# 1NC

### 1NC

#### Congress will successfully avert a government shutdown now, but time is super tight

Fox News, 9-11-2013, “House pulls spending bill amid backlash as government shutdown looms,” http://www.foxnews.com/politics/2013/09/11/house-leaders-pull-temporary-spending-bill-after-conservative-backlash/

House Republican leaders pulled their plan Wednesday to temporarily fund the federal government after rank-and-file party members said it sidestepped “defunding” ObamaCare. The action further narrowed Congress’ time to strike a budget deal before an Oct. 1 government shutdown. House Speaker John Boehner and his team pulled the plan, which could have gotten a full chamber vote as early as Thursday, after a conservative backlash led by the Tea Party movement and Heritage Action for America. The plan essentially called for the House to vote on defunding ObamaCare and the temporary spending bill, then send the package to the Democrat-controlled Senate, which almost certainly would have jettisoned the defund part and allowed the chambers to negotiate on a “clean” funding bill. “The Ruling Elite is up to it again,” the Tea Party Patriots group said Wednesday. “They want you to think they have voted for defunding ObamaCare. But it’s another shell game.” Meanwhile, Congress must also work on several other pressing issues, especially agreeing to increase the debt ceiling, which the government could hit as soon as mid-October, according to a recent Treasury Department assessment. Boehner defended his defund-spending plan Tuesday, saying his chamber has already voted 40 times to “defund, repeal and change” ObamaCare, so the Senate must now take up the fight. Although Boehner pulled the bill because he didn’t have the votes, sources tell Fox News the speaker has no intention of changing the plan and might revisit it next week -- after members realize its strengths. Meanwhile members from both parties appear optimistic about avoiding a partial government shutdown, despite the looming deadline and the potential for another internal House struggle. “We've got some time left,” Kentucky Republican Rep. Hal Rogers, chairman of the House Appropriations Committee, told Fox News. “It's not time to panic.” The postponement of a Capitol Hill vote on a military strike on Syria will indeed eliminate the related hearings and classified briefings that slowed work on other pending issues, including immigration reform, the Farm Bill and whether to limit the extent to which the National Security Agency can collect data on Americans in its efforts to thwart terrorism.

#### The plan would trade off with Congress’s ability to avert the shutdown - GOP has momentum and will, but they need literally every hour to get it done

Frank James, 9-13-2013, “Congress Searches For A Shutdown-Free Future,” NPR, http://www.npr.org/blogs/itsallpolitics/2013/09/13/221809062/congress-searches-for-a-shutdown-free-future

The only thing found Thursday seemed to be more time for negotiations and vote-wrangling. Republican leaders recall how their party was blamed for the shutdowns of the mid-1990s and earnestly want to avoid a repeat, especially heading into a midterm election year. Cantor alerted members Thursday that during the last week of September, when they are supposed to be on recess, they will now most likely find themselves in Washington voting on a continuing resolution to fund the government into October. It looks like lawmakers will need every hour of that additional time. While talking to reporters Thursday, Boehner strongly suggested that House Republicans weren't exactly coalescing around any one legislative strategy. "There are a lot of discussions going on about how — about how to deal with the [continuing resolution] and the issue of 'Obamacare,' and so we're continuing to work with our members," Boehner said. "There are a million options that are being discussed by a lot of people. When we have something to report, we'll let you know."

#### Shutdown wrecks the economy

Yi Wu, 8-27-2013, “Government Shutdown 2013: Still a Terrible Idea,” PolicyMic, http://www.policymic.com/articles/60837/government-shutdown-2013-still-a-terrible-idea

Around a third of House Republicans, many Tea Party-backed, sent a letter last week calling on Speaker John Boehner to reject any spending bills that include implementation of the Affordable Care Act, otherwise known as Obamacare. Some Senate Republicans echo their House colleagues in pondering this extreme tactic, which is nothing other than a threat of government shutdown as neither congressional Democrats nor President Obama would ever agree on a budget that abolishes the new health care law. Unleashing this threat would amount to holding a large number of of the federal government's functions, including processing Social Security checks and running the Centers for Disease Control, hostage in order to score partisan points. It would be an irresponsible move inflicting enormous damage to the U.S. economy while providing no benefit whatsoever for the country, and Boehner is rightly disinclined to pursue it. Government shutdowns are deleterious to the economy. Two years ago in February 2011, a similar government shutdown was looming due to a budget impasse, and a research firm estimated that quater's GDP growth would be reduced by 0.2 percentage points if the shutdown lasted a week. After the budget is restored from the hypothetical shutdown, growth would only be "partially recouped," and a longer shutdown would result in deeper slowdowns. Further, the uncertainties resulting from a shutdown would also discourage business. A shutdown was avoided last-minute that year, unlike in 1995 during the Clinton administration where it actually took place for four weeks and resulted in a 0.5 percentage-point dent in GDP growth. Billions of dollars were cut from the budget, but neither Boehner nor the Republicans at the time were reckless enough to demand cancellation of the entire health care reform enacted a year before.

#### Global nuclear war

Harris & Burrows 9 Mathew, PhD European History @ Cambridge, counselor of the U.S. National Intelligence Council (NIC) and Jennifer, member of the NIC’s Long Range Analysis Unit “Revisiting the Future: Geopolitical Effects of the Financial Crisis” http://www.ciaonet.org/journals/twq/v32i2/f\_0016178\_13952.pdf

Of course, the report encompasses more than economics and indeed believes the future is likely to be the result of a number of intersecting and interlocking forces. With so many possible permutations of outcomes, each with ample Revisiting the Future opportunity for unintended consequences, there is a growing sense of insecurity. Even so, history may be more instructive than ever. While we continue to believe that the Great Depression is not likely to be repeated, the lessons to be drawn from that period include the **harmful effects on fledgling democracies** and multiethnic societies (think Central Europe in 1920s and 1930s) and on the sustainability of multilateral institutions (think League of Nations in the same period). There is no reason to think that this would not be true in the twenty-first as much as in the twentieth century. For that reason, the ways in which **the potential for** greater **conflict could grow** would seem to be even more apt in a constantly volatile economic environment as they would be if change would be steadier. In surveying those risks, the report stressed the likelihood that terrorism and nonproliferation will remain priorities even as resource issues move up on the international agenda. **Terrorism**’s appeal will decline if economic growth continues in the Middle East and youth unemployment is reduced. For those terrorist groups that remain active in 2025, however, the diffusion of technologies and scientific knowledge will place some of the world’s most dangerous capabilities within their reach. Terrorist groups in 2025 will likely be a combination of descendants of long established groups\_inheriting organizational structures, command and control processes, and training procedures necessary to conduct sophisticated attacks and newly emergent collections of the angry and disenfranchised that become self-radicalized, particularly in the absence of economic outlets that would become narrower in an economic downturn. The most dangerous casualty of any **economically-induced drawdown** of U.S. military presence would almost certainly be the Middle East. Although Iran’s acquisition of nuclear weapons is not inevitable, worries about a nuclear-armed Iran could lead states in the region to develop new security arrangements with external powers, **acquire additional weapons**, and consider pursuing their own **nuclear ambitions**. It is not clear that the type of stable deterrent relationship that existed between the great powers for most of the Cold War would emerge naturally in the Middle East with a nuclear Iran. Episodes of low intensity conflict and terrorism taking place under a nuclear umbrella could lead to an **unintended escalation** and **broader conflict** if clear red lines between those states involved are not well established. The close proximity of potential **nuclear rivals** combined with underdeveloped surveillance capabilities and mobile dual-capable Iranian missile systems also will produce inherent difficulties in achieving reliable indications and warning of an impending nuclear attack. The lack of strategic depth in neighboring states like Israel, short warning and missile flight times, and uncertainty of Iranian intentions may place more focus on **preemption** rather than defense, potentially leading to **escalating crises**. 36 Types of conflict that the world continues to experience, such as over resources, could reemerge, particularly if protectionism grows and there is a resort to neo-mercantilist practices. Perceptions of renewed energy scarcity will drive countries to take actions to assure their future access to energy supplies. In the worst case, this could result in **interstate conflicts** if government leaders deem assured access to energy resources, for example, to be essential for maintaining domestic stability and the survival of their regime. Even actions short of war, however, will have important geopolitical implications. Maritime security concerns are providing a rationale for naval buildups and modernization efforts, such as China’s and India’s development of blue water naval capabilities. If the fiscal stimulus focus for these countries indeed turns inward, one of the most obvious funding targets may be military. Buildup of regional naval capabilities could lead to increased tensions, rivalries, and counterbalancing moves, but it also will create opportunities for multinational cooperation in protecting critical sea lanes. With water also becoming scarcer in Asia and the Middle East, cooperation to manage changing water resources is likely to be increasingly difficult both within and between states in a more dog-eat-dog world.

