37 which required a statute authorizing Hamdi’s extended detention. The government insisted that a U.S. citizen could be detained indefinitely, without access to counsel, without a hearing, and without knowing the basis for his detention. The Court plurality agreed that a U.S. citizen could be initially detained under the AUMF. But only “Taliban combatants”38; only with access to counsel39; only after “notice of the factual basis for his classification”40 ; only after a hearing41 ; and only if not “indefinite detention for … interrogation.”42 In other words, the Hamdi Court interpreted the scope of the AUMF narrowly, not broadly. Not even Hamdi’s lawyers had argued that the government had to release enemy soldiers captured on the battlefield. Yet each of the government’s other contentions were rebuffed by the Court. Indeed, if Hamdi were a victory for the government, why did the Defense Department release him after declaring in court papers that merely allowing Hamdi to meet with counsel would “jeopardize[] compelling national security interests” and “interfere with if not irreparably harm the military’s ongoing efforts to gather intelligence.”43 In summary, the AUMF does not address, much less authorize, warrantless domestic surveillance. V. Do the President’s Inherent War Powers Allow Him to Ignore FISA? Attorney General Gonzales has a second, more plausible, defense of warrantless surveillance — namely, Article II of the Constitution states that “The executive Power shall be vested in a President” who “shall be Commander in Chief” of the armed forces. That power, says the attorney general, trumps any contrary statute during time of war. I respectfully disagree — which is not to say I believe the president is powerless to order warrantless wartime surveillance. For example, intercepting enemy communications on the battlefield is clearly an incident of his war power. But warrantless surveillance of Americans inside the United States, who may have nothing to do with al-Qaeda, does not qualify as incidental wartime authority. The president’s war powers are broad, but not boundless. Indeed, the war powers of Congress, not the president, are those that are constitutionalized with greater specificity.44 The question is not whether the president has unilateral executive authority, but rather the extent of that authority. And the key Supreme Court opinion that provides a framework for resolving that question is Justice Robert Jackson’s concurrence in Youngstown Sheet & Tube v. Sawyer45 — the 1952 case denying President Truman’s authority to seize the steel mills. Truman had argued that a labor strike would irreparably damage national security because steel production was essential to the production of war munitions. But during the debate over the 1947 Taft-Hartley Act,46 Congress had expressly rejected seizure. Justice Jackson offered the following analysis, which was recently adopted by the Second Circuit in holding that the administration could no longer imprison Jose Padilla:47 First, when the president acts pursuant to an express or implied authorization from Congress, “his authority is at its maximum.”48 Second, when the president acts in the absence of either a congressional grant or denial of authority, “there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain.”49 But third, where the president takes measures incompatible with the express or implied will of Congress — such as the NSA program, which violates an express provision of the FISA statute — “his power is at its lowest.”50 Even under Youngstown’s second category (congressional silence), the president might have inherent wartime authority to interpret the “reasonableness” standard of the Fourth Amendment in a manner that would sanction certain warrantless surveillance. But the NSA program does not fit in Youngstown’s second category. It belongs in the third category, in which the president has acted in the face of an express statutory prohibition. Naturally, if the statutory prohibition is itself unconstitutional, the administration is not only permitted but obligated to ignore it. That’s the argument administration supporters have proffered to excuse the NSA’s defiance of FISA.51 To bolster their case, they cite the only opinion that the FISA Court of Review has ever issued, In re: Sealed Case.52 There, the appellate panel mentioned several earlier cases53 that concluded the president has “inherent authority to conduct warrantless searches to obtain foreign intelligence information.”54 The Court of Review then added: “We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President’s constitutional power.”55 Three responses: First, I do not contend that the president lacks “inherent authority to conduct warrantless searches to obtain foreign intelligence information.” He has such authority, but Congress, exercising its own concurrent wartime powers, has limited the scope of that authority by excluding warrantless surveillance intentionally targeted at a U.S. person in the United States. Second, the surveillance in the earlier cases cited by Sealed Case took place pre-FISA, so Congress had not yet laid out the rules. Third, the quote from Sealed Case conveniently stops one sentence short. Here is the very next sentence: “The question before us is the reverse, does FISA amplify the President’s power by providing a mechanism that at least approaches a classic warrant and which therefore supports the government’s contention that FISA searches are constitutionally reasonable.”56 In resolving that question, the Court of Review did not conclude that FISA “encroach[ed] on the President’s constitutional power.” Quite the contrary, according to the court, FISA permissibly amplified the president’s power. The restrictive provisions in FISA were simply a clarification of his new and expanded authority. Thus, Sealed Case provides no support for the assertion that FISA unconstitutionally constrains the president’s inherent wartime authority. Moreover, such claims leave important questions unanswered. For example: If warrantless domestic surveillance is incidental to the president’s inherent powers, so too are sneak-and-peek searches, roving wiretaps, library records searches, and national security letters — all of which were vigorously debated in deciding whether to reauthorize the PATRIOT Act. Could the president have proceeded with those activities even if they were not authorized by Congress? If so, what was the purpose of the debate? And if not, what makes the NSA program different? Further, the attorney general asserts that the AUMF and the commander-in-chief power are sufficient to justify the NSA program. He, or his predecessor, made similar claims for military tribunals without congressional authorization,57 secret CIA prisons,58 indefinite detention of U.S. citizens,59 enemy combatant declarations without hearings as required by the Geneva Conventions,60 and interrogation techniques that may have violated our treaty commitments banning torture.61 Is any of those activities outside the president’s commander-in-chief and AUMF powers? If not, what are the bounds, if any, that constrain the president’s unilateral wartime authority? VI. What Should Be Done to Remedy Unlawful Acts by the Executive Branch? Having concluded that NSA’s warrantless surveillance program is illegal, let me comment briefly on some remedial steps to cure the president’s violation of the FISA statute. At the outset, I reject the proposition that the president, but for his ability to order warrantless surveillance of U.S. persons, would be impotent in the war on terror. First, he has expansive power to conduct surveillance outside the United States. Second, the PATRIOT Act and other statutes have given him broad leeway within the United States. Third, he has considerable, although not plenary, inherent authority under the commander-in-chief power when Congress has approved, or even perhaps when Congress has been silent. But when Congress exercises its own powers and expressly prohibits what the president would like to undertake, the president’s power is limited. Yet, even then, if it’s necessary and desirable to monitor the communication of a U.S. person in the United States, then the president could, and should, have sought a FISA warrant. The requirement to obtain a warrant from the FISA court is probable cause that someone may be “an agent of a foreign power,”62 which includes international terrorist groups. That standard is far below the usual criminal-law requirement for probable cause that a crime has been, or is about to be, committed. Almost all FISA requests are granted, and emergency approval for wiretaps can be handled within hours. In fact, the FISA statute allows the government in emergency situations to put a wiretap in place immediately, then seek court approval later, within 72 hours.63 Attorney General Gonzales has declared that 72 hours is not enough; it takes longer than that to prepare a warrant application.64 That is tantamount to arguing that the Justice Department lacks sufficient personnel to handle its workload, so it’s compelled to act illegally to circumvent prescribed procedures. Moreover, the administration has not, to my knowledge, complained about the same 72-hour window that governs domestic-to-domestic communications under FISA. Why is the window too short only when the party on the other end happens to be outside the United States? Indeed, the window was increased from 24 to 72 hours in the Intelligence Authorization Act for Fiscal Year 2002.65 If the longer period is still inadequate, why hasn’t the administration requested another extension from Congress? In his recent Senate testimony on the NSA program,66 Attorney General Gonzales outlined the following steps that must be taken before an emergency warrant application is filed. (1) NSA officials identify a legitimate target. (2) NSA lawyers ensure that the application complies with FISA. (3) Justice Department lawyers must agree. (4) The attorney general must agree. (5) The application must be approved by a Cabinet-level officer. (6) It must be approved by a senior official with mass security responsibility, such as the director of the FBI. FISA itself imposes only three requirements:67 (1) The attorney general must approve. (2) An official confirmed by the Senate with foreign affairs responsibility must certify that the surveillance has foreign intelligence value. (3) “Minimization procedures” must ensure that surveillance is not overbroad (for example, by preventing retention of information unrelated to national security). Accordingly, the redundancies cited by the attorney general are not necessary to comply with FISA. My colleague at the Cato Institute, Mark Moller, points out that the president “could cull out duplicative layers of lawyer oversight at both NSA and the Department of Justice. He could eliminate multiple sign-offs by senior officials. NSA case officers could initiate the warrant request. An intelligence oversight counsel assigned to specific ongoing investigations could process the warrant within the 72-hour time frame.”68 Moller concludes that “the president can simply change the procedures and cut the red tape. The president’s authority to manage the executive branch is a far more modest assertion of power than an ‘inherent’ authority to ignore the law.”69 Admittedly, FISA warrants might not be available for some surveillance operations that the NSA would like to undertake. FISA allows warrants only against foreign powers, including terrorist groups, or their agents. Therefore, a warrant is not available if the intended domestic target is not an “agent,” even if he is an al-Qaeda contact (perhaps not aware that his communications have intelligence value). Conceivably, FISA could be amended so that warrants could issue merely upon showing that an individual has had contact with al-Qaeda. That is a policy question, not a legal question, on which I claim no special insight. But it is important to note that under current law, surveillance of non-agent U.S. persons is even more egregious than warrantless surveillance of agents. The latter could be cured by a warrant; the former could not. In other words, if NSA targets a non-agent U.S. person, the violation of FISA consists not merely of unauthorized surveillance without obtaining a FISA warrant, but of surveillance under circumstances where a FISA warrant would never have been granted. If the president thought the law should be amended to authorize warrantless surveillance of either agents or non-agents, he had a convenient vehicle for that purpose shortly after 9/11. That’s when the PATRIOT Act was passed, substantially enhancing the president’s authority under FISA and expanding his ability to conduct foreign intelligence surveillance. The president could have, but did not, seek new authority for the NSA — authority that he has now decreed, unilaterally, without input from either Congress or the courts. Maybe Congress would not have approved if asked. Or maybe the courts would have overridden any further loosening of the warrant provisions. But the legal stumbling block for the administration is not just that it failed to get affirmative support for expanded surveillance from Congress and the courts. The bigger predicament is that Congress, without objection from the president, expressly rejected warrantless domestic surveillance and codified that prohibition in the FISA statute, which the president implicitly accepted when he signed the PATRIOT Act. Because the central problem with the NSA surveillance program is too much unchecked authority in the executive branch, the obvious solution is for the federal legislature or the federal judiciary to intervene. But the courts may decide they cannot play a role: First, the Justice Department will not prosecute; second, surveillance targets who have been secretly monitored are unlikely to know of their victimization; third, potential targets may not be able to prove sufficient injury; and fourth, aggrieved members of Congress have previously been denied legal standing to sue.70 That elevates the need for congressional intervention. But the president has resisted asking Congress to approve NSA domestic surveillance because, among other things, publicity might tip off al-Qaeda.71 Perhaps his concern is legitimate, but “tipping off terrorists” is an excuse not to debate any counterterrorism statute, including the PATRIOT Act, which was nonetheless debated vigorously. Moreover, the president’s rationale assumes that al-Qaeda would be blissfully ignorant of the surveillance but for congressional deliberations. The administration may be justified in taking measures that in pre-9/11 times could be seen as infringements of civil liberties. After all, the fuzzy text of the Fourth Amendment (unreasonable searches) and the Fifth Amendment (due process) leaves room for exceptions at the margin. But the executive branch cannot, in the face of an express prohibition by Congress, unilaterally set the rules, execute the rules, and eliminate oversight by the other branches.

War power authority is the ability to determine WHO engages in combat - we restrict that

Manget 87 (<http://media.nara.gov/dc-metro/rg-263/6922330/Box-10-114-7/263-a1-27-box-10-114-7.pdf>, declassified document, “PRESIDENTIAL WAR POWERS” accessed 8/17/13)

judicial Interpretation of War Powers Authority ¶ There are a limited number of cases dealing with the specific war powers ¶ authority of the Executive Branch. Nevertheless, several clear principles have ¶ emerged from them. ¶ 1. Conduct of War ¶ The President has very wide discretion in conducting wars. The strategy, ¶ objectives, and methods of waging war are squarely within his constitutional ¶ authority. The Supreme Court has stated that: ¶ As Commander in Chief, (the President) is authorized to direct ¶ the movements of the naval and military forces placed by law at his ¶ command, and to employ them in the manner he may deem most ¶ .effectual to harass and conQuer and subdue the enemy.24 ¶ Other federal courts have been in accord.25 The President has wide latitude in action because the nature of modern warfare requires centralized ¶ command and control for the successful prosecution of a war. ¶ 26 The total war ¶ power shared by the President and Congress grants them authority to use all ¶ means necessary to weaken the enemy and to bring the struggle to a successful ¶ conclusion, and has very few limits:27 "While the Constitution protects against ¶ invasiom. of individual rights, it is not a suicide pact. "¶ 28 Thus, how a war is to ¶ be waged is a matter of presidential. authority subject only to regular ¶ constitutional restrictions.

THis is a narrow interp as the Commander in Chief power is the ONLY war power authority

Bajesky 13 (2013¶ Mississippi College Law Review¶ 32 Miss. C. L. Rev. 9¶ LENGTH: 33871 words ARTICLE: Dubitable Security Threats and Low Intensity Interventions as the Achilles' Heel of War Powers NAME: Robert Bejesky\* BIO: \* M.A. Political Science (Michigan), M.A. Applied Economics (Michigan), LL.M. International Law (Georgetown). The author has taught international law courses for Cooley Law School and the Department of Political Science at the University of Michigan, American Government and Constitutional Law courses for Alma College, and business law courses at Central Michigan University and the University of Miami.)