### 1NC

#### Restrictions are prohibitions on action --- the aff is a reporting requirement

Jean Schiedler-Brown 12, Attorney, Jean Schiedler-Brown & Associates, Appellant Brief of Randall Kinchloe v. States Dept of Health, Washington, The Court of Appeals of the State of Washington, Division 1, http://www.courts.wa.gov/content/Briefs/A01/686429%20Appellant%20Randall%20Kincheloe%27s.pdf

3. The ordinary definition of the term "restrictions" also does not include the reporting and monitoring or supervising terms and conditions that are included in the 2001 Stipulation.

Black's Law Dictionary, 'fifth edition,(1979) defines "restriction" as;

A limitation often imposed in a deed or lease respecting the use to which the property may be put. The term "restrict' is also cross referenced with the term "restrain." Restrain is defined as; To limit, confine, abridge, narrow down, restrict, obstruct, impede, hinder, stay, destroy. To prohibit from action; to put compulsion on; to restrict; to hold or press back. To keep in check; to hold back from acting, proceeding, or advancing, either by physical or moral force, or by interposing obstacle, to repress or suppress, to curb.

In contrast, the terms "supervise" and "supervisor" are defined as; To have general oversight over, to superintend or to inspect. See Supervisor. A surveyor or overseer. . . In a broad sense, one having authority over others, to superintend and direct. The term "supervisor" means an individual having authority, in the interest of the employer, to hire, transfer, suspend, layoff, recall, promote, discharge, assign, reward, or discipline other employees, or responsibility to direct them, or to adjust their grievances, or effectively to recommend such action, if in connection with the foregoing the exercise of such authority is not of a merely routine or clerical nature, but required the use of independent judgment.

Comparing the above definitions, it is clear that the definition of "restriction" is very different from the definition of "supervision"-very few of the same words are used to explain or define the different terms. In his 2001 stipulation, Mr. Kincheloe essentially agreed to some supervision conditions, but he did not agree to restrict his license.

#### Restrictions on authority are distinct from conditions

William Conner 78, former federal judge for the United States District Court for the Southern District of New York United States District Court, S. D. New York, CORPORACION VENEZOLANA de FOMENTO v. VINTERO SALES, http://www.leagle.com/decision/19781560452FSupp1108\_11379

Plaintiff next contends that Merban was charged with notice of the restrictions on the authority of plaintiff's officers to execute the guarantees. Properly interpreted, the "conditions" that had been imposed by plaintiff's Board of Directors and by the Venezuelan Cabinet were not "restrictions" or "limitations" upon the authority of plaintiff's agents but rather conditions precedent to the granting of authority. Essentially, then, plaintiff's argument is that Merban should have known that plaintiff's officers were not authorized to act except upon the fulfillment of the specified conditions.

#### Vote neg---

#### Only prohibitions on authority guarantee neg ground---their interpretation lets affs no link the best neg offense like deference

#### Precision---only our interpretation defines “restrictions on authority”---that’s key to adequate preparation and policy analysis

### 1NC

#### Text: The United States Federal Government should clarify that the Department of Defense has the legal authority and intent to conduct proportional offensive cyber operations to “counter [imminent] threats to [the United States’] national interests in cyberspace” on orders of the President. The United States Federal Government should store backups of offensive cyber capabilities in offline locations and invest in maintenance of secure telephone and radio lines for chain of command communications.

#### Recent advances in attribution capability mean the counterplan creates effective cyber-deterrence --- prevents cyber-attacks on the US --- the plan and permutation destroy deterrence credibility

Jack Goldsmith 12, is the Henry L. Shattuck Professor @ Harvard Law School, where he teaches and writes about national security law, presidential power, cybersecurity, international law, internet law, foreign relations law, and conflict of laws. Before coming to Harvard, Professor Goldsmith served as Assistant Attorney General, Office of Legal Counsel from 2003–2004, and Special Counsel to the Department of Defense from 2002–2003. Professor Goldsmith is a member of the Hoover Institution Task Force on National Security and Law, 10/15, “The Significance of Panetta’s Cyber Speech and the Persistent Difficulty of Deterring Cyberattacks,” Lawfare, <http://www.lawfareblog.com/2012/10/the-significance-of-panettas-cyber-speech-and-the-persistent-difficulty-of-deterring-cyberattacks/>