A numerical comparison indicates that the Framer's intended for Congress to be the dominant branch in war powers. Congressional war powers include the prerogative to "declare war;" "grant Letters of Marque and Reprisal," which were operations that fall short of "war"; "make Rules for Government and Regulation of the land and naval Forces;" "organize, fund, and maintain the nation's armed forces;" "make Rules concerning Captures on Land and Water," "raise and support Armies," and "provide and maintain a Navy." [n25](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n25) In contrast, the President is endowed with one war power, named as the Commander-in-Chief of the Army and Navy. [n26](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n26)¶ The Commander-in-Chief authority is a core preclusive power, predominantly designating that the President is the head of the military chain of command when Congress activates the power. [n27](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n27) Moreover, peripheral Commander-in-Chief powers are bridled by statutory and treaty restrictions [n28](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n28) because the President "must respect any constitutionally legitimate restraints on the use of force that Congress has enacted." [n29](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n29) However, even if Congress has not activated war powers, the President does possess inherent authority to expeditiously and unilaterally react to defend the nation when confronted with imminent peril. [n30](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n30) Explicating the intention behind granting the President this latitude, Alexander Hamilton explained that "it is impossible to foresee or to define the extent and variety of national exigencies, or the correspondent extent and variety of the means which may be necessary to satisfy them." [n31](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n31) The Framers drew a precise distinction by specifying that the President was empowered "to repel and not to commence war." [n32](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.771738.1261791409&target=results_DocumentContent&returnToKey=20_T17974748742&parent=docview&rand=1376677997032&reloadEntirePage=true#n32)

### 2AC – Substantial = Across the Board

#### We meet – the plan is a substantial restriction on authority – it limits OCO authority for US citizens and creates a statutory check

#### Splitting NSA and US Cyber is a restriction on war powers independently-

#### C/I – Substantial means a large amount

**Dictionary.com 12**

sub·stan·tial   [suhb-stan-shuhl] Show IPA adjective 1. of ample or considerable amount, quantity, size, etc.: a substantial sum of money.

#### Anderson is in the context of school districts and assessing a student’s life not authority which clearly can’t be quantified or qualified

#### NSA performing Offensive Cyber Operations

McKalin ’13 (Vamien McKalin, Journalist for dotTech an online tech news agency, “New leaked documents show NSA’s cyber offensive against Russia, Iran, China, and North Korea”, <http://dottech.org/124872/new-leaked-documents-show-nsas-cyber-offensive-russia-iran-china-north-korea/>, September 1, 2013)

In 2011, the U.S. National Security Agency (NSA) carried out 231 offensive cyber operations using a computer program called GENIE. According to a leaked document revealed by the Washington Post, the NSA — and other agencies — use this program to plant covert implants into tens of thousands of machines every year. These implants then give these agencies some sort of access to the devices in question. What’s interesting is that the top priority targets for GENIE are in no other than North Korea, China, Iran, and Russia. Furthermore, the documents claim America sends agents out into the field to modify hardware and software at undisclosed locations. However, we understand the most common situation is to use a custom software gears composed by the NSA’s Tailored Access Operations (TAO). TAO has the ability to gain access to any kind of switches, firewalls, and routers anywhere in the world. In addition, TAO is resistive to any form of software update or upgrades, which should give you an idea of how powerful this GENIE program is. The documents went on to further reveal how TAO will soon have the ability to identify voice communications and secretly send out information whenever it sees fit. Washington Post claims the GENIE program aims to control over 85,000 secret implants by the end of 2013 — that’s up from 21,252 in 2008. Just recently, the NSA proposed a $52.6 billion budget, and we’re certain a large portion will go directly into funding the GENIE program. Seeing the likes of Russia, China, Iran, and North Korea on the list of high level targets, it would be very interesting to see how those countries react. The American government must quickly realize it is walking on a thin line here… especially seeing as the US is quick to point the finger at China for any and all cyber attacks.

#### Splitting head of command ends NSA offensive attacks

Masnick ’13 (Mike Masnick, Mike is the founder and CEO of Floor64 and editor of the Techdirt blog, “NSA Claims It Doesn't Do Online Attacks; That's A Different Organization... Run By The NSA”, <http://www.techdirt.com/articles/20131012/01195424849/nsa-claims-it-doesnt-do-online-attacks-thats-different-organization-run-nsa.shtml>, October 14, 2013)

There are times you just shake your head and wonder who the NSA top officials think they're kidding with their statements. Take, for example, some recent comments from the NSA's number two guy in charge, Chris Inglis, the Deputy Director, who gave an interview to the BBC where he tried to paint the NSA as not being quite as bad as everyone says, but admitted that there could be more transparency. That's all the usual stuff, but the following tidbit caught my eye: The job of the NSA, Mr Inglis said, was to exploit networks to collect intelligence in cyberspace and to defend certain networks - but not carry out destructive acts. "NSA had a responsibility from way back, from our earliest days, to both break codes and make codes," he said. "We have a responsibility to do intelligence in a space we once called the telecommunications arena - now cyberspace - and the responsibility to make codes or to defend signals communications of interest. "That's different than what most people conceive as offence or attack in this space." That task of destructive cyber attack, if ordered, lies with the US military's rapidly expanding Cyber Command. Except, as we've noted more than a few times, US Cyber Command is the NSA. It's run by Keith Alexander, the director of the NSA, and it's housed in the same place as the NSA. For all intents and purposes, US Cyber Command is the NSA, and Alexander has no problem at all swapping hats depending on what's most convenient. He regularly tries to talk about "protecting the network" when it suits him, ignoring that the same efforts he's looking at (greater access to corporate networks) would also make it much easier for the NSA and US Cyber Command to launch offensive attacks -- which Snowden's leaks proved the NSA did hundreds of times. Pretending the two are different, and that the NSA only focuses on "breaking codes and making codes" is yet another bogus claim from an NSA official, adding to a very long list.

#### And meet War Powers

Sasso ’13 (Brendan Sasso, Technology policy reporter for National Journal and The Hill, “NSA director to retain cyber war powers”, <http://thehill.com/blogs/hillicon-valley/193088-nsa-director-to-retain-cyber-war-powers>, December 13, 2013)

The White House has decided to preserve the cyber war powers held by the director of the National Security Agency (NSA). The decision to maintain NSA control over U.S. Cyber Command, a team of military hackers, means that the agency's next director will be a military officer and not a civilian, as privacy advocates had hoped.

#### Prefer our interp:

#### Over limits – their arg restricts the topic to one aff per topic area, kills innovation, creativity and aff ground which is vital to two sided engagement

#### Precision – no ev in the context of the topic proves excluding the aff is arbitrary – turns limits because imprecise limits are worse than not at all

#### Functional limits guarantee ground – ESR etc

#### The next paragraph of their O’ Connor card says the plan meets because its important and it’s a restriction

Justice O’Connor ‘02 Sandra Day, No. 00—1089 TOYOTA MOTOR MANUFACTURING, KENTUCKY,

INC., PETITIONER v. ELLA WILLIAMS, Jan 8, http://www.law.cornell.edu/supct/html/00-1089.ZO.html

We therefore hold that to be substantially limited in performing manual tasks, an individual must have an impairment that prevents or severely restricts the individual from doing activities that are of central importance to most people's daily lives. The impairment's impact must also be permanent or long-term. See 29 CFR §§1630.2(j)(2)(ii)-(iii) (2001).

#### A race to the most limiting interpretation causes a race to the bottom that kills substantive debate

#### Reasonability is uniquely applicable to determining whether an aff is substantial

Linda **Stadler 93** “NOTE: Corrosion Proof Fittings v. EPA: Asbestos in the Fifth Circuit--A Battle of Unreasonableness ” Tulane Environmental Law Journal Summer, 1993 6 Tul. Envtl. L.J. 423

n3 Matthew J. McGrath, Note, Convergence of the Substantial Evidence and Arbitrary and Capricious Standards of Review During Informal Rulemaking, 54 GEO. WASH. L. REV. 541, 546 n.30 (1986), (quoting H.R. REP. NO. 1980, 79th Cong., 2d Sess. 45 (1945)), reprinted in ADMINISTRATIVE PROCEDURE ACT LEGISLATIVE HISTORY, S. DOC. NO. 248, 79th Cong., 2d Sess. 11, 233, 279 (1945). The substantial evidence standard does however possess some ambiguity as to the definition of "substantial." See, e.g., Chemical Mfrs. Ass'n v. EPA, 899 F.2d 344, 359 (5th Cir. 1990) (stating that "'substantial' is an **inherently imprecise** word"). However, 'substantial' is generally **held to a reasonableness** standard, i.e., would a **reasonable mind** accept it as adequate to support a conclusion. E.g., Consolidated Edison Co. v. NLRB, 305 U.S. 197, 229 (1938).

### 2AC- Comission

TK

### 2AC- XO

#### Counterplan doesn’t solve

#### Intra-executive action doesn’t solve NSA Overreach

#### Doesn’t allow Congressional oversight and management of head of agency- that’s key to reform NSA- Congressional confirmation key

Clarke et al. ’13 (Richard A. Clarke (Clarke served the last three Presidents as a senior White House Advisor. Over the course of an unprecedented 11 consecutive years of White House service, he held the titles of: - Special Assistant to the President for Global Affairs - National Coordinator for Security and Counterterrorism - Special Advisor to the President for Cyber Security Prior to his White House years, Clarke served for 19 years in the Pentagon, the Intelligence Community, and State Department. During the Reagan Administration, he was Deputy Assistant Secretary of State for Intelligence. During the Bush (41) Administration, he was Assistant Secretary of State for Political-Military Affairs and coordinated diplomatic efforts to support the 1990–1991 Gulf War and the subsequent security arrangements. As a Partner in Good Harbor Consulting, LLC, Clarke advises clients on a range of issues including: - Corporate security risk management - Information security technology - Dealing with the Federal Government on security and IT issues - Counterterrorism In a Special Report by Foreign Policy Magazine, Clarke was chosen as one of The Top 100 Global Thinkers of 2010, Council on Foreign Relations, Former international affairs fellow in residence), Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, Peter Swire, “Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies”, <http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>, December 12, 2013)

The Director of NSA has not been a Senate-confirmed position; selection has been in the hands of the President alone. Because of the great impact of NSA actions, the need for public confidence in the Director, the value of public trust, and the importance of the traditional system of checks and balances, Senate confirmation is appropriate. Senate confirmation would increase both transparency and accountability. When appointing the directors of other intelligence organizations, Presidents have exercised their discretion to choose from the ranks of both civilian and military personnel. Both active duty military officers and civilians have been selected to be the Director of the CIA and the Director of the National Reconnaissance (NRO). It is important to the future of NSA that it be understood by the American people to be acting under appropriate controls and supervision.

#### Doesn’t require outside checks- militarized culture maintains in place- that causes cyber groupthink- triggers accidental war

Libicki ‘9 (Martin C. Libick, Senior Management Scientist; Professor, Pardee RAND Graduate School, Ph.D. in economics, M.A. in city and regional planning, University of California, Berkeley; S.B. in mathematics, Massachusetts Institute of Technology, “Cyberdeterrence and Cyberwar”, <http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf>, 2009)

Wars, in general, are most likely to start when one or both sides seriously misestimate the results of starting a conflict. If nothing else, the narrative so far suggests the many ambiguities that attend conflict in cyberspace: doubts about the ability to discover who did what (or hid the evidence thereof), weapon effects (both prospective and retro- spective), recovery time, the ability to continue similar lines of attack, cascading failures (or the lack thereof), the ability to route around damage, or the actions of third parties. If all parties react to uncer- tainty by shrinking from conflict, crises can be avoided—but it is not unknown for one or both sides to swallow their doubts (a common consequence of groupthink) and charge ahead.

#### Doesn’t solve relations through failed signal

#### Legislation is key to solve Obama international trust deficit with NSA

Witte 1/17 (Griff Witte, Post’s London bureau chief. He has previously served as the paper’s deputy foreign editor and as the bureau chief in Kabul, Islamabad and Jerusalem. Before joining the Post, Witte was a reporter for The Miami Herald. He also served as researcher for Steve Coll’s Pulitzer Prize-winning book, Ghost Wars, “Tepid global reaction to Obama’s NSA vow”, <http://www.washingtonpost.com/world/tepid-global-reaction-to-obamas-nsa-vow/2014/01/17/a37a43ac-7fb5-11e3-97d3-b9925ce2c57b_story.html?algtrack=mixedrec-4&tid=btm_rex_4>, January 17, 2014)

LONDON — After months of revelations that strained U.S. relations with allies and cast a harsh light on the National Security Agency’s global surveillance reach, President Obama’s speech Friday was aimed at least in part at reassuring the world of American intentions. But the initial reaction overseas suggested he still has a significant way to go to heal the rifts, with many wondering why he didn’t offer more specific protections. In Germany, where revelations that the NSA had been eavesdropping on the calls of Chancellor Angela Merkel stirred deep anger and unusually tough criticism of Washington, Obama’s promises to rein in the excesses of U.S. spying were met with a tepid welcome from the German government — and scorn from some analysts. Government spokesman Steffen Seibert tweeted that the government would appreciate better safeguards of the rights of non-U.S. citizens but would need more time to review Obama’s words in detail. Obama in his speech promised greater privacy protections for foreigners. But the new rules have yet to be written, leaving the possibility that intelligence officials will still have wide discretion in sweeping up information about private citizens overseas. Obama also said he had ordered new restrictions on spying on allied foreign heads of state. But the president did not define who would be considered an ally, nor did he promise an end to spying on foreign leaders’ aides, advisers or opponents. The seemingly limited nature of the new restrictions prompted German blogger and author Sascha Lobo to comment on Twitter: “Good to know that in the future you can escape surveillance by simply becoming chancellor.” German magazine Der Spiegel, meanwhile, accused the NSA of “turning the Internet into a weapons system.” Reaction was muted in Britain, which has been shown in leaked documents to be a key partner with the United States in global surveillance efforts. The government released a statement affirming that a parliamentary committee would review British law to find “the appropriate balance between our individual right to privacy and our collective right to security.” But British Prime Minister David Cameron has not come under the same sort of pressure to speak out on the issue that Obama has in the United States. Tony Travers, a professor at the London School of Economics, said that is unlikely to change. “Britain has always had such a powerful tradition of secrecy,” he said. “I doubt there have been anguished telephone calls across the Atlantic to get a change in American intelligence agency behavior.” Guardian editor Alan Rusbridger, whose newspaper has published revelations from files leaked by former NSA contractor Edward Snowden, said Britain has been “complacent” about the disclosures because both major political parties have been complicit. “I think they are closing their eyes and hoping it will go away,” Rusbridger said in remarks Friday to the BBC. “But it’s not going to go away, because it’s impossible to reform the NSA without that having a deep knock-on effect on what our own intelligence services do.” In other regions where the NSA revelations have made a big impact — including Latin America — there was no rush from governments to embrace Obama’s vows. Officials in Brazil, where President Dilma Rousseff has been outspoken in condemning the NSA surveillance, said they would have no comment on the matter.

### US-German Relations

#### Us-German relations solves laundry list

Scharioth, 11 -- Ph.D. in international economics from Tufts University Fletcher School

(Klaus, former German ambassador to the United States- 2006-11, "Germany And The U.S.," The Metropolitan, 5-2-11, www.metrocorpcounsel.com/articles/13811/germany-and-us-strong-working-relationship, accessed 10-16-12, mss)

Editor: What are the elements in German-U.S. relations that further the principles and goals of the New Transatlantic Agenda? Scharioth: The transatlantic relationship remains one of the cornerstones of Germany's foreign policy, and the United States is Germany's essential political and economic partner. We share the same values, which remain the bedrock of our enduring, close relationship. Transatlantic ties come in many shapes and forms - from the political and economic relationship, to the memories of U.S. service men and women and their families posted in Germany, to the unforgettable experiences young Germans and Americans take back with them after spending time at a high school or university in each other's country. Personal links and friendships add an essential dimension to our bilateral relationship. Clearly, our relationship has evolved since the end of the Cold War. Still, Germany highly appreciates the security umbrella that the United States continues to extend through NATO and its engagement in Europe. Politically, the Transatlantic Agenda of the 21st century differs significantly from the agenda of past decades. Fighting nuclear proliferation, promoting global disarmament, preventing failed states, settling regional conflicts, reforming the international financial markets, addressing climate change, strengthening global trade, defending our open societies - all these topics are of a global nature. Germany and the U.S. are tackling these challenges together and in unison with likeminded partners worldwide. For example, Germany is one of the main contributors to multilateral military, police, and humanitarian relief missions - in Afghanistan, where Germany's troop contingent is the third largest; in the Balkans, where it is the largest; or in the Gulf of Aden, where Germans and Americans have joined forces to foster stability and security. Our countries work hand in hand to coordinate our policies on Iran's nuclear program, and we closely coordinate our strategic partnership with Russia. Our partnership remains as vital as ever, while adapting to this new agenda while defending the values that bind us together.

### CMR Addon

#### Civilian control key to prevent CMR collapse

Lord ’11 (**Kristin M. Lord** is Vice President and Director of Studies at the Center for a New American Security. **Travis Sharp** is the Bacevich Fellow at the Center for a New American Security. **Joseph S. Nye,** Jr. is University Distinguished Service Professor at the Kennedy School of Government at Harvard University. **Mike McConnell** is Executive Vice President of Booz Allen Hamilton and former Director of National Intelligence and Director of the National Security Agency. **Gary McGraw** is Chief Technology Officer of Cigital, Inc., a software security consultancy, and author of eight books on software security. **Nathaniel Fick** is Chief Executive Officer of the Center for a New American Security. **Thomas G. Mahnken** is Jerome E. Levy Chair of Economic Geography and National Security at the U.S. Naval War College and a Visiting Scholar at the Johns Hopkins School of Advanced International Studies. **Gregory J. Rattray** is a Partner at Delta Risk LLC and Senior Vice President for Security at BITS, the technology policy division of The Financial Services Roundtable. **Jason Healey** is Director of the Cyber Statecraft Initiative at the Atlantic Council and Executive Director of the Cyber Conflict Studies Association. **Martha Finnemore** is Professor of Political Science and International Affairs at The George Washington University. **David A. Gross** is a Partner at Wiley Rein LLP and a former Ambassador and Coordinator for International Communications and Information Policy at the State Department. **Nova J. Daly** is a Public Policy Consultant at Wiley Rein LLP and former Deputy Assistant Secretary for Investment Security in the Office of International Affairs at the Treasury Department. **M. Ethan Lucarelli** is an Associate at Wiley Rein LLP. **Roger H. Miksad** is an Associate at Wiley Rein LLP. **James A. Lewis** is a Senior Fellow and Director of the Technology and Public Policy Program at the Center for Strategic and International Studies. **Richard Fontaine** is a Senior Fellow at the Center for a New American Security. **Will Rogers** is a Research Associate at the Center for a New American Security. **Christopher M. Schroeder** is an Internet entrepreneur, Chief Executive Officer of HealthCentral.com and a member of the Center for a New American Security’s board of advisors. **Daniel E. Geer**, Jr. is Chief Information Security Officer of In-Q-Tel, the independent investment firm that identifies innovative technologies in support of the missions of the U.S. intelligence community. **Robert E. Kahn** is President and Chief Executive Officer of the Corporation for National Research Initiatives and co-inventor of the TCP/IP protocol that is the foundation of the modern Internet. **Peter Schwartz** is Co-Founder and Chairman of Global Business Network and a member of the Center for a New American Security’s board of directors., America’s Cyber Future, “Security and Prosperity in the Information Age”, <https://www.llis.dhs.gov/sites/default/files/cyber%20future.pdf>, June 2011)

Lack of transparency in cyberspace also complicates oversight of government activities. The time available for careful decision-making is far shorter in cyberspace due to the dramatic increase in the breadth, source and speed of threaten- ing activities. This volatile reality challenges fundamental principles of U.S. national security by creating pressure to decentralize decision- making and provide pre-delegated authority to more junior military commanders. Were this to happen, senior civilian leaders might exercise less control over cyber operations, which could potentially erode civilian control of the military, a central tenet of American government.

Breakdown of CMR leads to global conflict

Cohen 97 - Robert E. Osgood Professor of Strategic Studies at the Paul H. Nitze School of Advanced International Studies (SAIS) at the Johns Hopkins University (Eliot, “Civil-military relations – Are U.S. Forces Overstretched”, <http://findarticles.com/p/articles/mi_m0365/is_n2_v41/ai_19416332/?tag=content;col1>)

Left uncorrected, the trends in American civil-military relations could breed certain pathologies. **The most serious possibility is that of a dramatic civil-military split** during a crisis involving the use of force. In the recent past, such tensions did not result in open division; for example, Franklin Roosevelt insisted that the United States invade North Africa in 1942, though the chiefs of both the army and the navy vigorously opposed such a course, favoring instead a buildup in England and an invasion of the continent in 1943. Back then it was inconceivable that a senior military officer would leak word of such a split to the media, where it would have reverberated loudly and destructively. To be sure, from time to time individual officers broke the vow of professional silence to protest a course of action, but in these isolated cases the officers paid the accepted price of termination of their careers. In the modern environment, such cases might no longer be isolated. Thus,presidents might try to shape U.S. strategy so that it complies with military opinion, and rarely in the annals of statecraft has military opinion alone been an adequate guide to sound foreign policy choices. Had Lincoln followed the advice of his senior military advisors there is a good chance that the Union would have fallen. Had Roosevelt deferred to General George C. Marshall and Admiral Ernest J. King there might well have been a gory debacle on the shores of France in 1943. Had Harry S Truman heeded the advice of his theater commander in the Far East (and it should be remembered that the Joint Chiefs generally counseled support of the man on the spot) there might have been a third world war. Throughout much of its history, the U.S. military was remarkably politicized by contemporary standards. One commander of the army, Winfield Scott, even ran for president while in uniform, and others (Leonard Wood, for example) have made no secret of their political views and aspirations. But until 1940, and with the exception of periods of outright warfare, the military was a negligible force in American life, and America was not a central force in international politics. That has changed. Despite the near halving of the defense budget from its high in the 1980s, it remains a significant portion of the federal budget, and the military continues to employ millions of Americans. More important, civil-military relations in the United States now no longer affect merely the closet-room politics of Washington, but **the relations of countries around the world.** American choices about the use of force, the shrewdness of American strategy, the soundness of American tactics, and the will of American leaders **have global consequences.** What might have been petty squabbles in bygone years are now magnified into **quarrels of a far larger scale**, and conceivably with far more grievous consequences. To ignore the problem would neglect one of the cardinal purposes of the federal government: "to provide for the common defense" in a world in which security cannot be taken for granted.

### Iran Ptx

#### Sanctions will pass now- its veto-proof

Koring, 1-15 -- Globe and Mail (Canada) International Affairs and Security Correspondent

[Paul, "Showdown on Iran looms in U.S. Senate; Hawks are circling over Capitol Hill and Obama's bargain with Tehran is further imperilled by members of his own party", The Globe and Mail (Canada), PAS) Accessed on LexisNexis 1-16-14]

Rapprochement with Iran - the United States' most unpredictable enemy since the mullahs toppled the Shah more than three decades ago - might eventually emerge as President Barack Obama's most significant foreign-policy achievement.¶ Ending the enmity, if not quite deserving of the Nobel Peace Prize the President has already pocketed, would avert the risk of a nuclear-weapons race in the region. The pact to expose Tehran's nuclear program to international inspection is only a first step.¶ But hawks are circling over Capitol Hill and Mr. Obama's bargain with Tehran is imperilled, not just by doubters like Benjamin Netanyahu in Jerusalem and John Baird in Ottawa who claim Iran's leaders can't be trusted, but more importantly, by defecting Democrats.¶ **Nearly two dozen** Democrat senators have joined Republicans in backing a bill that would slap new sanctions on Iran. Mr. Obama has vowed to veto any new sanctions. But a showdown looms. In a rare show of bipartisanship, the pro-sanctions group is nearing the magic number of 67 - sufficient to provide the **veto-overriding** two-thirds majority in the 100-seat Senate that could doom the deal under which Tehran has agreed to stop enriching uranium to anywhere close to weapons-grade.¶ President Obama's domestic problems with his Congressional flank were made worse Tuesday by some internal politicking in Iran.¶ Iran's President Hassan Rouhani boasted United States had capitulated to Tehran in the deal, saying on Twitter that "world powers surrendered to Iranian nation's will." That may please hard-liners at home but is certain to inflame them in the United States. The White House sought to dampen the impact, saying Mr. Rouhani was playing to a domestic audience. "It doesn't matter what they say. It matters what they do," said Mr. Obama's spokesman, Jay Carney.

#### Sanctions will pass now- AIPAC lobbying

Fallows 1-17 -- national correspondent for The Atlantic

[James “The Iran Vote: This Really Matters, and You Should Let Your Senators Know,” 1-14-14, <http://www.theatlantic.com/politics/archive/2014/01/the-iran-vote-this-really-matters-and-you-should-let-your-senators-know/283070/> DOA: 1-17-14]

That derailment is what seems to be underway in the Senate right now. Republicans led by Mitch McConnell are pushing for a sanctions bill that is universally recognized (except by its sponsors) as a poison-pill for the current negotiations. Fine; opposing the administration is the GOP's default position. But a striking number of Democrats have joined them, for no evident reason other than **AIPAC's whole-hearted,** priority-one **support** for the sanctions bill. The screen clip below is from AIPAC's site, and here is some political reporting on AIPAC's role in the sanctions push: NYT, Politico, JTA, Jerusalem Post-JTA, and our own National Journal here and here. Also see Greg Sargent in the Washington Post. In the long run, **these Democrats** are not in a tenable position. Or not a good one. They **are opposing** what **their president**, his secretaries of state and defense, our normal major allies, and even the Russians and Chinese view as a step toward peace. And their stated reason for doing so—that new sanction threats will "help" the negotiations, even though every American, French, British, German, etc., and Iranian figure involved in the talks says the reverse—doesn't pass the straight-face test.

Obama will use unilateral sanctions relief—solves

Adam Kredo, 1/21/14, White House Seeks to Bypass Congress on Iran Deal, freebeacon.com/white-house-seeks-to-bypass-congress-on-iran-deal/

The White House has been exploring ways to circumvent Congress and unilaterally lift sanctions on Iran once a final nuclear agreement is reached, according to sources with knowledge of White House conversations and congressional insiders familiar with its strategy.

The issue of sanctions relief has become one of the key sticking points in the Iran debate, with lawmakers pushing for increased economic penalties and the White House fighting to roll back regulations.

While many in Congress insist that only the legislative branch can legally repeal sanctions, senior White House officials have been examining strategies to skirt Congress, according to those familiar with internal conversations.

Sen. Mark Kirk (R., Ill.), who is leading the charge on new sanctions legislation, said that it is unacceptable for the White House to try to bypass Congress on such a critical global issue.

“The American people must get a say in any final nuclear agreement with Iran to ensure the mullahs never get the bomb,” Kirk told the Washington Free Beacon. “The administration cannot just ignore U.S. law and lift sanctions unilaterally.”

Congressional insiders say that the White House is worried Congress will exert oversight of the deal and demand tougher nuclear restrictions on Tehran in exchange for sanctions relief.

Top White House aides have been “talking about ways to do that [lift sanctions] without Congress and we have no idea yet what that means,” said one senior congressional aide who works on sanctions. “They’re looking for a way to lift them by fiat, overrule U.S. law, drive over the sanctions, and declare that they are lifted.”

Under the interim nuclear deal with Iran that began on Monday, Tehran will receive more than $4 billion in cash, according to the White House.

President Barack Obama could unilaterally unravel sanctions through several executive channels, according to former government officials and legal experts.

Executive orders grant the president significant leverage in the how sanctions are implemented, meaning that Obama could choose to stop enforcing many of the laws on the books, according to government insiders.

Those familiar with the ins and outs of sanctions enforcement say that the White House has long been lax with its enforcement of sanctions regulations already on the books.

“It’s no secret that the president, with executive power, can determine sanctions implementation, particularly with waivers and the decision not to sanction certain entities,” said Jonathan Schanzer, a former terrorism finance analyst at the Treasury Department, which is responsible for enforcing sanctions.

“The financial pressure has always been about closing loopholes and identifying new ones to close,” Schanzer added. “If you stop that process of constant gardening, you leave a backdoor open.”

Obama could also use executive waivers to “bypass restrictions imposed by the law,” according to a report by Patrick Clawson, director of research at the Washington Institute for Near East Policy (WINEP).

The president has a lot of leverage when it comes to sanctions and could effectively “turn a blind eye” to Iranian infractions.

“In the case of Iran, such an approach could allow Washington to reach a nuclear accord without Congress having to vote on rescinding, even temporarily or conditionally, certain sanctions,” Clawson wrote. “No matter how stiff and far-reaching sanctions may be as embodied in U.S. law, they would have less bite if the administration stopped enforcing them.”

One former senior government official said that President Obama’s legal team has likely been investigating the issue for quite some time.

“I’d be shocked if they weren’t putting the various sanctions laws under a microscope to see how they can waive them or work around them in order to deliver to Iran sanctions relief without having to worry about Congress standing in their way,” said Stephen Rademaker, who served as deputy legal adviser to former President George H.W. Bush’s National Security Council (NSC).

Executive branch lawyers are often tasked with finding ways to get around existing legislation, Rademaker said.

“I’m sure pretty early in the negotiating process they developed a roadmap” to ensure the president has the authority to promise Iran significant relief from sanctions, said Rademaker, who also served as chief council for the House Committee on International Relations. “I’m sure they’ve come up with an in depth analysis of what they can do relying exclusively on the president’s legal authority.”

The White House has been known to disregard portions of the sanctions laws that it disagrees with, according to Schanzer.