Secretary of Defense Leon Panetta’s speech last week on cyber is more significant than has been reported. Most of the coverage focused on Panetta’s grave warnings about cyber threats facing the nation, but the speech’s real significance, I think, concerns DOD’s evolving deterrence posture. (The speech has other significant elements, but I focus here on deterrence.)¶ Panetta had two main messages related to deterrence. First, because the USG’s attribution skills have improved, “[p]otential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America.” Second, “If we detect an imminent threat of attack that will cause significant, physical destruction in the United States or kill American citizens,” then on the orders of the President, DOD can “conduct effective operations to counter threats to our national interests in cyberspace.” (This second point echoes earlier USG statements, including one made earlier this month by DRNSA Keith Alexander, who said, somewhat less cautiously than Panetta, that DOD must be able to “stop [an attack] before it happens. . . . Part of our defense has to consider offensive measures like that to stop it from happening.”)¶ Here is what I think is significant about Panetta’s speech.¶ First, DOD has previously said that it is trying to improve is attribution capabilities, and in conversation officials have noted some success. Panetta goes further, saying concretely and definitively that DOD has “made significant advances in solving” the attribution problem, presumably through a combination of tracing back the source of a cyber attack and identifying the attacker through “behavior-based algorithms” and human and electronic intelligence. Panetta does not tell us how good or fast DOD is at attribution, and he may to some unknown degree be puffing. Nonetheless, this is a potentially big deal for cyber deterrence.¶ Second, Panetta was more aggressive than DOD has been in the past about the trigger for a self-defensive cyberattack by the United States. Previously, DOD has stated that adversaries would face a “grave risk” if they launched a “crippling” or “significant” cyberattack on the homeland. Panetta’s speech changes this posture in two ways. He is less definitive about the high threshold of a “significant” or “crippling” attack as a trigger for a USG response, and indeed implies that the threshold is (or can be) lower. And more importantly, he makes plain that the DOD has the capabilities and desire to engage in a preemptive attacks against imminent cyber threats. This possibility has been hinted at before (most recently, in Alexander’s comment above and in Harold Koh’s NSA Cyber Command legal conference speech last month). But Panetta was more definitive about DOD’s capacity and desire to engage in such attacks. (Herb Lin, chief scientist at the National Research Council’s Computer Science and Telecommunications Board, noted to me that Panetta referred to the need to “take action” with “effective operations” against imminent cyberthreats, and pointedly did not state that such actions or operations would necessarily involve cyber means or cyber targets. This is consistent with DOD’s prior claims that it would use “cyber and/or kinetic capabilities” to redress large-scale cyberattacks.) Panetta was ambiguous, however, about whether DOD currently has the authorities to engage in such preemptive attacks (by cyber means or other means) in the face of cyber threats. He said that “we need to have the option to take action against those who would attack us to defend this nation when directed by the president” (emphasis added), and he emphasized DOD capabilities while several times calling for more DOD authorities.¶ I have previously criticized DOD’s announced deterrence policy, so I should say that Panetta’s speech takes steps in the right direction. Panetta noted improvement in attribution (which is potentially huge), he warned that the USG would hold attackers responsible, he appeared to eliminate unjustifiably super-high thresholds for a self-defensive responses to cyberattacks, and he noted DOD’s capacity and need for preemptive attacks in the face of imminent cyberattacks.¶ That said, Panetta made these points in an after-dinner speech, not an official declaratory policy. And many questions remain, such as: How much better (in terms of speed and accuracy) is our attribution capacity? How do adversaries know whether the USG’s supposed attribution advances are not a bluff? What exactly is the threshold for a self-defensive offensive operation in response to a cyber attack? What counts as an imminent threat of cyberattack that would warrant a preemptive attack by the USG? The effectiveness of any deterrence posture depends on the answers to these (and related) questions, and (very importantly) on our adversaries’ beliefs about the answers to these questions. Ambiguity about the answers might over-deter (as vague criminal law often does), but it might also under-deter (because the adversary misperceives where the red lines are).¶ The effectiveness of deterrence also depends, crucially, on the credibility of our threat to attack in the face of actual or imminent attacks. Several obstacles prevent our threats from being entirely credible. Panetta’s speech and other DOD pronouncements, as well as news reports, indicate that DOD does not think it has adequate legal authorities to engage in offensive operations related to defense, and that USG lawyers are currently putting up affirmative obstacles to such operations. To the extent that the USG is and appears to be legally constrained from acting as it says it needs to, its threats to act are not credible.

### 1NC

#### Congressional restrictions cause adversaries to doubt the credibility of our threats --- causes crisis escalation

Matthew Waxman 8/25/13, Professor of Law @ Columbia and Adjunct Senior Fellow for Law and Foreign Policy @ CFR, “The Constitutional Power to Threaten War,” Forthcoming in Yale Law Journal, vol. 123, August 25, 2013, SSRN

A claim previously advanced from a presidentialist perspective is that stronger legislative checks on war powers is harmful to coercive and deterrent strategies, because it establishes easily-visible impediments to the President’s authority to follow through on threats. This was a common policy argument during the War Powers Resolution debates in the early 1970s. Eugene Rostow, an advocate inside and outside the government for executive primacy, remarked during consideration of legislative drafts that any serious restrictions on presidential use of force would mean in practice that “no President could make a credible threat to use force as an instrument of deterrent diplomacy, even to head off explosive confrontations.”178 He continued:¶ In the tense and cautious diplomacy of our present relations with the Soviet Union, as they have developed over the last twenty-five years, the authority of the President to set clear and silent limits in advance is perhaps the most important of all the powers in our constitutional armory to prevent confrontations that could carry nuclear implications. … [I]t is the diplomatic power the President needs most under the circumstance of modern life—the power to make a credible threat to use force in order to prevent a confrontation which might escalate.179

#### Perception of weak Presidential crisis response collapses heg

John R. Bolton 9, Senior fellow at the American Enterprise Institute & Former U.S. ambassador to the United Nations, “The danger of Obama's dithering,” Los Angeles Times, October 18, http://articles.latimes.com/2009/oct/18/opinion/oe-bolton18

Weakness in American foreign policy in one region often invites challenges elsewhere, because our adversaries carefully follow diminished American resolve. Similarly, presidential indecisiveness, whether because of uncertainty or internal political struggles, signals that the United States may not respond to international challenges in clear and coherent ways. Taken together, weakness and indecisiveness have proved historically to be a toxic **combination for America's global interests**. That is exactly the combination we now see under President Obama. If anything, his receiving the Nobel Peace Prize only underlines the problem. All of Obama's campaign and inaugural talk about "extending an open hand" and "engagement," especially the multilateral variety, isn't exactly unfolding according to plan. Entirely predictably, we see more clearly every day that diplomacy is not a policy but only a technique. **Absent** presidential leadership, **which at a minimum means** clear policy direction and persistence in the face of criticism and adversity**, engagement simply embodies** weakness and indecision.

#### Hegemony solves great power war

Khalilzad 11 – Zalmay Khalilzad, the United States ambassador to Afghanistan, Iraq, and the United Nations during the presidency of George W. Bush and the director of policy planning at the Defense Department from 1990 to 1992, February 8, 2011, “The Economy and National Security; If we don’t get our economic house in order, we risk a new era of multi-polarity,” online: <http://www.nationalreview.com/articles/259024/economy-and-national-security-zalmay-khalilzad>

We face this domestic challenge while other major powers are experiencing rapid economic growth. Even though countries such as China, India, and Brazil have profound political, social, demographic, and economic problems, their economies are growing faster than ours, and this could alter the global distribution of power. These trends could in the long term produce a multi-polar world. If U.S. policymakers fail to act and other powers continue to grow, it is not a question of whether but when a new international order will emerge. The closing of the gap between the United States and its rivals could intensify geopolitical competition among major powers, increase incentives for local powers to play major powers against one another, and undercut our will to preclude or respond to international crises because of the **higher risk of escalation.**¶ The stakes are high. In modern history, the longest period of peace among the great powers has been the era of U.S. leadership. By contrast, multi-polar systems have been unstable, with their competitive dynamics resulting in frequent crises and major wars among the great powers. Failures of multi-polar international systems produced both world wars.¶ American retrenchment could have devastating consequences. Without an American security blanket, regional powers could rearm in an attempt to balance against emerging threats. Under this scenario, there would be a heightened possibility of arms races, miscalculation, or other crises spiraling into all-out conflict. Alternatively, in seeking to accommodate the stronger powers, weaker powers may shift their geopolitical posture away from the United States. Either way, hostile states would be emboldened to make aggressive moves in their regions.¶ As rival powers rise, Asia in particular is likely to emerge as a zone of **great-power competition**. Beijing’s economic rise has enabled a dramatic military buildup focused on acquisitions of naval, cruise, and ballistic missiles, long-range stealth aircraft, and anti-satellite capabilities. China’s strategic modernization is aimed, ultimately, at denying the United States access to the seas around China. Even as cooperative economic ties in the region have grown, China’s expansive territorial claims — and provocative statements and actions following crises in Korea and incidents at sea — have roiled its relations with South Korea, Japan, India, and Southeast Asian states. Still, the United States is the most significant barrier facing Chinese hegemony and aggression.