#### Healthcare thumps the link- democrats abandoning Obama, guarantees sanctions now. PC is not high enough to outweigh the Israel lobby

Finkel 1-15-- editor of Against the Current

[David “Will the Iran deal hold?” <http://internationalviewpoint.org/spip.php?article3239>, DOA: 1-17-14]

A politically weakened U.S. president is pulled by a powerful domestic lobby and influential foreign governments toward launching a war that U.S. imperialism right now doesn’t want, that the world doesn’t want, and that the large majority of the American public doesn’t want — what will be the outcome? It’s an interesting, if dangerous and scary, test of how U.S. politics actually work. The initial results, at least, are in: The unleashed fury of the Israeli government and the “pro-Israel” lobby, the monarchy of Saudi Arabia, the neoconservative warmongers and the much-feared religious right weren’t able to block the Obama administration and European partners from reaching a six-month interim agreement with Iran over that country’s nuclear enrichment program. Any socialist, progressive or sane person must welcome this agreement. That’s not because it resolves the proliferation of nuclear weapons, or changes the hideous character of the Iranian regime in relation to its own population, or addresses the multiple underlying issues of the Middle East crisis — it does none of these things — but because it pushes back the imminent danger of a really catastrophic war. That’s one strike against the widely held theory that the toxic influence of the Israel Lobby can drag the United States into wars that this country‘s ruling class disapproves. The political fight, of course, is hardly over. We’ll explore the underlying reasons for the Israeli and Saudi sound and fury over the deal with Iran, which in fact have little to do with the rather distant specter of an Iranian atomic bomb. But we need to note the U.S. political context in which the fight will play out. If anything, this might have been expected to strengthen the hand of the “war party.” A Wounded Presidency The spectacular disaster of the Afford­able Care Act website is a self-inflicted wound from which the Obama administration will not easily, or perhaps ever, fully recover. Certainly all of us who support single-payer health insurance realized that the fantastically tangled system of “Obamacare” would ultimately fail, due to its scheme for subsidizing the parasitical private insurance industry, but no one could have expected such an immediate display of arrogant incompetence in the “rollout.” The Republican Party has regained big chunks of the ground lost during its own government shutdown fiasco. It’s true that Congress’s approval ratings remain even deeper in the toilet than the President’s, but that fact affects both capitalist parties — and now, Congressional Democrats who stood united against repealing “Obamacare,” because that would have represented the effective end of the Obama presidency and virtual suicide for the party, are angry, alienated and afraid to be near him. Whatever political capital the President had for immigration reform, seriously raising the minimum wage, protecting food stamps from savage cuts, or much of anything else including the climate change crisis, has been dissipated. The Democrats’ chances of regaining the House of Representatives in the November 2014 midterm election, marginal to begin with, are now much less than those of losing the Senate as well. In these circumstances, this might be considered a favorable moment for the power of the Israel Lobby, Saudi Arabia and rightwing militarists to derail the Obama administration’s deal with Iran. In fact, France made a last-minute move to block the first version of the interim agreement — right after Saudi Arabia signed off on a huge purchase of French weapons (a point worth noting in case anyone thought it’s only the USA that has a military-industrial complex). The President’s **loss of control over his own party** is such that many prominent Democratic Senators have taken to the airwaves loudly denouncing his “appeasement” of the Iranians and abandonment of Israel in its hour of existential peril.

### 2AC- Politics

#### PC theory is wrong- winners win

Hirsh ’13 (National Journal chief correspondent, citing various political scientists, Michael, former Newsweek senior correspondent, "There’s No Such Thing as Political Capital," National Journal, 2-9-13, www.nationaljournal.com/magazine/there-s-no-such-thing-as-political-capital-20130207, accessed 2-8-13, mss]

The idea of political capital—or mandates, or momentum—is so poorly defined that presidents and pundits often get it wrong. On Tuesday, in his State of the Union address, President Obama will do what every president does this time of year. For about 60 minutes, he will lay out a sprawling and ambitious wish list highlighted by gun control and immigration reform, climate change and debt reduction. In response, the pundits will do what they always do this time of year: They will talk about how unrealistic most of the proposals are, discussions often informed by sagacious reckonings of how much “political capital” Obama possesses to push his program through. Most of this talk will have no bearing on what actually happens over the next four years. Consider this: Three months ago, just before the November election, if someone had talked seriously about Obama having enough political capital to oversee passage of both immigration reform and gun-control legislation at the beginning of his second term—even after winning the election by 4 percentage points and 5 million votes (the actual final tally)—this person would have been called crazy and stripped of his pundit’s license. (It doesn’t exist, but it ought to.) In his first term, in a starkly polarized country, the president had been so frustrated by GOP resistance that he finally issued a limited executive order last August permitting immigrants who entered the country illegally as children to work without fear of deportation for at least two years. Obama didn’t dare to even bring up gun control, a Democratic “third rail” that has cost the party elections and that actually might have been even less popular on the right than the president’s health care law. And yet, for reasons that have very little to do with Obama’s personal prestige or popularity—variously put in terms of a “mandate” or “political capital”—chances are fair that both will now happen. What changed? In the case of gun control, of course, it wasn’t the election. It was the horror of the 20 first-graders who were slaughtered in Newtown, Conn., in mid-December. The sickening reality of little girls and boys riddled with bullets from a high-capacity assault weapon seemed to precipitate a sudden tipping point in the national conscience. One thing changed after another. Wayne LaPierre of the National Rifle Association marginalized himself with poorly chosen comments soon after the massacre. The pro-gun lobby, once a phalanx of opposition, began to fissure into reasonables and crazies. Former Rep. Gabrielle Giffords, D-Ariz., who was shot in the head two years ago and is still struggling to speak and walk, started a PAC with her husband to appeal to the moderate middle of gun owners. Then she gave riveting and poignant testimony to the Senate, challenging lawmakers: “Be bold.” As a result, momentum has appeared to build around some kind of a plan to curtail sales of the most dangerous weapons and ammunition and the way people are permitted to buy them. It’s impossible to say now whether such a bill will pass and, if it does, whether it will make anything more than cosmetic changes to gun laws. But one thing is clear: The political tectonics have shifted dramatically in very little time. Whole new possibilities exist now that didn’t a few weeks ago. Meanwhile, the Republican members of the Senate’s so-called Gang of Eight are pushing hard for a new spirit of compromise on immigration reform, a sharp change after an election year in which the GOP standard-bearer declared he would make life so miserable for the 11 million illegal immigrants in the U.S. that they would “self-deport.” But this turnaround has very little to do with Obama’s personal influence—his political mandate, as it were. It has almost entirely to do with just two numbers: 71 and 27. That’s 71 percent for Obama, 27 percent for Mitt Romney, the breakdown of the Hispanic vote in the 2012 presidential election. Obama drove home his advantage by giving a speech on immigration reform on Jan. 29 at a Hispanic-dominated high school in Nevada, a swing state he won by a surprising 8 percentage points in November. But the movement on immigration has mainly come out of the Republican Party’s recent introspection, and the realization by its more thoughtful members, such as Sen. Marco Rubio of Florida and Gov. Bobby Jindal of Louisiana, that without such a shift the party may be facing demographic death in a country where the 2010 census showed, for the first time, that white births have fallen into the minority. It’s got nothing to do with Obama’s political capital or, indeed, Obama at all. The point is not that “political capital” is a meaningless term. Often it is a synonym for “mandate” or “momentum” in the aftermath of a decisive election—and just about every politician ever elected has tried to claim more of a mandate than he actually has. Certainly, Obama can say that because he was elected and Romney wasn’t, he has a better claim on the country’s mood and direction. Many pundits still defend political capital as a useful metaphor at least. “It’s an unquantifiable but meaningful concept,” says Norman Ornstein of the American Enterprise Institute. “You can’t really look at a president and say he’s got 37 ounces of political capital. But the fact is, it’s a concept that matters, if you have popularity and some momentum on your side.” The real problem is that the idea of political capital—or mandates, or momentum—is so poorly defined that presidents and pundits often get it wrong. “Presidents usually over-estimate it,” says George Edwards, a presidential scholar at Texas A&M University. “The best kind of political capital—some sense of an electoral mandate to do something—is very rare. It almost never happens. In 1964, maybe. And to some degree in 1980.” For that reason, political capital is a concept that misleads far more than it enlightens. It is distortionary. It conveys the idea that we know more than we really do about the ever-elusive concept of political power, and it discounts the way unforeseen events can suddenly change everything. Instead, it suggests, erroneously, that a political figure has a concrete amount of political capital to invest, just as someone might have real investment capital—that a particular leader can bank his gains, and the size of his account determines what he can do at any given moment in history. Naturally, any president has practical and electoral limits. Does he have a majority in both chambers of Congress and a cohesive coalition behind him? Obama has neither at present. And unless a surge in the economy—at the moment, still stuck—or some other great victory gives him more momentum, it is inevitable that the closer Obama gets to the 2014 election, the less he will be able to get done. Going into the midterms, Republicans will increasingly avoid any concessions that make him (and the Democrats) stronger. But the abrupt emergence of the immigration and gun-control issues illustrates how suddenly shifts in mood can occur and how political interests can align in new ways just as suddenly. Indeed, the pseudo-concept of political capital masks a larger truth about Washington that is kindergarten simple: You just don’t know what you can do until you try. Or as Ornstein himself once wrote years ago, “Winning wins.” In theory, and in practice, depending on Obama’s handling of any particular issue, even in a polarized time, he could still deliver on a lot of his second-term goals, depending on his skill and the breaks. Unforeseen catalysts can appear, like Newtown. Epiphanies can dawn, such as when many Republican Party leaders suddenly woke up in panic to the huge disparity in the Hispanic vote. Some political scientists who study the elusive calculus of how to pass legislation and run successful presidencies say that political capital is, at best, an empty concept, and that almost nothing in the academic literature successfully quantifies or even defines it. “It can refer to a very abstract thing, like a president’s popularity, but there’s no mechanism there. That makes it kind of useless,” says Richard Bensel, a government professor at Cornell University. Even Ornstein concedes that the calculus is far more complex than the term suggests. Winning on one issue often changes the calculation for the next issue; there is never any known amount of capital. “The idea here is, if an issue comes up where the conventional wisdom is that president is not going to get what he wants, and [they]he gets it, then each time that happens, it changes the calculus of the other actors” Ornstein says. “If they think he’s going to win, they may change positions to get on the winning side. It’s a bandwagon effect.” ALL THE WAY WITH LBJ Sometimes, a clever practitioner of power can get more done just because [they’re]he’s aggressive and knows the hallways of Congress well. Texas A&M’s Edwards is right to say that the outcome of the 1964 election, Lyndon Johnson’s landslide victory over Barry Goldwater, was one of the few that conveyed a mandate. But one of the main reasons for that mandate (in addition to Goldwater’s ineptitude as a candidate) was President Johnson’s masterful use of power leading up to that election, and his ability to get far more done than anyone thought possible, given his limited political capital. In the newest volume in his exhaustive study of LBJ, The Passage of Power, historian Robert Caro recalls Johnson getting cautionary advice after he assumed the presidency from the assassinated John F. Kennedy in late 1963. Don’t focus on a long-stalled civil-rights bill, advisers told him, because it might jeopardize Southern lawmakers’ support for a tax cut and appropriations bills the president needed. “One of the wise, practical people around the table [said that] the presidency has only a certain amount of coinage to expend, and you oughtn’t to expend it on this,” Caro writes. (Coinage, of course, was what political capital was called in those days.) Johnson replied, “Well, what the hell’s the presidency for?” Johnson didn’t worry about coinage, and he got the Civil Rights Act enacted, along with much else: Medicare, a tax cut, antipoverty programs. He appeared to understand not just the ways of Congress but also the way to maximize the momentum he possessed in the lingering mood of national grief and determination by picking the right issues, as Caro records. “Momentum is not a mysterious mistress,” LBJ said. “It is a controllable fact of political life.” Johnson had the skill and wherewithal to realize that, at that moment of history, he could have unlimited coinage if he handled the politics right. He did. (At least until Vietnam, that is.)

#### Obama uses the plan to shift blame- solves losers lose

Wehner ’13 (Peter Wehner, “Barack Obama’s Staggering Incompetence”, <http://www.commentarymagazine.com/2013/09/02/barack-obamas-staggering-incompetence/>, September 2, 2013)

It’s reported that President Obama was ready to order a military strike against Syria, with or without Congress’s blessing, but “on Friday night, he suddenly changed his mind.” According to the Huffington Post: Senior administration officials describing Obama’s about-face Saturday offered a portrait of a president who began to wrestle with his own decision – at first internally, then confiding his views to his chief of staff, and finally summoning his aides for an evening session in the Oval Office to say he’d had a change of heart. In light of all this, it’s worth posing a few questions: 1. Why didn’t the president seek congressional authority before the administration began to beat the war drums this past week? Did the idea not occur to him? It’s not as if this is an obscure issue. When you’re in the White House and preparing to launch military force against a sovereign nation, whether or not to seek the approval of Congress is usually somewhere near the top of the to-do list. And why has the urgency to act that we saw from the administration during the last week–when Assad’s use of chemical weapons was referred to by the secretary of state as a “moral obscenity”–given way to an air of casualness, with Obama not even calling Congress back into session to debate his military strike against Syria? 2. The president didn’t seek congressional approval for his military strike in Libya. Why does he believe he needs it in Syria? 3. Mr. Obama, in his Rose Garden statement on Saturday, still insisted he has the authority to strike Syria without congressional approval. So what happens if Congress votes down a use-of-force resolution? Does the president strike Syria anyway? If so, will it be an evanescent bombing, intended to be limited in scope and duration, while doing nothing to change the war’s balance of power? Or does the president completely back down? Does he even know? Has he thought through in advance anything related to Syria? Or is this a case of Obama simply making it up as he goes along? This latest volte-face by the president is evidence of a man who is completely overmatched by events, weak and confused, and deeply ambivalent about using force. Yet he’s also desperate to get out of the corner he painted himself into by declaring that the use of chemical weapons by the Assad regime would constitute a “red line.” As a result he’s gone all Hamlet on us. Not surprisingly, Obama’s actions are being mocked by America’s enemies and sowing doubt among our allies. (Read this New York Times story for more.) What explains this debacle? It’s impossible for us to know all the reasons, but one explanation appears to be a CYA operation. According to Politico, “At the very least, Obama clearly wants lawmakers to co-own a decision that he can’t back away from after having declared last year that Assad would cross a ‘red line’ if he used chemical weapons against his own people.” And the Washington Post reports: Obama’s proposal to invite Congress dominated the Friday discussion in the Oval Office. He had consulted almost no one about his idea. In the end, the president made clear he wanted Congress to share in the responsibility for what happens in Syria. As one aide put it, “We don’t want them to have their cake and eat it, too.” Get it? The president of the United States is preparing in advance to shift the blame if his strike on Syria proves to be unpopular and ineffective. He’s furious about the box he’s placed himself in, he hates the ridicule he’s (rightly) incurring, but he doesn’t see any way out. What he does see is a political (and geopolitical) disaster in the making. And so what is emerging is what comes most naturally to Mr. Obama: Blame shifting and blame sharing. Remember: the president doesn’t believe he needs congressional authorization to act. He’s ignored it before. He wants it now. For reasons of political survival. To put it another way: He wants the fingerprints of others on the failure in Syria. Rarely has an American president joined so much cynicism with so much ineptitude.