#### OCOs give the US coercive leverage to deescalate North Korean nuclear brinksmanship --- speed is key

Martin C. Libicki 13, Senior Management Scientist @ RAND and adjunct fellow @ Georgetown’s Center for Security Studies, “Brandishing Cyberattack Capabilities,” RAND, <http://www.rand.org/pub> s/research\_reports/RR175.html

Our inquiry is therefore more humble. Could a U.S. threat that it might interfere with a rogue state’s nuclear weapon delivery help shape a nuclear confrontation? For this question, assume a rogue nuclear power with a handful of weapons capable of hitting nearby countries (but generally incapable of hitting the continental United States). The United States has a robust cyberattack capability (in general terms), from which the rogue state’s nuclear arsenal is not provably immune. Although the United States enjoys escalation dominance, the rogue state is far more willing to go to the nuclear brink than the United States is. The rogue state (thinks it) has more at stake (i.e., regime survival). Furthermore, it may act in ways that are irrational by Western perspectives.¶ We first model a two-state confrontation, then later introduce a friendly state on whose behalf the United States has intervened. The United States enters this scenario facing the choice of acting when doing so risks the rogue state releasing a nuclear weapon. Whether the threat is explicit or implicit is secondary. The usual calculus applies. The rogue state is better off if its threat leads the United States to stop. The United States is better off ignoring the threat and going ahead with what it would have done in the absence of the threat if the threat can be nullified but cannot know that it will be for certain. The rogue state understands that if it does use nuclear weapons, it could face great retaliation.1¶ If the United States acts (successfully) in the face of warning and if the rogue state does not use nuclear weapons, the United States achieves its objectives and wins the overall confrontation.2 If the United States flinches, the rogue state wins. If the rogue state uses its nuclear weapons and if, as is likely, the United States responds likewise, the rogue state loses greatly, but the United States is also far worse off.3¶ Two-Party Confrontations¶ In a confrontation in which disaster would result from both sides carrying out their threats, each must ask: Are such threats credible? If one side thinks the other will yield, it pays to stand firm. If it thinks, however, that the other is implacable, it may have no good choice but to yield itself. The projection of implacability is beneficial, but the reality of implacability is frequently suicidal.¶ Note that the basis for the implacability can also be entirely subjective, which is to say, unfounded on the facts of the matter. If one party is convinced that it will never pay a high price for being implacable, communicates as much, and acts as if it were so, the other cannot take any comfort from the fact that the first has no technical basis for the belief. The only consideration is whether the first party actually believes as much, is willing to act accordingly, and can ignore the logic that whispers that no one can possibly be completely confident on the basis of iffy information. To one party, the willingness to act on the basis of the impossible seems like cheating. To use an analogy, imagine a game of “chicken” in which the driver of one of the two oncoming cars throws the steering wheel out the window. This cheat forces the opponent to choose between a certain crash or veering away (and thus losing). However, when the consequences of a crash are far greater than the benefits of winning, this strategy is irrational if there is a nontrivial likelihood that the other side will be intent on punishing cheaters at the cost of all other values. In the analogy, the second driver might rather crash than lose to a cheater.4 But in general, a strategy of implacability, can, if credible, do well, as long as the other side is not equally implacable.¶ So, the United States creates the belief (whether by saying so, hinting, or letting others draw their own conclusion) that the rogue state cannot carry out its nuclear threat. That is, the United States acts as though a flaw somewhere in the nuclear command-and-control cycle, probably an induced flaw, prevents immediate nuclear use. A lesser case is that the command and control is less certain, the weapon is weaker, and/or the delivery system is far less accurate than feared.5 Although permanently disabling a nuclear command-and-control system is quite a stretch for cyberwar, it is less fantastic to imagine that the United States could delay a weapon’s use. A temporary advantage, though, may still give the United States time to cross the red line and thereby attain a fait accompli.¶ So posturing, the United States prepares to cross the red line, while communicating its confidence that the rogue state will not retaliate. This confidence stems from a combination of its own nuclear deterrence capability plus its ability to confound the rogue state’s nuclear capability: The rogue nuclear state probably will not decide to retaliate, and if it did decide to, probably cannot retaliate. The combination, in this case, is what reduces the odds of a nuclear response to a sufficiently low level, if the rogue state is at all rational. Even if it later assures itself and others that its nuclear capacity is intact, but the United States has already acted, the onus then falls on the rogue nuclear state to respond to what could well be a done deal. If the rogue state understands the logic before brandishing its own nuclear weapons, it may choose not to ratchet up tensions in advance of the U.S. crossing red lines.

#### Threat of OCO strikes deescalates Senkaku conflict --- prevents great power war

Leigh Drogen 13, founder and chief investment officer of Surfview Capital, LLC, a New York based investment management firm, “Why Cyber Weapons Will Make The World Even Safer,” 3/4, http://www.leighdrogen.com/why-cyber-weapons-will-make-the-world-even-safer/

Scene: China has just exchanged fire with Japan over the East China Sea Islands. The US Navy is in theatre and has as promised under its security umbrella treaty with Japan vows to protect the sovereignty of Japanese territory. In response China has threatened to hold US infrastructure (power, water, transportation) hostage and gives the US 48 hours to exit the theatre. The US immediately responds with a similar threat to cripple Chinese infrastructure via cyber attacks unless China relinquishes cyber attacks within 48 hours.¶ Now you can bet your last dollar that the US has been holding war games designed to simulate exactly this scenario. And while we don’t know how they’ve played out, we can make some pretty informed assumptions based on the corollary of nuclear war theory.¶ The ability for foreign agents to hijack critical infrastructure and cripple it within a short period of time is now to the point where we, and our potential adversaries, could face damage many magnitudes higher than a nuclear strike, not in lives lost, but economic, social, and political damage.¶ Cyber warfare has reached a level where we can say that there is mutually assured destruction of critical infrastructure in a war between the US and China.¶ Which is exactly why I’m ready to say that cyber warfare will make the world an even safer place.¶ There is no argument against the claim that nuclear weapons have massively decreased overall warfare across the world since World War II. During that time we haven’t seen a war between two nuclear states.¶ But the more important development, as Tom Friedman loves to point out, we haven’t seen a major conflict between two countries with a McDonalds. Now, look past the frivolity of that statement through to the bigger point, lives lost is no longer the major determinant of why countries decide to forgo war, it is now primarily an economic and social decision.¶ The cost in treasure and political capital that it takes to go to war as a developed economy with another state is massive. The US has had a huge hand in this no doubt playing the world’s policeman since World War II. Police are not very effective at hunting down transgressors, their job is primarily prevention, a job that the US has pretty much perfected at this point.¶ China will not follow through on its cyber war threat because the cost in economic, social, and political damage to the regime from a crippling US cyber attack would be far too much to handle versus the benefit from its move on the islands. What do you think middle and upper class urban Chinese citizens would do if China risked everything they’ve worked so hard to build over the past 25 years for the islands? They risk nothing less than the regime being toppled. They are already walking on thin ice under the unwritten deal they’ve made, continued economic development for the regime’s position in power.¶ Cyber war has reached the level of mutually assured destruction as the damage caused will lead to popular revolt. It certainly would here in the US.¶ The flip side to this argument, as it is made with nuclear weapons, is that non state actors are not tied to the same consequences and therefor are much more dangerous. I would agree, and in the case of cyber war they it’s even scarier as their capability to inflict damage is far greater (this was the theme of Skyfall), it’s hard to obtain and deliver a nuclear weapon.¶ That said, I believe cyber weapons will add to global security as they become more pervasive.