#### Obama and Congress want the plan- no fight link

AP 1/9 (Associated Press, “Obama weighing changes to NSA restrictions”, <http://nypost.com/2014/01/09/obama-weighing-changes-to-nsa-restrictions/>, January 9, 2014)

WASHINGTON — President Barack Obama is still grappling with key decisions on the future of the National Security Agency’s phone collection program and the makeup of the secret court that approved the surveillance, congressional lawmakers said Thursday following a 90-minute meeting at the White House. Obama is expected to back tighter restrictions on foreign leader spying and also is considering a presidential commission’s recommendation to strip the NSA of its ability to store telephone records from millions of Americans. The president could announce his final decisions as early as next week. “The president and his administration are wrestling with the issues,” Sen. Ron Wyden, an Oregon Democrat and privacy advocate, said after the meeting. “It’s fair to say that the next few weeks are going to be crunch time in terms of judgments being made in both the administration and the Congress.” Rep. Adam Schiff, D-Calif., said the meeting focused in particular on the telephone data program and the Foreign Intelligence Surveillance Court. He said that while Obama didn’t appear to have made a decision on either issue yet, he expects him to do so soon. The president met this week with his top intelligence advisers, many of whom oppose changes to the NSA programs, and a review group appointed by Congress that is working on a report focused on the surveillance systems. Privacy advocates were meeting with senior White House staff Thursday afternoon, and technology companies have been invited to a meeting on Friday. The president’s decisions will test how far he is willing to go in scaling back the NSA’s broad surveillance powers. A presidential commission handed him more than 40 recommendations, many of which were more sweeping than expected. However, Obama is not obligated to accept any of the panel’s proposals. The White House indicated that whatever the president announces in the coming days may not be his final word on the matter. Obama spokesman Jay Carney said that while Obama is likely to announce some changes he wants implemented right away, “there may be some that would require further review.” Congress is also likely to play a role in implementing some of the president’s recommendations, particularly if he makes changes to the phone collection program. Lawmakers in both parties have said they would support congressional involvement on the matter. “With each new revelation of the scope of these programs, it’s increasingly clear that we need to take legislative action to reform some of our nation’s intelligence-gathering programs to ensure that they adequately protect Americans’ civil liberties and operate in a sensible manner,” said Rep. Bob Goodlatte, R-Va., who also attended Thursday’s White House meeting.

#### Plan popular- this is evidence specific about the aff

Romm ’13 (Tony Romm, technology reporter for POLITICO Pro. He closely follows tech topics and debates on Capitol Hill and before agencies like the Federal Trade Commission, keeping a close eye on issues such as online privacy, antitrust and competitiveness, tech industry lobbying and PAC spending, intellectual property and cybersecurity, “Congress could see power to confirm NSA chief”, <http://www.politico.com/story/2013/11/congress-could-seek-nsa-confirmation-99650.html>, November 10, 2013)

Frustration with the National Security Agency’s spying and the impending departure of its longtime director have fueled a congressional push to put its future leaders through the potentially grueling process of Senate confirmation — a scenario the White House has warned in the past could harm intelligence efforts. The idea — backed by California Democratic Sen. Dianne Feinstein, the leader of the Intelligence Committee and one of the NSA’s top allies in Congress — is among the more prominent agency reforms percolating on Capitol Hill, where lawmakers are rethinking the agency’s expansive surveillance authorities in light of Edward Snowden’s leaks. Some believe Senate confirmation for the director could bring sweeping change and more accountability to the ultrasecretive NSA. But it also threatens to subject the agency to public political showdowns and delays — which the Obama administration has said it wants to avoid. “Given the enormous power of the NSA and its important mission, I certainly am open to the idea of having the director being a confirmed position,” Rep. Jim Langevin (D-R.I.) said, adding: “The more oversight we have, the better.” The confirmation concept is one of several NSA reforms under serious consideration on Capitol Hill. Administration officials also have weighed whether to split leadership of the NSA away from U.S. Cyber Command — both currently led by Gen. Keith Alexander, who’s slated to depart in 2014. Such a change could forge the way for a civilian to head the NSA for the first time. For his part, Alexander has had some vetting by Congress. The Senate approved his nomination to lead CyberCom, the Pentagon’s cyberwar forces, in 2010. And the chamber approved the general’s third star before he was tapped for the NSA post in 2005. But much has changed during his record-setting tenure of eight years at the NSA, including once-unthinkable leaks about the agency’s sprawling phone record and Internet surveillance programs. As he prepares to depart the government, some members of Congress see an opportunity to rethink the agency’s future — not to mention lawmakers’ role in overseeing it. Feinstein’s new surveillance reform bill — widely panned by civil-liberties advocates as weak — contains a provision ensuring that future NSA directors obtain the Senate’s so-called advice and consent. That requirement has even drawn the backing of her bill’s opponents, including Sen. Mark Udall (D-Colo.), whose spokesman told POLITICO that Senate confirmation of NSA directors is a “long overdue measure.” And another Senate proposal, which would authorize all of the intelligence community’s activities in 2014, includes a similar confirmation mandate. That cleared Feinstein’s committee last week. However, the idea long has left a sour taste at the White House. When Feinstein’s intelligence committee counterpart in the House — Rep. Mike Rogers (R-Mich.) — tried to advance a measure that included NSA confirmation in 2011, the White House said it “strongly objects” to the change. The reason: “The administration believes that if this provision were to become law, a critical national security position would likely remain unfilled for a significant period of time, adversely impacting the management and function of the National Security Agency.” The White House declined to comment on the issue. Such a move could mean more oversight for future directors of the NSA. The confirmation process would permit two key congressional panels — Feinstein’s intelligence committee and the Senate’s top defense committee — to get a crack at questioning the NSA nominee, one intelligence aide told POLITICO. In fact, the two committees already have worked out an initial plan to ensure they can share that crucial role, the aide added. And that’s all before a vote by the full Senate, which historically has held up federal candidates when lawmakers want documents or answers from the White House. Feinstein’s plan also might serve as a signal to the White House. One former senior intelligence official told POLITICO it’s designed to ensure that the Senate gets the chance to confirm a civilian nominee, should the administration choose to go that route. A civilian NSA director would make waves at the Pentagon, where Alexander always has worn “dual hats” leading both the NSA and CyberCom. The general himself told POLITICO in October he firmly believes one director should run both entities given their overlap in mission and close proximity, with the two based at Fort Meade in Maryland.

#### Obama just caved to Congress and restricted the NSA- triggers their losers lose argument

Nakashima and Miller 1/17 ( Ellen Nakashima and Greg Miller, Washington Post, “Obama calls for significant changes in collection of phone records of U.S. citizens”, <http://www.washingtonpost.com/politics/in-speech-obama-to-call-for-restructuring-of-nsas-surveillance-program/2014/01/17/e9d5a8ba-7f6e-11e3-95c6-0a7aa80874bc_story.html?tid=ts_carousel>, January 17, 2014)

President Obama on Friday made a forceful call to narrow the government’s access to millions of Americans’ phone records as part of an overhaul of surveillance activities that have raised concerns about official overreach. The president said he no longer wants the National Security Agency to maintain a database of such records. But he left the creation of a new system to subordinates and lawmakers, many of whom are divided on the need for reform. In a speech at the Justice Department, Obama ordered several immediate steps to limit the NSA program that collects domestic phone records, one of the surveillance practices that was exposed last year by former intelligence contractor Edward Snowden. Obama directed that from now on, the government must obtain a court order for each phone number it wants to query in its database of records. Analysts will be able to review phone calls that are two steps removed from a number associated with a terrorist organization instead of three. And he ordered a halt to eavesdropping on dozens of foreign leaders and governments that are friends or allies. The changes, White House officials said, mark the first significant constraints imposed by the Obama administration on surveillance programs that expanded dramatically in the decade after the Sept. 11, 2001 attacks. But the most significant change he called for, to remove the phone database from government hands, could take months if not longer to implement. And already critics from diverse camps — in Congress and outside it — are warning that what he has called for may be unworkable. Obama is retaining the vast majority of intelligence programs and capabilities that came to light over the past six months in a deluge of reports based on leaked documents. Even the most controversial capability — the government’s access to bulk telephone records, known as metadata — may well be preserved, although with tighter controls and with the records in the hands of some outside entity. The database holds phone numbers and call lengths and times, but not actual phone call content. Obama recognized that others have raised alternatives, such as the moving custodianship of the records to the phone companies or an independent third party — and that such plans face significant logistical and political hurdles. He gave subordinates including Attorney General Eric H. Holder Jr. until March 28 to develop a plan to “transition” the bulk data out of the possession of the government. Existing authorities for the phone records program are set to expire on that date, requiring a reauthorization by the Foreign Intelligence Surveillance Court (FISC). Both in his speech and in the specifics of his plan, Obama straddled competing security and civil liberties imperatives. His proposals are aimed at containing a public backlash triggered by Snowden, but also preserving capabilities that U.S. intelligence officials consider critical to preventing another terrorist attack. [Read the text of Obama’s speech.] Reaction to Obama’s call to end the phone records collection was mixed and underscored the political challenge he faces in achieving his goal. The chairmen of the House and Senate intelligence committees issued a joint statement focusing on Obama’s remarks that “underscored the importance of using telephone metadata to rapidly identify possible terrorist plots.” Sen. Dianne Feinstein (D-Calif.) and Rep. Mike Rogers (R-Mich.) added that they have reviewed the existing NSA bulk collection program and “found it to be legal and effective,” indicating they would oppose efforts to end it. “Ending this dragnet collection will go a long way toward restoring Americans’ constitutional rights and rebuilding the public’s trust,” Sens. Ron Wyden (D-Ore.), Mark Udall (D-Colo.) and Martin Heinrich (D-N.M.) said in a joint statement. “Make no mistake, this is a major milestone in our longstanding efforts to reform the National Security Agency’s bulk collection program.” Adam B. Schiff (D-Calif.), a House Intelligence Committee member who opposes bulk collection, said he thought that ultimately the NSA would have to transition to a model in which the government seeks data from individual phone companies, without forcing the companies to hold the data for longer than they do now. But many civil liberties groups said Obama failed to advance real reform by leaving open the door to third-party storage of records and data retention mandates. “He doesn’t commit to ending the bulk data collection of telephone records,” said Anthony Romero, executive director of the American Civil Liberties Union. “He gets close to understanding the concerns, but he backs away from the real reform, which is to end the bulk data collection. He gets to the finish line, but he doesn’t cross it.” Romero said he was trying to bridge irreconcilable positions: “Clearly this is a president who wants to agree with the criticism of the bulk data collection and retention, and yet wishes to retain that power notwithstanding the serious concerns,” Romero said. “And you can’t have it both ways.” John McLaughlin, a former CIA deputy director, said Obama “was trying to find a midway here.” Obama’s dilemma, he said, is responding to dual challenges: the perception that the program might one day be abused, and the reality that al-Qaeda and its affiliates are growing stronger. “So as president, he’s got to think, ‘I don’t want to take any chances here.’ ” Obama also called on Congress to establish a panel of public advocates who can represent privacy interests before the FISC, which hears government applications for surveillance in secret. Obama has instructed Holder to reform the use of national security letters — a form of administrative subpoena used to obtain business and other records — so that the traditional gag order that accompanies them does not remain in place indefinitely. But he did not, as has been recommended by a White House review panel, require judicial approval for issuance of the letters. The president also addressed another major NSA surveillance program, which involves collection of e-mail and phone calls of foreign targets located overseas, including when they are in contact with U.S. citizens or residents. He acknowledged that the information has been valuable, but directed subordinates to develop new protections for the information collected on U.S. persons. He also said he will order that certain privacy safeguards given Americans whose data are collected be extended to foreigners, including limits on the use of the information and how long it can be kept. Accompanying his speech, Obama issued a new directive Friday that states that the United States will use signals intelligence only “for legitimate national security purposes, and not for the purpose of indiscriminately reviewing the e-mails or phone calls of ordinary people.” It says that authorities will not collect intelligence “to suppress criticism or dissent” or to give U.S. companies a competitive advantage. Unless there is a compelling national security purpose, Obama said, “we will not monitor the communications of heads of state and government of our close friends and allies.” Friendly leaders “deserve to know that if I want to learn what they think about an issue, I will pick up the phone and call them, rather than turning to surveillance,” he said. As he made the case for reforms, Obama also cautioned that “we cannot unilaterally disarm our intelligence agencies.” And he caustically criticized foreign intelligence services that “feign surprise” over disclosures of U.S. surveillance while “constantly probing our government and private sector networks and accelerating programs to listen to our conversations, intercept our e-mails or compromise our systems.” He noted that some countries that “have loudly criticized the NSA privately acknowledge that America has special responsibilities as the world’s only superpower . . . and that they themselves have relied on the information we obtain to protect their own people.” Expressing frustration at those who “assume the worst motives by our government,” Obama said at another point in his speech: “No one expects China to have an open debate about their surveillance programs, or Russia to take privacy concerns of citizens in other places into account.” But he said the United States is held to a higher standard “precisely because we have been at the forefront in defending personal privacy and human dignity.” The president’s speech comes after months of revelations about the breadth and secrecy of the NSA’s surveillance activities, based on hundreds of thousands of documents taken by Snowden. New revelations based on the documents are expected to continue this year.