### 1NC

#### TEXT: The US Congress and US Executive should cooperate to develop guidelines for the use of offensive cyber operations. The US Congress should require that ex-post notification be part of these guidelines.

#### Congress should create guidelines with the president, not restrict

Stephen Dycus—1AC Author—10, Professor, Vermont Law School, 8/11/10, “Congress’s Role in Cyber Warfare,” <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>

Congress obviously cannot act alone to develop a cyber warfare policy for the United States. Its members and staff lack the technical expertise, agility, and organization to wield this new, evolving weaponry. On the other hand, Congress’s job in our constitutional system is to set national policy for the executive branch to execute. Especially in the matter of cyber warfare, where the diplomatic and strategic stakes are potentially as high as they are in any kinetic conflict, Congress has a critical role to play. It has perspective gained from long experience in foreign affairs and a host of related issues, and it may be more responsive to the popular will. The solution to this apparent conundrum may be found in a close collaboration between the political branches in the planning and implementation of rules for cyber warfare.58¶ Congress needs to act now to create authority and set boundaries within which the President may develop more refined protocols. This legislative development should be guided by advice from executive branch officials. The process must be cooperative rather than competitive. The resulting rules will necessarily be partly statutory, partly executive. The recent White House Cybersecurity Policy Review recommended that the “Administration should partner appropriately with Congress to ensure [that] adequate law, policies, and resources are available to support the U.S. cybersecurity-related missions.”59¶ Set out below are some steps that Congress might take to create an appropriate partnership. Some of these steps involve changes in congressional committees and responsibilities. Others would require coordination of cybersecurity functions within the executive branch. Still others would direct the President to keep Congress fully informed about anticipated and actual uses of cyber weapons. Several would restrict potential executive branch actions that seem – as a matter of policy – particularly unwise.

#### Notification kills effective cyber responses

Stephen Dycus—1AC Author—10, Professor, Vermont Law School, 8/11/10, “Congress’s Role in Cyber Warfare,” <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>

Cyber weapons bear a striking resemblance to nuclear weapons in some important ways. An enemy’s cyber attack would, like a nuclear strike, probably come without a clear warning. There are as yet no reliable defenses against either a cyber attack or a nuclear attack. Collateral damage from a nuclear attack would almost certainly be very extensive and would linger for an extended period.48 The direct and indirect effects of a cyber attack, while different in kind and degree, still could be widespread and indiscriminate.49¶ In other ways, cyber weapons are critically different from their nuclear counterparts. For one thing, the time frame for response to a cyber attack might be much narrower. A nuclear weapon delivered by a land-based ICBM could take 30 minutes to reach its target. An electronic attack would arrive instantaneously, and leave no time to consult with or even inform anyone outside the executive branch before launching a counterstrike, if that were U.S. policy.

# Case

## Solvency

### 1NC Circumvention

#### Secrecy means Congress would be ineffective—no solvency

Stephen Dycus—1AC Author—10, Professor, Vermont Law School, 8/11/10, “Congress’s Role in Cyber Warfare,” <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>

The National Security Act of 1947 23 showed Congress’s determination to exert some control over this nation’s intelligence apparatus. That determination was strengthened after the disclosure of widespread intelligence abuses by the CIA and other agencies.24¶ In 1991, in response to the Iran-Contra Affair, Congress adopted a measure directing the President to keep the congressional intelligence committees “fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity.”25 The term “intelligence activity” expressly includes “covert actions,”26 which additionally require a written finding by the President that they are “necessary to support identifiable foreign policy objectives of the United States and [are] important to the national security of the United States.”27 Intelligence activities are also understood to include “all activities that elements of the Intelligence Community are authorized to conduct pursuant to [Executive Order No. 12,333],” the executive charter for such activities.28 The “intelligence community” includes the Office of the Director of National Intelligence, CIA, NSA, other Defense Department intelligence components, and other federal intelligence elements,29 which are authorized to engage in, inter alia, intelligence collection and analysis and “activities to protect against international terrorism . . . and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents.”30 This broad mandate certainly encompasses many U.S. efforts to defend against cyber attack and to employ cyber weapons offensively. By this definition, most preparations for and conduct of cyber warfare should be reported to the intelligence committees as “intelligence activities.” It is significant that the reporting requirement in the 1991 law is not limited to agencies within the intelligence community. ¶ Yet this legislation provides no guarantee that Congress will receive the information it needs to play a meaningful role in the development or execution of cyber warfare policy. It is not known, for example, precisely what it means for the intelligence committees to be “fully and currently” informed, what kinds of intelligence activities are regarded as “significant” enough to report, or who decides.31 Other sections of the 1991 law call on all agencies involved in intelligence activities, not just the President, to keep the intelligence committees informed about those activities, but only “[t]o the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters.”32 The “due regard for” language might be invoked to keep Congress in the dark. ¶ Under the 1991 law, “covert actions,” those with respect to which “it is intended that the role of the United States Government will not be apparent or acknowledged publicly,”33 need only be reported to a small group of legislators known as the “Gang of Eight,”34 and then only in a “timely fashion,” a term not defined by statute.35 Characterization of U.S. planning and execution of electronic warfare as “covert” could enable reporting to the smaller group, making it more difficult for Congress to play a significant role.36 Moreover, any reporting might be delayed indefinitely.37

#### Military procedures means cyber operations wouldn’t be reported—kills solvency

Stephen Dycus—1AC Author—10, Professor, Vermont Law School, 8/11/10, “Congress’s Role in Cyber Warfare,” <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>

Another potential obstacle to congressional involvement is the reportedly common but statutorily unauthorized practice of informal reporting to an even smaller “Gang of Four” – the leaders of the intelligence committees – generally for sensitive non-covert intelligence activities.38¶ The Defense Department is heavily engaged in preparations for cyber warfare, having recently announced the establishment of a new U.S. Cyber Command.39 But congressional oversight of the work of this command could be hampered by the military’s reported practice of labeling its clandestine activities – those that are intended to be secret, but that can be publicly acknowledged if discovered or inadvertently revealed – as “operational preparation of the environment,” rather than intelligence activities, even though they may pose the same diplomatic and national security risks.40 As thus characterized, these activities might not be reported to the intelligence committees.41 Any oversight that occurred would be conducted instead by the House and Senate Armed Services Committees.42 Such a division of responsibilities might create dangerous confusion. ¶ Congressional involvement also might be frustrated by the statutory exclusion of “traditional . . . military activities or routine support to such activities” from the definition of “covert action.”43 If secret military preparations for cyber war are regarded as “traditional military activities,” under the rationale outlined above they might escape both the presidential findings requirement for covert actions and any reporting to the intelligence committees.44

#### The President would ignore the plan

Stephen Dycus—1AC Author—10, Professor, Vermont Law School, 8/11/10, “Congress’s Role in Cyber Warfare,” <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>

Congress’s active role in the development and implementation of cyber warfare policy is no guarantee of national security. The policy might be flawed in various ways. There is also a risk that whatever policy is adopted will not be properly executed or that its execution will have unintended results. The policy might be misunderstood or might not provide clear or appropriate guidance in the urgent circumstances facing its interpreter. The person charged with implementing the policy might make a mistake – for example, by interpreting a potential enemy’s electronic espionage as an attack. Available cyber weaponry might not work as planned. Or a purely defensive move by U.S. operators might be construed by another nation as offensive, and provoke an attack. Nor can the clearest policy, statutory or executive, guarantee compliance by an Executive determined to ignore it.71 The rules might be construed by the President in a way that reduces the importance of Congress’s role. Or they might be challenged in court.