### 2AC- Key

The GOP doesn’t need the plan to discredit Obama’s push—he lacks capital and a slew of other issues could be exploited

Earl Hutchinson, MSNBC Contributor, 1/12/14, Overplaying President Obama’s supposed second term hex, www.philasun.com/news/5063/57/Overplaying-President-Obama-s-supposed-second-term-hex.html

President Barack Obama’s slumping approval numbers seem to confirm the belief that second term presidents run into trouble, sometimes big trouble, in trying to hold it together during their second term. In Obama’s case, the NSA spy debacle, **the lingering anger over** Benghazi, the AP leaks, and the big contentious issue, the worry over the Affordable Health Care Act website glitches and possible rising insurance costs has raised **deep concerns** that the supposed two term hex will make his administration **even more vulnerable** to GOP attacks. Obama’s numbers seemingly aren’t good in comparison with other recent presidents. In a recent CNN poll that measured presidential approval ratings immediately after their reelection, George W. Bush stood at 41 percent a year after his reelection. Bill Clinton stood at 56 percent and Ronald Reagan stood at 63 percent in the year after their reelection. But Obama’s alleged bungles hardly add up to an indelible second term curse. Past presidents have certainly had their share of second term woes. This was the case with Eisenhower, Nixon, of course, Reagan, George H.W. Bush, Clinton and George W. Bush. This shouldn’t surprise. They were in office for a relatively long time. They run a big sprawling government with thousands of appointees and personnel. It is simply beyond the pale of one person to control every facet and decision their appointees and personnel make. Just as time can work for a second term president, it can also work against him too. The longer he’s in office, **it’s** almost **assured that some issue**, event, or catastrophe **will happen that can mar a president’s image, and that he may** or may **not have any real control over**. The uncontrollable factors are a recession, a cataclysmic natural or human made disaster, or a major scandal. These are tests and the public watches closely to see how a president handles the situation. A real or perceived fumble will quickly taint him as a man that’s incapable of handling a crisis. The president’s popularity ratings just as quickly tumble when that happens. Then there’s the other party. **It has an inherent vested interest in seeing a president stumble**. **The GOP has gone much further to hammer Obama**. It has not been content to sit back and wait for a crisis or policy flub to embroil his administration. It’s done everything humanly possible to try to insure that Obama is a failed president, even announcing that that’s its sworn aim. That mission started long before the GOP went to war against him over the health care act, the budget, the deficit, the debt limit, appointments, unemployment insurance extension, and job creation programs. **Any initiative no matter how picayune has been fair game in the GOP’s campaign of** delay, **hectoring and obstruction of Obama’s program**. It’s no accident that more often than not a president’s party will lose control over one sometimes both houses of Congress after a president’s triumphant reelection bid. Obama is no exception. The GOP solidified its control of the House in the 2010 mid-term elections. That’s been a launch pad for its prolonged campaign to torpedo virtually every Obama legislative initiative. The game plan is to take back the Senate in 2014 and render Obama’s legislative program on immigration and tax reform during the remainder of his term a shambles.

### 2AC- Laundry List

#### Laundry list thumps- elections, trade, budget, energy and Podesta nomination

Peckingpaugh et al. 1/16 (Tim L. Peckinpaugh (Partner of K&L Law Firm- focus on Energy), Darrell L. Conner (Government Affairs Counselor), Sean P. McGlynn (Government Affairs Analyst), “2014 Legislative & Regulatory Outlook”, <http://www.klgates.com/2014-legislative--regulatory-outlook-01-16-2014/>, January 16, 2014)

As this memo makes clear, the combined factors of the 2013 budget deal, the recent Senate rules changes, and the appointment of John Podesta would seem to increase the likelihood for both legislative and regulatory action even during an election year. While it’s certainly reasonable to expect that legislative and regulatory action may begin to slow as Congress gets closer to the election in November, it’s important to engage lawmakers and regulators early in 2014 to ensure that you are influencing the policymaking process when it matters most and before it is too far developed. And remember, there is always the possibility – if not an almost certainty – that a lame duck session will occur to complete Congressional work in 2014.

### AT: MW Willis Evidence

#### Their link card concludes aff- winners win k2 Obama agenda

Lillis and Wasson, The Hill, 9-7-13

(Mike and Erik, “Fears of wounding Obama weigh heavily on Democrats ahead of vote,” http://thehill.com/homenews/house/320829-fears-of-wounding-obama-weigh-heavily-on-democrats, accessed 9-15-13, CMM)

The prospect of wounding President Obama is weighing heavily on Democratic lawmakers as they decide their votes on Syria.¶ Obama needs all the political capital he can muster heading into bruising battles with the GOP over fiscal spending and the debt ceiling.¶ Democrats want Obama to use his popularity to reverse automatic spending cuts already in effect and pay for new economic stimulus measures through higher taxes on the wealthy and on multinational companies.¶ But if the request for authorization for Syria military strikes is rebuffed, some fear it could limit Obama's power in those high-stakes fights.¶ That has left Democrats with an agonizing decision: vote "no" on Syria and possibly encourage more chemical attacks while weakening their president, or vote "yes" and risk another war in the Middle East.¶ “I’m sure a lot of people are focused on the political ramifications,” a House Democratic aide said.¶ Rep. Jim Moran (D-Va.), a veteran appropriator, said the failure of the Syria resolution would diminish Obama's leverage in the fiscal battles.¶ "It doesn't help him," Moran said Friday by phone. "We need a maximally strong president to get us through this fiscal thicket. These are going to be very difficult votes."¶ “Clearly a loss is a loss,” a Senate Democratic aide noted.¶ Publicly, senior party members are seeking to put a firewall between a failed Syria vote — one that Democrats might have a hand in — and fiscal matters.¶ Rep. Gerry Connolly (D-Va.) said Friday that the fear of damaging Obama just eight months into his second term "probably is in the back of people's minds" heading into the Syria vote. But the issue has not percolated enough to influence the debate.¶ "So far it hasn't surfaced in people's thinking explicitly," Connolly told MSNBC. "People have pretty much been dealing with the merits of the case, not about the politics of it — on our side."¶ Moran said he doesn't think the political aftershocks would be the “deciding factor” in their Syria votes.¶ "I rather doubt that most of my colleagues are looking at the bigger picture," he said, "and even if they were, I don't think it would be the deciding factor."¶ Moran said the odds of passing the measure in the House looked slim as of Friday.¶ Other Democrats are arguing that the Syria vote should be viewed in isolation from other matters before Congress.¶ “I think it’s important each of these major issues be decided on its own — including this one,” Rep. Sander Levin (Mich.), senior Democrat on the House Ways and Means Committee, said Friday.¶ With Obama scheduled to address the country Tuesday night, several Democrats said the fate of the Syria vote could very well hinge on the president's ability to change public opinion.¶ “This is going to be a fireside chat, somewhat like it was in the Thirties," Levin said. "I wasn’t old enough to know, one has to remember how difficult it was for President Roosevelt in WWII."¶ Rep. Elijah Cummings (D-Md.), who remains undecided on the Syria question, agreed.¶ "It's very, very important that the case for involvement in Syria not only be made to the members of Congress and the Senate, but it must also be made to the American people," Cummings said Friday in the Capitol.¶ Still other Democrats, meanwhile, are arguing that the ripple effects of a Syria vote are simply too complicated to game out in advance. Some said the GOP has shown little indication it will advance Obama’s agenda even after his reelection, so a Syria failure would do little damage.¶ “There is a constant wounding [of Obama] going on with the Tea Party on budgets, appropriations and the debt ceiling,” said Rep. Sheila Jackson Lee (D-Texas). “I am going to reach out to my colleagues, Tea Party or not, and ask is this really the way you want to project the political process?”¶ Jackson Lee said using Syria to score political points would be “frolicking and frivolity” by the Tea Party.¶ Yet others see a more serious threat to the Democrats' legislative agenda if the Syria vote fails.¶ A Democratic leadership aide argued that Republicans — some of whom are already fundraising on their opposition to the proposed Syria strikes — would only be emboldened in their fight against Obama's agenda if Congress shoots down the use-of-force resolution.¶ "It's just going to make things harder to do in Congress, that's for sure," the aide said Friday.¶ But other aides said Obama could also double down on fighting the cuts from sequestration if he becomes desperate for a win after Syria, and the net effect could be positive.¶ A leading Republican strategist echoed that idea.¶ “Should the President lose the vote in Congress, he will be severely weakened in the eyes of public opinion, the media, the international crowd and the legislative branch," The Hill columnist John Feehery said Friday on his blog.

THEIR CARD ENDS

"Unless he wants to take the rest of his Presidency off and leave the keys with Harry Reid, that means he will have to show that he is still relevant to the process, which means he will need to somehow get a victory in the debt limit/appropriations battles that are now coming close to being engaged."

### Warfighting

#### Turn- the aff *focuses* NSA on foreign intel- increases capabilities

Clarke et al. ’13 (Richard A. Clarke (Clarke served the last three Presidents as a senior White House Advisor. Over the course of an unprecedented 11 consecutive years of White House service, he held the titles of: - Special Assistant to the President for Global Affairs - National Coordinator for Security and Counterterrorism - Special Advisor to the President for Cyber Security Prior to his White House years, Clarke served for 19 years in the Pentagon, the Intelligence Community, and State Department. During the Reagan Administration, he was Deputy Assistant Secretary of State for Intelligence. During the Bush (41) Administration, he was Assistant Secretary of State for Political-Military Affairs and coordinated diplomatic efforts to support the 1990–1991 Gulf War and the subsequent security arrangements. As a Partner in Good Harbor Consulting, LLC, Clarke advises clients on a range of issues including: - Corporate security risk management - Information security technology - Dealing with the Federal Government on security and IT issues - Counterterrorism In a Special Report by Foreign Policy Magazine, Clarke was chosen as one of The Top 100 Global Thinkers of 2010, Council on Foreign Relations, Former international affairs fellow in residence), Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, Peter Swire, “Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies”, <http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>, December 12, 2013)

B. The National Security Agency We recommend major changes to the structure of the National Security Agency. There should be greater civilian control over the agency, including Senate confirmation for the Director and openness to having a civilian Director. NSA should refocus on its core function: the collection and use of foreign intelligence information. To distinguish the warfighting role from the intelligence role, the military Cyber-Command should not be led by the NSA Director. Because the defense of both civilian and government cyber-systems has become more important in recent years, we recommend splitting the defensive mission of NSA’s Information Assurance Directorate into a separate organization. Before discussing these recommendations, we offer some general observations. No other organization in the world has the breadth and depth of capabilities NSA possesses; its prowess in the realm of signals intelligence is extraordinary. Since World War II, NSA and its predecessors have worked to keep our nation and our allies safe from attack. SIGINT collected by NSA is used daily to support our warfighters and to combat terrorism, the proliferation of weapons of mass destruction, and international criminal and narcotics cartels. Its successes make it possible for the United States and our allies around the world to safeguard our citizens and prevent death, disaster, and destruction. In addition to its leading-edge technological developments and operations, NSA employs large numbers of highly trained, qualified, and professional staff. The hard work and dedication to mission of NSA’s workforce is apparent. NSA has increased the staff in its compliance office and addressed many concerns expressed previously by the FISC and others. After the terrorist acts in the United States of September 11, 2001, many people in both the Legislative and Executive Branches of government believed that substantial new measures were needed to protect our national security. We have noted that if a similar or worse incident or series of attacks were to occur in the future, many Americans, in the fear and heat of the moment, might support new restrictions on civil liberties and privacy. The powerful existing and potential capabilities of our intelligence and law enforcement agencies might be unleashed without adequate controls. Once unleashed, it could be difficult to roll back these sacrifices of freedom. Our recommendations about NSA are designed in part to create checks and balances that would make it more difficult in the future to impose excessive government surveillance. Of course, no structural reforms create perfect safeguards. But it is possible to make restraint more likely. Vigilance is required in every age to maintain liberty

## 1AR

### Fetweis

#### Heg doesn’t solve conflict

**Fettweis 10** – Professor of national security affairs @ U.S. Naval War College (Chris, Georgetown University Press, “Dangerous times?: the international politics of great power peace” 173-75)

Simply stated, the hegemonic stability theory proposes that international peace is only possible when there is one country strong enough to make and enforce a set of rules. At the height of Pax Romana between 27 BC and 180 AD, for example, Rome was able to bring unprecedented peace and security to the Mediterranean. The Pax Britannica of the nineteenth century brought a level of stability to the high seas. Perhaps the current era is peaceful because the United States has established a de facto Pax Americana where no power is strong enough to challenge its dominance, and because it has established a set of rules that a generally in the interests of all countries to follow. Without a benevolent hegemony, some strategists fear, instability may break out around the globe. Unchecked conflicts could cause humanitarian disaster and, in today’s interconnected world economic turmoil that would ripple throughout global financial markets. If the United States were to abandon its commitments abroad, argued Art, the world would “become a more dangerous place” and, sooner or later, that would “rebound to America’s detriment.” If the massive spending that the United States engages in actually produces stability in the international political and economic systems, then perhaps internationalism is worthwhile. There are good theoretical and empirical reasons, however, the belief that U.S. hegemony is not the primary cause of the current era of stability. First of all, the hegemonic stability argument overstates the role that the United States plays in the system. No country is strong enough to police the world on its own. The only way there can be stability in the community of great powers is if self-policing occurs, ifs **states have decided that their interest are served by peace**. **If no pacific normative shift had occurred** among the great powers that was filtering down through the system, then **no amount of** international constabulary **work** by the United States **could maintain stability**. Likewise, if it is true that such a shift has occurred, then most of what the hegemon spends to bring stability would be wasted. The 5 percent of the world’s population that live in the United States simple could not force peace upon an unwilling 95. At the risk of beating the metaphor to death, the United States may be patrolling a neighborhood that has already rid itself of crime. Stability and unipolarity may be simply **coincidental**. In order for U.S. hegemony to be the reason for global stability, the rest of the world would have to expect reward for good behavior and fear punishment for bad. Since the end of the Cold War, the United States has not always proven to be especially eager to engage in humanitarian interventions abroad. Even rather incontrovertible evidence of genocide has not been sufficient to inspire action. Hegemonic stability can only take credit for influence those decisions that would have ended in war without the presence, whether physical or psychological, of the United States. Ethiopia and Eritrea are hardly the only states that could go to war without the slightest threat of U.S. intervention. Since most of the world today is free to fight without U.S. involvement, something else must be at work. Stability exists in many places where no hegemony is present. Second, the limited **empirical evidence** we have **suggests** that there is **little connection between** the relative level of U.S. **activism and** international **stability**. During the 1990s the United States cut back on its defense spending fairly substantially, By 1998 the United States was spending $100 billion less on defense in real terms than it had in 1990. **To** internationalists, defense hawks, and other **believers in hegemonic stability this** irresponsible "peace dividend" **endangered** both national and **global security "**No serious analyst of American military capabilities," argued Kristol and Kagan, "doubts that the defense budget has been cut much too far to meet Americas responsibilities to itself and to world peace."" If the pacific trends were due not to U.S. hegemony but a strengthening norm against interstate war, however, one would not have expected an increase in global instability and violence. The verdict from the past two decades is fairly plain: **The world grew more peaceful** while the United States cut its forces. **No state** **seemed to believe** that its **security was endangered** by a less-capable Pentagon, **or** at least none **took any action** that would suggest such a belief. No militaries were enhanced to address power vacuums; **no** **security dilemmas drove mistrust and arms races; no regional balancing occurred** once the stabilizing presence of the U.S. military was diminished. The rest of the world acted as if the threat ofinternational war was not a pressing concern, despite the reduction in U.S. capabilities. The incidence and magnitude of global conflict declined while the United States cut its military spending under President Clinton, and it kept declining as the Bush Administration ramped spending back up. No complex statistical analysis should be necessary to reach the conclusion that the two are unrelated. It is also worth noting for our purposes that the United States was no less safe. Military spending figures by themselves are insufficient to disprove a connection between overall U.S. actions and international stability. Once again, one could presumably argue that spending is not the only or even the best indication of hegemony, and that it is instead U.S. foreign political and security commitments that maintain stability. Since neither was significantly altered during this period, instability should not have been expected. Alternately, advocates of hegemonic stability could believe that relative rather than absolute spending is decisive in bringing peace. Although the United States cut back on its spending during the 1990s, its relative advantage never wavered. However, even if it is true that either U.S. commitments or relative spending account for global pacific trends, then at the very least stability can evidently be maintained at drastically lower levels of both. In other words, even if one can be allowed to argue in the alternative for a moment and suppose that there is in fact a level of engagement below which the United States cannot drop without increasing international disorder, a rational grand strategist would still recommend cutting back on engagement and spending until that level is determined. Grand strategic decisions are never final; continual adjustments can and must be made as time goes on. Basic logic suggests that the United States ought to spend the minimum amount of its blood and treasure while seeking the maximum return on its investment. And if the current era of stability is as stable as many believe it to be, no increase in conflict would ever occur irrespective of U.S. spending, which would save untold trillions for an increasingly debt-ridden nation. It is also perhaps worth noting that if opposite trends had unfolded, if other states had reacted to news of cuts in U.S. defense spending with more aggressive or insecure behavior, then internationalists would surely argue that their expectations had been fulfilled. If increases in conflict would have been interpreted as proof of the wisdom of internationalist strategies, then logical consistency demands that the lack thereof should at least pose a problem. As it stands, the only evidence we have regarding the likely systemic reaction to a more restrained United States suggests that the current peaceful trends are **unrelated** to U.S. military spending. Evidently **the rest of the world can operate** quite **effectively without the presence of a global policeman**. **Those who think otherwise base their view on faith alone.**

### China

#### Case turns China

Blair ’13 (Eric Blair, Activist Post, “Does Obama Need Congress to Declare Cyber War on China?”, <http://www.activistpost.com/2013/02/does-obama-need-congress-to-declare.html>, February 20, 2013)

The whole world is a battlefield for the U.S. war machine and the Internet is its new favorite weapon. Anonymous officials in the U.S. government leaked today that it is set to go on the offensive in the cyberwar against China in retaliation for alleged state-run cyberattacks against U.S. interests. The Associated Press reports that the US is ready to strike back against China: As public evidence mounts that the Chinese military is responsible for stealing massive amounts of U.S. government data and corporate trade secrets, the Obama administration is eyeing fines and other trade actions it may take against Beijing or any other country guilty of cyberespionage. According to officials familiar with the plans, the White House will lay out a new report Wednesday that suggests initial, more-aggressive steps the U.S. would take in response to what top authorities say has been an unrelenting campaign of cyberstealing linked to the Chinese government. The officials spoke on condition of anonymity because they were not authorized to speak publicly about the threatened action. Even if we are to assume what the anonymous officials are saying is true, where's the proof? The supposed paper of record the New York Times broke the story yesterday that cyber attacks appearing to originate in China came from a building occupied by China's People's Liberation Army's Unit 61398. NYT writes: A growing body of digital forensic evidence — confirmed by American intelligence officials who say they have tapped into the activity of the army unit for years — leaves little doubt that an overwhelming percentage of the attacks on American corporations, organizations and government agencies originate in and around the white tower. As warlike tensions mount with China, it can't be ignored that the very same paper of record ran false "weapons of mass destruction" stories to push for war in Iraq. Those, too, were famously planted by anonymous officials and experts close to the "evidence". This latest evidence inciting a more-aggressive response from the U.S. comes from a report put together by the computer security firm Mandiant. Mandiant has been called "The Go-To Security Firm" for cyber attacks. Their $100 million in revenue is up 76% from last year and they count 30 percent of the Fortune 100 as clients -- conveniently including The New York Times who sought their help during its supposed hacking by China. Mandiant's report on China concludes; "Either Unit 61398 is responsible for the persistent attacks or they are being done by a secret organization of Chinese speakers with direct access to the Shanghai telecommunications infrastructure who are engaged in a multi-year espionage campaign being run right outside the military unit's gates." Some are saying it's an attack bigger than September 11th. “I call it cyberterrorism that makes 9/11 pale in comparison,” Rep. Mike Rogers (R-Mich), told NBC News. But what evidence and damages can be proven that can compare with the devastation and death on 9/11? In an effort to provide compelling evidence Mandiant produces a video that shows, as a private security company, their creepy ability to completely shadow Internet users: This all appears very damning for China and these alleged hackers, but it begs the questions, how is Mandiant allowed to spy on Internet users so thoroughly? Do they have the authority to do that to Americans? Who gave them this authority and with what oversight? And, as a final observation, this video can be easily staged with another compliant actor instead of a genuine hacker threat. It really proves nothing, just like Scooter Libby's fake Yellow-Cake-from-Niger document proved nothing when NYT's Judith Miller printed it, but it still led to war. This new threat is clearly being used for several purposes. First, it serves to justify Obama's urgency in bypassing Congress by signing his cybsecurity executive order. Second, it comes right when the privacy-killing cybersecurity legislation CISPA is headed to the Senate for another contentious vote after having failed in two previous attempts. Third, it warrants expanding cyber surveillance contracts to Mandiant and others, and increases in U.S. Cyber Command personnel. For some advantageous lawmakers like Sen. Dianne Feinstein (D-Calif) it requires global governance for the Internet to police these threats. Feinstein told the AP that "the report reinforces the need for international agreements that prohibit cybercrimes and have a workable enforcement mechanism." Clearly there is an agenda of controlling the Internet working in the background of these threats. And given the government's history of lying to get us into wars that only benefit the military-industrial complex, I remain skeptical of the severity of the cyber threat. However, the establishment is taking this quite seriously and it may lead to a cyberwar if not outright war. So it seems Americans should be asking the most obvious question: What is Congress' role in overseeing cyberwars? If Obama is set to take "more-aggressive steps" in an escalating cyberwar with China including offensive action, then it seems that the War Powers Clause of the U.S. Constitution which vests in the Congress the power to declare war comes into play. Perhaps I'm just speaking into the wilderness since the executive branch has been ignoring this clause for decades. However, it would be nice to know whether the people's representatives (sic) have any say in who we declare cyberwar on because any type of war can quickly lead to bullets and bombs.

### MW Impact Re-Cut

#### Their impact card concludes failure of Obama ienvitable

Leverett, Penn State IR prof, and Leverett, American University, 12

(Flynt and Hillary Mann, 7-5-12. “America’s Iran Policy and the Undermining of International Order,” http://www.worldfinancialreview.com/?p=3490, accessed 11-18-13, CMM)

Second, secondary sanctions are a political house of cards. American officials are well aware of their presumptive illegality. Successive U.S. administrations have been reluctant to impose them on non-U.S. entities transacting with Iran, precisely to avoid formal challenges at the WTO. U.S. secondary sanctions are, in effect, an enormous bluff, leveraging the specter of legal and reputational risk in America to bully companies and banks in third countries to stop transacting with Iran, but without pulling the trigger on the threat to punish those that continue doing business in Iran. ¶ The UK and European sanctions now facing legal challenges are a product of this bullying campaign. For over a decade, the EU has condemned America’s threatened ‘extraterritorial’ application of national trade law, warning it would go to the WTO if Washington ever sanctioned European companies over Iran-related business. Over the last several years, though, enough British and European businesses stopped transacting with Iran that the EU was no longer under pressure to defend European commercial interests and could begin subordinating its Iran policy to American preferences. By last year, it has imposed a nearly comprehensive economic embargo against the Islamic Republic. ¶ While Europe has surrendered on having an independent Iran policy, the U.S. bluff on secondary sanctions will soon be called, most likely by China. To be sure, Beijing does not seek confrontation with America over Iran, and has sought to accommodate Washington in many ways—e.g., by not developing trade and investment positions in the Islamic Republic as rapidly as it might have, and by shifting some Iran-related transactional flows into renminbi to help the Obama administration avoid sanctioning Chinese banks. While China’s imports of Iranian oil appear, in the aggregate, to be growing, Beijing reduces them when the administration is deciding about six-month sanctions waivers for countries buying Iranian crude. ¶ The Obama administration, for its part, continues giving China sanctions waivers; the one Chinese bank barred from America for Iran-related transactions is a Chinese energy company subsidiary with no U.S. business. But as Congress legislates more secondary sanctions, Obama’s room to maneuver is shrinking. ¶ Obama will soon be in the position of demanding that China cut Iranian oil imports in ways that would harm its economy, and that Chinese banks stop virtually all Iran-related transactions. Beijing will not be able to accommodate such radical demands; it will have to say ‘no’, putting Obama in a classic lose-lose situation. ¶ “If America wants a nuclear deal grounded in the NPT, Hassan Rohani is an ideal interlocutor. But this would require Washington to bring its own policy in line with the NPT.” Obama could retreat. But then the world will know that secondary sanctions are a bluff, undercutting their deterrent effect. Alternatively, he could sanction major Chinese firms and banks. But that will force Beijing to respond—at least by taking America to the WTO (where China will win), perhaps by retaliating against U.S. companies. At this point, Beijing has more ways to impose costs on America for violations of international economic law impinging on Chinese interests than Washington has levers to coerce Chinese compliance with U.S. policy preferences. America and its partners will not come out ahead in this scenario. ¶ Third, U.S. secondary sanctions accelerate the shift of economic power from West to East. As non-Western economies surpass more Western countries in their relative importance to the global economy, America has a strong interest in keeping non-Western states tied to established, U.S.-dominated mechanisms for conducting, financing, and settling international transactions. Secondary sanctions, though, push in the opposite direction, incentivizing emerging powers to speed up development of non-Western alternatives to existing transactional platforms. ¶ “Strategic recovery will also entail reversing Washington’s reliance on secondary sanctions—not because of Iranian surrender (which won’t be forthcoming), but because they delegitimize America’s claim to continuing leadership in international economic affairs.” ¶ This trend will diminish Western influence in myriad ways—e.g., reducing the dollar’s role as a transactional currency, lowering the share of cross-border commodity trades on New York and London exchanges, and shrinking the global near-monopoly of Western-based reinsurance companies and P&I clubs. Add the cost of a U.S.-instigated trade dust-up with China, and the self-damaging quality of America’s dysfunctional Iran policy becomes even clearer. ¶ Finding a New Approach ¶ Putting America on a better strategic trajectory will take thoroughgoing revision of its Iran policy. In this regard, the election of Hassan Rohani—who ran the Islamic Republic’s Supreme National Security Council for sixteen years, was its chief nuclear negotiator during 2003-2005, and holds advanced degrees in Islamic law and civil law—as Iran’s next president is an opportunity. If America wants a nuclear deal grounded in the NPT, Rohani is an ideal interlocutor. But this would require Washington to bring its own policy in line with the NPT—first of all, by acknowledging Iran’s right to safeguarded enrichment. ¶ Strategic recovery will also entail reversing Washington’s reliance on secondary sanctions—not because of Iranian surrender (which won’t be forthcoming), but because they delegitimize America’s claim to continuing leadership in international economic affairs. This, however, is even more difficult than revising the U.S. position on Iranian enrichment—for Congress has legislated conditions for lifting sanctions that stipulate Iran’s abandonment of all alleged WMD activities, cutting all ties to those Washington deems terrorists, and political transformation. Overcoming this will require Obama to do what President Nixon did to enable America’s historic breakthrough with China—going to Tehran, strategically if not physically, to accept a previously demonised political order as a legitimate entity representing legitimate national interests. ¶ None of this is particularly likely. But if America doesn’t do these things, it condemns itself to a future as an increasingly failing, and flailing, superpower—and as an obstacle, rather than a facilitator, of rules-based international order.

#### Their card concludes American sanctions collapsing now

Leverett, Penn State IR prof, and Leverett, American University, 12

(Flynt and Hillary Mann, 7-5-12. “America’s Iran Policy and the Undermining of International Order,” http://www.worldfinancialreview.com/?p=3490, accessed 11-18-13, CMM)

Notwithstanding Washington’s drive to enact ever more sanctions against Tehran, the edifice of U.S. sanctions policy is collapsing. In June, Britain’s supreme court ordered the Treasury to lift sanctions imposed by Her Majesty’s Government on the Iranian Bank Mellat. Earlier this year, Europe’s [General Court](http://curia.europa.eu/juris/fiche.jsf?id=T%3B496%3B10%3BRD%3B1%3BP%3B1%3BT2010%2F0496%2FJ&pro=&lgrec=en&nat=&oqp=&dates=&lg=&language=en&jur=C%2CT%2CF&cit=none%2CC%2CCJ%2CR%2C2008E%2C%2C%2C%2C%2C%2C%2C%2C%2C%2Ctrue%2Cfalse%2Cfalse&num=T-496%2F10&td=ALL&pcs=O&avg=&mat=or&jge=&for=&cid=1270743) overturned European sanctions against Bank Mellat and another Iranian bank. More banks and other pillars of Iran’s economy, like the National Iranian Oil Company, are now contesting their sanctioned status in European courts. These cases directly challenge European sanctions against Iran (whether imposed nationally or by the EU). They also threaten the whole web of U.S.-instigated sanctions that has expanded dramatically since Obama’s accession in 2009.

America has, for three decades, put unilateral sanctions on the Islamic Republic—over its alleged pursuit of WMD, support for groups that Washington labels terrorist organisations, and its domestic governance. Six of the seven Security Council resolutions on the nuclear issue authorize multilateral sanctions against Iran. But neither unilateral nor UN measures have had decisive impact on Iran’s economy or decision-making: even a superpower’s unilateral sanctions don’t work if other countries won’t replicate them, and China and Russia ensure that UN sanctions don’t impinge on their most important interests with Iran.