### 1NC Norms Fail

#### Norms fail—cheating and miscalc

Stewart Baker 12, former official at the U.S. Department of Homeland Security and the National Security Agency, 5/1/12, “What Is the Role of Lawyers in Cyberwarfare?,” http://www.abajournal.com/magazine/article/what\_is\_the\_role\_of\_lawyers\_in\_cyberwarfare/

Former Prime Minister Stanley Baldwin summed up Britain’s strategic position in 1932 with a candor no American leader has dared to match in talking about cyberwar: “I think it is well also for the man in the street to realize that there is no power on earth that can protect him from being bombed, whatever people may tell him. The bomber will always get through. ... The only defense is in offense, which means that you have got to kill more women and children more quickly than the enemy if you want to save yourselves.”¶ The British may have been realists about air war, but Americans still hoped to head off the nightmare. The American tool of choice was international law. (Some things never change.) When war broke out on Sept. 1, 1939, President Franklin D. Roosevelt sent a cable to all the combatants seeking express limits on the use of airpower and expressing his view that “ruthless bombing from the air of civilians in unfortified centers of population … has sickened the hearts of every civilized man and woman, and has profoundly shocked the conscience of humanity. ... I am therefore addressing this urgent appeal to every government which may be engaged in hostilities publicly to affirm its determination that its armed forces shall in no event, and under no circumstances, undertake the bombardment from the air of civilian populations or of unfortified cities.”¶ Roosevelt had a pretty good legal case. The Hague Conventions on the Law of War, adopted just two years after the Wright Brothers’ first flight, declared that in bombardments “all necessary steps should be taken to spare as far as possible edifices devoted to religion, art, science, and charity, hospitals, and places where the sick and wounded are collected, provided they are not used at the same time for military purposes.” The League of Nations had recently declared that, in air war, “the intentional bombing of civilian populations is illegal.”¶ But FDR didn’t rely just on law. He asked for a public pledge that would bind all sides. Remarkably, he got it. The horror of aerial bombardment ran so deep in that era that England, France, Germany and Poland all agreed—before nightfall on the same day.¶ What’s more, they tried to honor their pledges. In a June 1940 order for Luftwaffe operations against Britain, Hermann Göring “stressed that every effort should be made to avoid unnecessary loss of life amongst the civilian population.”¶ It began to look like a great victory for the international law of war. All sides had stared into the pit of horrors that civilian bombing would open up. And all had stepped back.¶ It was exactly what the lawyers and diplomats now dealing with cyberwar hope to achieve.¶ But as we know, that’s not how this story ends. On the night of Aug. 24, a Luftwaffe air group made a fateful navigational error. Aiming for oil terminals along the Thames, they miscalculated, instead dropping their bombs in the civilian heart of the city of London.¶ It was a mistake. But that’s not how Churchill saw it. He insisted on immediate retaliation. The next night, British bombers hit targets in Berlin for the first time. The military effect was negligible, but the political impact was profound. Göring had promised that the Luftwaffe would never allow a successful attack on Berlin. The Nazi regime was humiliated, the German people enraged. Ten days later, Hitler told a wildly cheering crowd that he had ordered the bombing of London: “Since they attack our cities, we will extirpate theirs.”¶ The Blitz was on.¶ In the end, London survived. But the extirpation of enemy cities became a permanent part of both sides’ strategy. No longer an illegal horror to be avoided at all costs, the destruction of enemy cities became deliberate policy. Later in the war, British strategists would launch aerial attacks with the avowed aim of causing “the destruction of German cities, the killing of German workers, … the disruption of civilized life throughout Germany … the creation of a refugee problem on an unprecedented scale, and the breakdown of morale both at home and at the battle fronts.”¶ The Hague Conventions, the League of Nations resolution, even the explicit pledges given to President Roosevelt—all these “norms” for the use of airpower had been swept away by the logic of the technology and the predictable psychology of war.¶ So, why do today’s lawyers think that their limits on cyberwar will fare better than FDR’s limits on air war?¶ It beats me. If anything, they have a much harder task. Roosevelt could count on a shared European horror at the aerial destruction of cities. He used that to extract an explicit and reciprocal understanding from both sides as the war was beginning. We have no such understanding, indeed no such shared horror. Quite the contrary, for some of our potential adversaries, cyberweapons are uniquely asymmetric—a horror for us, another day in the field for them. It doesn’t take a high-tech infrastructure to maintain an army that is ready in a pinch to live on grass.¶ What’s more, cheating is easy and strategically profitable. American compliance will be enforced by all those lawyers. Our adversaries can ignore the rules and say—hell, they are saying—“We’re not carrying out cyberattacks. We’re victims too. Maybe you’re the attacker. Or maybe it’s Anonymous. Where’s your proof?”¶ Even if all sides were genuinely committed to limiting cyberwar, as all sides were in 1939, we’ve seen that the logic of airpower eventually drove all sides to the horror they had originally recoiled from. Each side felt that it had observed the limits longer than the other. Each had lawyerly justifications for what it did, and neither understood or gave credence to the other’s justifications. In that climate, all it took was a single error to break the legal limits irreparably.¶ And error was inevitable. Bombs dropped by desperate pilots under fire go astray. But so do cyberweapons. Stuxnet infected thousands of networks as it searched blindly for Natanz. The infections lasted far longer than intended. Should we expect fewer errors from code drafted in the heat of battle and flung at hazard toward the enemy?¶ Of course not. But the lesson for the lawyers and the diplomats is stark: Their effort to impose limits on cyberwar is almost certainly doomed.¶ No one can welcome this conclusion, at least not in the United States. We have advantages in traditional war that we lack in cyberwar. We are not used to the idea that launching even small wars on distant continents may cause death and suffering here at home. That is what drives the lawyers. They hope to maintain the old world. But they’re driving down a dead end.¶ If we want to defend against the horrors of cyberwar, we need first to face them with the candor of a Stanley Baldwin. Then we need to charge our military strategists, not our lawyers, with constructing a cyberwar strategy for the world we live in, not the world we’d like to live in.

#### Cyberweapons are inev --- US restraint does nothing --- norm setting is utopian

James Lewis 12, Director of the Technology and Public Policy Program at the Center for Strategic and International Studies, “Benefits Are Great, and the Risks Exist Anyway,” Oct 17, NYT, http://www.nytimes.com/roomfordebate/2012/06/04/do-cyberattacks-on-iran-make-us-vulnerable-12/benefits-are-great-and-the-risks-exist-anyway

Nor do cyberattacks against Iran increase the risk of damaging cyberattacks against the United States. It is true that we are defenseless; efforts to make us safer are hamstrung by self-interest, ideology and the gridlock of American politics. But we are no more vulnerable today than we were the day before the news. If someone decides to attack us, they may cite Iran as precedent, but it will only be to justify a decision they had already made.¶ We could ask whether the United States creates more problems for itself when it makes public a new weapon while potential opponents keep it secret. Four other countries can launch sophisticated and damaging cyber attacks -- including China and Russia -- and plan to use them in warfare. Another 30 nations are acquiring cyber weapons, including Iran and North Korea.¶ There is a very old argument for disarmament that holds that if the United States were to renounce some weapons -- usually nuclear weapons -- the world would be a better place. This utopianism has a revered place in American political thinking, but when humans invent weapons they rarely give them up, especially useful weapons whose components are easy to acquire. Cyberattack is now part of warfare, no different from any other weapon. The publicity around Stuxnet may complicate U.S. efforts to get international rules for the use of cyberattack, but the White House decided that tampering with Iran’s nuclear program was more important than possible risk to slow-moving negotiations.

#### Pandora’s box has already been opened --- cyber-war inevitable

Mikko Hypponen 12, an authority on cybercrime and one of Foreign Policy’s ‘Top 100 Global Thinkers,’ is the chief research officer at F-Secure Corporation, “A Pandora’s Box We Will Regret Opening,” June 5, NYT, http://www.nytimes.com/roomfordebate/2012/06/04/do-cyberattacks-on-iran-make-us-vulnerable-12/a-pandoras-box-we-will-regret-opening

If somebody would have told me five years ago that by 2012 it would be commonplace for countries to launch cyberattacks against each other, I would not have believed it. If somebody would have told me that a Western government would be using cybersabotage to attack the nuclear program of another government, I would have thought that's a Hollywood movie plot. Yet, that's exactly what's happening, for real.¶ Cyberattacks have several advantages over traditional espionage or sabotage. Cyber attacks are effective, cheap and deniable. This is why governments like them. In fact, if Obama administration officials would not have leaked the confirmation that the U.S. government (together with the Israelis) was behind Stuxnet, we probably would have never known for sure.¶ In that sense, it's a bit surprising that the U.S. government seems to have taken the credit ­ and the blame ­ for Stuxnet. Why did they do it? The most obvious answer seems to be that it's an election year and the voters like to see the president as taking on adversaries like Iran. But we don't really know.¶ The downside for owning up to cyberattacks is that other governments can now feel free to do the same. And the United States has the most to lose from attacks like these. No other country has so much of its economy linked to the online world.¶ Other governments are already on the move. The game is on, and I don't think there's anything we could do to stop it any more. International espionage has already gone digital. Any future real-world crisis will have cyberelements in play as well. So will any future war. The cyberarms race has now officially started. And nobody seems to know where it will take us.¶ By launching Stuxnet, American officials opened Pandora's box. They will most likely end up regretting this decision.

#### Can’t stop cyberweapons --- incentives to use are too high

Dr. Paul Kaminski 13, Chairman of the Defense Science Board Task Force on Resilient Military Systems & PhD from Stanford, “Department of Defense Defense Science Board Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,” January, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

There is no single silver bullet to solve the threat posed by cyber-attack or warfare. Solving this problem is analogous to previous complex national security and military strategy developments including counter U-boat strategy in WWII, nuclear deterrence in the Cold War , commercial air travel safety and countering IEDs in the Global War on terrorism . The risks involved with these challenges were never driven to zero, but through broad systems engineering of a spectrum of techniques, the challenges were successfully contained and managed. ¶ There are several characteristics of the cyber challenge that collectively thwart our attempts to discover a closed-form solution to this national security issue. First, DoD’s comprehensive dependence on this vulnerable technology is a magnet to U.S. opponents. DoD’s dependency is not going to be reduced and will continue to grow. Thus, the adversary is not going away and their attraction to this weakness will increase. This adversarial persistence yields a never-ending challenge.¶ Secondly, there are no technical approaches that will comprehensively protect DoD against a determined adversary. DoD’s diligent work over decades attempting to drive inherent vulnerability out of these systems and components has resulted in some progress, although DoD has barely begun to address the daunting problem of operationally introduced vulnerabilities into systems which is compounded by the large dependence on the global supply chain. In the face of the evolving cyber threat, DoD must recognize the limits to vulnerability reduction and the effectiveness of protection mechanisms and move to employ the threshold of “good enough ” and work to reduce overall risk by managing all three risk parameters from a systems perspective.¶ Third, while there are many tests to demonstrate the vulnerability or weakness in a system, there will never be a test that demonstrates or proves the security of a system. This fact reinforces the need to seek “good enough” and the enduring existence of residual uncertainty. ¶ Finally, because the opponent’s advantage in exploiting/compromising /attacking DoD’s information technology is substantial (game - changing), they will be highly motivated in their pursuit, innovative in their approach, and adaptive to U.S. strategy. The adversary gets a vote and this brings us back to the never-ending challenge. (However, they have many of the same risks to their systems).

## Cyber War

### AT: Cyber Arms Race

#### Uncontrollability of cyber-war is a neg warrant --- means countries won’t use them

Thomas P.M. Barnett 13, special assistant for strategic futures in the U.S. Defense Department's Office of Force Transformation from 2001 to 2003, is chief analyst for Wikistrat, March/April 2013, “Think Again: The Pentagon,” Foreign Policy, http://www.foreignpolicy.com/articles/2013/03/04/the\_pentagon?page=full

As for cyber serving as a stand-alone war-fifighting domain, there you'll find the debates no less theological in their intensity. After serving as senior managing director for half a dozen years at a software firm that specializes in securing supply chains, I'm deeply skeptical. Given the uncontrollable nature of cyberweapons (see: Stuxnet's many permutations), I view them as the 21st century's version of chemical weapons -- nice to have, but hard to use. Another way to look at it is to simply call a spade a spade: Cyberwarfare is nothing more than espionage and sabotage updated for the digital era. Whatever cyberwar turns out to be in the national security realm, it will always be dwarfed by the industrial variants -- think cyberthieves, not cyberwarriors. But you wouldn't know it from the panicky warnings from former Defense Secretary Leon Panetta and the generals about the imminent threat of a "cyber Pearl Harbor."¶ Please remember amid all this frenetic scaremongering that the Pentagon is never more frightened about our collective future than when it's desperately uncertain about its own. Given the rising health-care costs associated with America's aging population and the never-ending dysfunction in Washington, we should expect to be bombarded with frightening scenarios of planetary doom for the next decade or two. None of this bureaucratic chattering will bear any resemblance to global trends, which demonstrate that wars have grown increasingly infrequent, shorter in duration, and diminished in lethality. But you won't hear that from the next-warriors on the Potomac.