Besides unilateral and multilateral measures, America has, since 1996, threatened to impose ‘secondary’ sanctions on third-country entities doing business with Iran. Secondary sanctions now cover most commercial activities, including investment in and provision of services to Iran’s hydrocarbon and shipping sectors, buying Iranian crude oil, and virtually all financial transactions. The penalties that can be levied now include being cut off from the U.S. financial system.

America’s increasing reliance on secondary sanctions in its Iran policy is ultimately self-defeating in at least three significant ways.

First, secondary sanctions are a legal house of cards. The UK and EU sanctions challenged by targeted Iranian entities reflect American policy parameters. By extension, court decisions invalidating some of these sanctions highlight a major legal defect in U.S. secondary sanctions: they cannot survive scrutiny as focused measures targeting entities directly involved in alleged nefarious activities. They are broad-brush instruments meant to shut down as much Iranian economic activity—and inflict as much hardship on Iranians—as possible. Besides its inhumanity, such an approach is bound to impinge on increasingly important interests of more and more states, setting the stage for backlash.

Moreover, secondary sanctions violate U.S. commitments under the World Trade Organisation, which allows members to cut trade with states they deem national security threats but not to sanction other members over business conducted in third countries. If challenged on this in the WTO’s Dispute Resolution Mechanism, Washington would surely lose. Meanwhile, America’s accelerating resort to the threatened application of secondary sanctions boosts non-Western cynicism not just about the real objectives of U.S. Iran policy, but also about the universal applicability of WTO rules and norms, thereby eroding confidence in the existing trade regime.

“Neither unilateral nor UN measures have had decisive impact on Iran’s economy: even a superpower’s unilateral sanctions don’t work if other countries won’t replicate them, and China and Russia ensure that UN sanctions don’t impinge on their most important interests with Iran.”

THEI START

Second, secondary sanctions are a political house of cards. American officials are well aware of their presumptive illegality. Successive U.S. administrations have been reluctant to impose them on non-U.S. entities transacting with Iran, precisely to avoid formal challenges at the WTO. U.S. secondary sanctions are, in effect, an enormous bluff, leveraging the specter of legal and reputational risk in America to bully companies and banks in third countries to stop transacting with Iran, but without pulling the trigger on the threat to punish those that continue doing business in Iran.

### Politics Uniqueness

#### PC and spin fails---no support behind Obama

Weber 1/1 -- FoxNews Staff

[Joseph, “After rough year, Obama looks for 2014 comeback, amid some unsolicited New Year's resolutions,” <http://www.foxnews.com/politics/2014/01/01/after-rough-year-obama-looks-for-2014-comeback-amid-some-unsolicited-new-year/> DOA: 1-1-14]

However, Obama’s political power began to wane soon after, starting with his failed effort to tighten federal gun laws in the wake of two mass shootings and concluding with the disastrous rollout of his signature health care law. Obama’s job approval rating continued to fall as the HealthCare.gov website continued to malfunction and millions of Americans learned they, in fact, could not keep their existing insurance policies -- earning him PolitiFact’s lie-of-the-year award. “It’s never too late to get it right,” Dan Holler, communications director for the conservative group Heritage Action for America, said Tuesday. “So the president should finally honor the promise he made to the American people when he said they could keep their health insurance and doctors.” Along the way, even some members of the liberal media, among the president's strongest supporters, have piled on. A Washington Post political blogger wrote Obama had “the worst year in Washington.” And perhaps even worse, MSNBC commentator Chris Matthews hinted at a lost second term. “It’s not just a bad year in terms of the rollout,” Matthews said. "There’s erosion in interest. ... It feels like the seventh or eighth year of a presidency. It doesn't feel like the fifth.” His comments were included in a 15-page Republican National Committee release this week that chronicled Obama’s rough year and included the IRS scandal, in which agents targeted Tea Party groups, and revelations about the National Security Agency spying on friendly foreign leaders. Moreover, Obama “standing on the sidelines” as the events unfolded has even thrown in jeopardy his entire political legacy, the RNC argues. Democratic strategist Joe Trippi says the president and his administration could improve their lot almost immediately by being more transparent about ObamaCare enrollment numbers, releasing them every two weeks instead of every month “no matter how bad they are.” He thinks the president would have limited success trying to further extend a hand to a Congress that is stuck in partisan gridlock and should instead focus on finishing what he started. “There’s no spin that will fix things,” Trippi said Monday. “It’s now about getting things done. You cannot just say ObamaCare is great. What matters is will 7.5 million people really sign up?”

### Sargent Card

#### Their card proves that IT’S INEVITABLE or any THUMPER should have triggered

Sargent, Washington Post, 1-22-14

(Greg, “Another blow to the Iran sanctions bill,” http://www.washingtonpost.com/blogs/plum-line/wp/2014/01/22/another-blow-to-the-iran-sanctions-bill/, accessed 1-23-14, CMM)

Add two more prominent Senators to the list of lawmakers who oppose a vote on an Iran sanctions bill right now: Patty Murray and Elizabeth Warren.¶ Murray’s opposition — which she declared in a letter to constituents that was sent my way by a source — is significant, because she is a member of the Senate Dem leadership, which is now clearly split on how to proceed. While Chuck Schumer favors the Iran sanctions bill, Murray, Harry Reid and (reportedly) Dick Durbin now oppose it. This could make it less likely that it ever gets a vote.¶ From Murray’s letter:¶ Please know that I share your concerns about the Iranian government’s nuclear program. Like you, I am troubled by Iran’s nuclear enrichment program and their desire to enrich nuclear materials above levels required for energy production. That is why I was pleased to see Iran take measurable steps toward addressing the international community’s concerns by signing the Joint Plan of Action last fall…While I still remain concerned about Iran’s nuclear program, I believe this agreement could be an important step in our efforts to reach a diplomatic solution to this complicated issue.¶ I believe the Administration should be given time to negotiate a strong verifiable comprehensive agreement. However, if Iran does not agree to a comprehensive agreement that is acceptable, or if Iran does not abide by the terms of the interim agreement, I will work with my colleagues to swiftly enact sanctions in order to increase pressure on the Iranian regime.¶ This hits some of the key points: The mere possibility of a long term deal is worth trying for, and sanctions can always be imposed later if the talks go awry.¶ Meanwhile, Elizabeth Warren is circulating a letter to constituents out there that also opposes a vote. Asked about the letter, Warren spokesperson Lacey Rose emails me:¶ “Senator Warren believes we must exhaust every effort to resolve the Iranian nuclear issue through diplomacy, and she does not support imposing additional sanctions through new legislation while diplomatic efforts to achieve a long-term agreement are ongoing.”¶ Warren’s pull with the Democratic base, of course, is largely rooted in her emphasis on economic issues, but there has been some chatter in liberal circles inquiring about her stance on Iran. Since a mobilized left is important in preventing a vote that could derail diplomacy, her opposition can only help.¶ The method by which both Senators declared their positions — letters to constituents, in response to questions perhaps stoked by pressure from outside groups — says something about the caution Dems are demonstrating when it comes to the domestic politics of engagement with Iran. Those who favored a vote were far more vocal at first — as of now, 16 Dem Senators have signed on. But the continued silence of many Dem Senators signaled a broad unwillingness to join the bill, even as many were unwilling to publicly declare this to be the case, since Dems apparently see allowing negotiations to proceed, without getting a chance to vote in favor of getting tougher on Iran, as a politically difficult position to take.¶ If current conditions remain, a vote is starting to look less and less likely. Right now, the bill has 58 co-sponsors. On the other side, 10 Dem Senate committee chairs have signed a letter opposing a vote. Around half a dozen Dem Senators subsequently came out against it. With Murray and Warren, the number of Dems against a vote has comfortably surpassed the number who want one.

**THEIR CARD ENDS**

Meanwhile, announcements like the one earlier this month indicating that the deal with Iran is moving forward make a vote still less likely. With Murray now opposed, that means virtually the whole Dem leadership is a No. On the other hand, those who adamantly want a vote — insisting it would only help the White House and make success more likely, despite what the White House itself wants – will be looking for any hook they can find to reactivate pressure.

### NSA Thumper

#### More restrictions are popular but squo triggers PC backlash

Wilson 1/17 (Scott Wilson, Chief White House correspondent for the Washington Post. Previously, he was the paper’s deputy Assistant Managing Editor/Foreign News after serving as a correspondent in Latin America and in the Middle East. He was awarded an Overseas Press Club citation and an Interamerican Press Association award for his work abroad. For his coverage of the Obama administration, he received the 2011 Gerald R. Ford Prize for Distinguished Reporting on the Presidency and the 2012 Aldo Beckman Award given by the White House Correspondents’ Association. He joined the Post in 1997, “Obama acknowledges real-world limits on changing U.S. intelligence practices”, <http://www.washingtonpost.com/politics/obama-acknowledges-real-world-limits-on-changing-us-intelligence-practices/2014/01/17/21be329c-7f9c-11e3-93c1-0e888170b723_story.html>, January 17, 2014)

Four months after taking office, President Obama spoke at the National Archives, steps away from the Constitution, and described in sharply critical terms “the season of fear” in the United States that followed the Sept. 11, 2001, attacks. Torture had been practiced in interrogations. Terrorism suspects were held without trial in an offshore military prison. U.S. troops invaded a country without links to the attacks on New York and Washington. The National Security Agency was exposed for eavesdropping on U.S. citizens without warrants. “In other words,” Obama said, “we went off course.” It was understood that Obama, the constitutional law lecturer, would find the country’s compass. But as Obama acknowledged Friday, in a speech delivered just around the corner from the archives at the Justice Department, he is still navigating the politically complicated legacy of the “war on terror.” It is a legacy that has profound implications for his own as president. “When you cut through the noise, what’s really at stake is how we remain true to who we are in a world that is remaking itself at dizzying speed,” Obama said Friday, in an echo of his message almost five years ago. Obama moved quickly to fulfill his pledge to close the military prison at Guantanamo Bay, Cuba, although political obstacles have prevented him from seeing it through. Also in those first days, he officially banned the practice of torture in interrogation, methods that had ceased by the close of the Bush administration. But those were issues where Obama’s policy inclinations, his principles and the politics of his party all came together — the easiest remnants of post-9/11 national security policy to criticize and work to end. Now he faces a more consequential challenge in changing, amid public pressure at home and abroad, a series of intelligence practices that he has called useful in preventing another terrorist attack in the United States. “This is the hard stuff,” said Anthony D. Romero, executive director of the American Civil Liberties Union. “The surveillance collection issues will go to the heart of what America is all about for generations to come. The due process issues, the torture issues certainly go to American values. But they will not affect the vast majority of Americans or others around the world. This is where the rubber meets the road.” Obama spoke both as a longtime lawyer and as a second-term commander in chief, more defensive than contrite over the work done by U.S. intelligence officers and of the utility and care with which the NSA’s bulk collection program has been managed. “It may seem sometimes that America is being held to a different standard, and I’ll admit the readiness of some to assume the worst motives by our government can be frustrating,” Obama said. “But let us remember that we are held to a different standard precisely because we have been at the forefront in defending personal privacy and human dignity.” The changes Obama ordered to NSA practices emphasize additional oversight — the “checks and balances and accountability” that he first mentioned at the National Archives years ago. Other than curtailing American eavesdropping on allied leaders, the agency’s collection efforts will remain largely intact, an enduring concern to privacy groups who argue that the government has no right to collect information about U.S. citizens without a warrant. Many of the programs disclosed by The Washington Post and the British newspaper the Guardian in recent months, based on documents provided by former NSA contractor Edward J. Snowden, will remain untouched. Having run for office as a critic of the Bush administration’s national security policies, Obama was always going to be measured, in part, by how he scaled back the excesses of post-9/11 national security practices and preserved the essentials in a still-dangerous world. The reviews on that account have been mixed. Obama withdrew U.S. troops from Iraq, a conflict he once called a “dumb war,” and has set an end-of-the-year end date for U.S. participation in Afghanistan’s war. At the same time, he has expanded the battlefield for the U.S. drone fleet and stepped up the tempo of strikes from the Bush years, another counterterrorism tool that many within his party say should have far more accountability and oversight. Only the bombings in Boston last year could be considered a successful mass terrorist attack on Obama’s watch, although there have been some near misses. As Obama alluded to several times Friday, technological leaps have both greatly expanded U.S. surveillance capabilities and made obsolete the rules governing those practices. Setting those limits now involves a set of decisions, some of which Obama presented Friday, that put into conflict his role as a commander in chief and the promises he made as a new president, particularly to those in his own party. Obama made himself vulnerable to conservative charges that by ending some Bush administration national security policies, he was putting the nation at risk of another attack. He argued that American values and national security policy could coexist. But he and his advisers were also mindful that his credibility on the subject — and more broadly, his political viability — would likely be only a terrorist attack away from ruin as a result. As the more visible elements of post-9/11 national security policy diminished, namely the large military deployments overseas, the secret elements typified by drone strikes and electronic spying grew under a president who had promised unprecedented transparency. He captured the conflict in his Friday speech. “I maintained a healthy skepticism toward our surveillance programs after I became president,” Obama said Friday, even though he had previously acknowledged that he was unaware of the sensitive “head of state” program that targeted the personal cellphones of such allies as German Chancellor Angela Merkel. Obama’s political considerations are particularly challenging on the question of surveillance, resembling those he had to consider when deciding whether to increase the U.S. presence in Afghanistan four years ago. Now, as then, many in his party are demanding more change to the NSA’s spying practices than he is willing to carry out. A Washington Post-ABC News poll in November found that Democrats were twice as likely to disapprove of Obama’s handling of the NSA than of his overall job performance. The party ambivalence was reflected on Capitol Hill in the hours after Obama’s speech. Some Democrats applauded the president for addressing the controversy, particularly over the phone-record collection program, while others urged him to do more. “The reforms outlined by President Obama today are a welcome first step in reining in the government’s unacceptable infringement on Americans’ privacy rights,” Sen. Tom Udall (D-N.M.) said in a statement. “But I’m not satisfied these reforms go far enough.” Behind Obama’s words Friday was a question asked increasingly around the West Wing: How does he want to be remembered? To a president who has already made history by being the first African American to hold the office, Obama’s answer goes beyond a simple record of his administration. He is mindful of history and his place in it, and to many of his advisers and supporters, any assessment of his legacy should provide the end of the sentence: “He was the president who . . .” Successfully ended the “season of fear” and the government excesses that defined it? Or cemented in place a vast surveillance state he once opposed? On Friday, he began to provide the answer. “I have often reminded myself that I would not be where I am today were it not for the courage of dissidents, like Dr. King, who were spied on by their own government,” Obama said. “And as a president, a president who looks at intelligence every morning, I also can’t help but be reminded that America must be vigilant in the face of threats.”