#### Zero impact to cyber arms race --- overwhelming consensus of qualified authors goes neg

- No motivation---can’t be used for coercive leverage

- Defenses solve---benefits of offense are overstated

- Too difficult to execute/mistakes in code are inevitable

- AT: Infrastructure attacks

- Military networks are air-gapped/difficult to access

- Overwhelming consensus goes neg

Colin S. Gray 13, Prof. of International Politics and Strategic Studies @ the University of Reading and External Researcher @ the Strategic Studies Institute @ the U.S. Army War College, April, “Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling,” U.S. Army War College Press, <http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1147.pdf>

CONCLUSIONS AND RECOMMENDATIONS: THE SKY IS NOT FALLING¶ This analysis has sought to explore, identify, and explain the strategic meaning of cyber power. The organizing and thematic question that has shaped and driven the inquiry has been “So what?” Today we all do cyber, but this behavior usually has not been much informed by an understanding that reaches beyond the tactical and technical. I have endeavored to analyze in strategic terms what is on offer from the largely technical and tactical literature on cyber. What can or might be done and how to go about doing it are vitally important bodies of knowledge. But at least as important is understanding what cyber, as a fifth domain of warfare, brings to national security when it is considered strategically. Military history is stocked abundantly with examples of tactical behavior un - guided by any credible semblance of strategy. This inquiry has not been a campaign to reveal what cy ber can and might do; a large literature already exists that claims fairly convincingly to explain “how to . . .” But what does cyber power mean, and how does it fit strategically, if it does? These Conclusions and Rec ommendations offer some understanding of this fifth geography of war in terms that make sense to this strategist, at least. ¶ 1. Cyber can only be an enabler of physical effort. Stand-alone (popularly misnamed as “strategic”) cyber action is inherently grossly limited by its immateriality. The physicality of conflict with cyber’s human participants and mechanical artifacts has not been a passing phase in our species’ strategic history. Cyber action, quite independent of action on land, at sea, in the air, and in orbital space, certainly is possible. But the strategic logic of such behavior, keyed to anticipated success in tactical achievement, is not promising. To date, “What if . . .” speculation about strategic cyber attack usually is either contextually too light, or, more often, contextually unpersuasive. 49 However, this is not a great strategic truth, though it is a judgment advanced with considerable confidence. Although societies could, of course, be hurt by cyber action, it is important not to lose touch with the fact, in Libicki’s apposite words, that “[i]n the absence of physical combat, cyber war cannot lead to the occupation of territory. It is almost inconceivable that a sufficiently vigorous cyber war can overthrow the adversary’s government and replace it with a more pliable one.” 50 In the same way that the concepts of sea war, air war, and space war are fundamentally unsound, so also the idea of cyber war is unpersuasive. ¶ It is not impossible, but then, neither is war conducted only at sea, or in the air, or in space. On the one hand, cyber war may seem more probable than like environmentally independent action at sea or in the air. After all, cyber warfare would be very unlikely to harm human beings directly, let alone damage physically the machines on which they depend. These near-facts (cyber attack might cause socially critical machines to behave in a rogue manner with damaging physical consequences) might seem to ren - der cyber a safer zone of belligerent engagement than would physically violent action in other domains. But most likely there would be serious uncertainties pertaining to the consequences of cyber action, which must include the possibility of escalation into other domains of conflict. Despite popular assertions to the contrary, cyber is not likely to prove a precision weapon anytime soon. 51 In addition, assuming that the political and strategic contexts for cyber war were as serious as surely they would need to be to trigger events warranting plausible labeling as cyber war, the distinctly limited harm likely to follow from cyber assault would hardly appeal as prospectively effective coercive moves. On balance, it is most probable that cyber’s strategic future in war will be as a contribut - ing enabler of effectiveness of physical efforts in the other four geographies of conflict. Speculation about cyber war, defined strictly as hostile action by net - worked computers against networked computers, is hugely unconvincing.¶ 2. Cyber defense is difficult, but should be sufficiently effective. The structural advantages of the offense in cyber conflict are as obvious as they are easy to overstate. Penetration and exploitation, or even attack, would need to be by surprise. It can be swift almost beyond the imagination of those encultured by the traditional demands of physical combat. Cyber attack may be so stealthy that it escapes notice for a long while, or it might wreak digital havoc by com - plete surprise. And need one emphasize, that at least for a while, hostile cyber action is likely to be hard (though not quite impossible) to attribute with a cy - berized equivalent to a “smoking gun.” Once one is in the realm of the catastrophic “What if . . . ,” the world is indeed a frightening place. On a personal note, this defense analyst was for some years exposed to highly speculative briefings that hypothesized how unques - tionably cunning plans for nuclear attack could so promptly disable the United States as a functioning state that our nuclear retaliation would likely be still - born. I should hardly need to add that the briefers of these Scary Scenarios were obliged to make a series of Heroic Assumptions. ¶ The literature of cyber scare is more than mildly reminiscent of the nuclear attack stories with which I was assailed in the 1970s and 1980s. As one may observe regarding what Winston Churchill wrote of the disaster that was the Gallipoli campaign of 1915, “[t]he terrible ‘Ifs’ accumulate.” 52 Of course, there are dangers in the cyber domain. Not only are there cyber-competent competitors and enemies abroad; there are also Americans who make mistakes in cyber operation. Furthermore, there are the manufacturers and constructors of the physical artifacts behind (or in, depending upon the preferred definition) cyber - space who assuredly err in this and that detail. The more sophisticated—usually meaning complex—the code for cyber, the more certain must it be that mistakes both lurk in the program and will be made in digital communication.¶ What I have just outlined minimally is not a reluc - tant admission of the fallibility of cyber, but rather a statement of what is obvious and should be anticipat - ed about people and material in a domain of war. All human activities are more or less harassed by friction and carry with them some risk of failure, great or small. A strategist who has read Clausewitz, especially Book One of On War , 53 will know this. Alternatively, anyone who skims my summary version of the general theory of strategy will note that Dictum 14 states explicitly that “Strategy is more difficult to devise and execute than are policy, operations, and tactics: friction of all kinds comprise phenomena inseparable from the mak - ing and execution of strategies.” 54 Because of its often widely distributed character, the physical infrastruc - ture of an enemy’s cyber power is typically, though not invariably, an impracticable target set for physical assault. Happily, this probable fact should have only annoying consequences. The discretionary nature and therefore the variable possible characters feasible for friendly cyberspace(s), mean that the more danger - ous potential vulnerabilities that in theory could be the condition of our cyber-dependency ought to be avoidable at best, or bearable and survivable at worst. Libicki offers forthright advice on this aspect of the subject that deserves to be taken at face value: ¶ [T]here is no inherent reason that improving informa - tion technologies should lead to a rise in the amount of critical information in existence (for example, the names of every secret agent). Really critical information should never see a computer; if it sees a computer, it should not be one that is networked; and if the computer is networked, it should be air-gapped.¶ Cyber defense admittedly is difficult to do, but so is cyber offense. To quote Libicki yet again, “[i]n this medium [cyberspace] the best defense is not necessarily a good offense; it is usually a good defense.” 56 Unlike the geostrategic context for nuclear-framed competition in U.S.–Soviet/Russian rivalry, the geographical domain of cyberspace definitely is defensible. Even when the enemy is both clever and lucky, it will be our own design and operating fault if he is able to do more than disrupt and irritate us temporarily.¶ When cyber is contextually regarded properly— which means first, in particular, when it is viewed as but the latest military domain for defense planning—it should be plain to see that cyber performance needs to be good enough rather than perfect. 57 Our Landpower, sea power, air power, and prospectively our space systems also will have to be capable of accepting combat damage and loss, then recovering and carrying on. There is no fundamental reason that less should be demanded of our cyber power. Second, given that cyber is not of a nature or potential character at all likely to parallel nuclear dangers in the menace it could con - tain, we should anticipate international cyber rivalry to follow the competitive dynamic path already fol - lowed in the other domains in the past. Because the digital age is so young, the pace of technical change and tactical invention can be startling. However, the mechanization RMA of the 1920s and 1930s recorded reaction to the new science and technology of the time that is reminiscent of the cyber alarmism that has flour - ished of recent years. 58 We can be confident that cyber defense should be able to function well enough, given the strength of political, military, and commercial motivation for it to do so. The technical context here is a medium that is a constructed one, which provides air-gapping options for choice regarding the extent of networking. Naturally, a price is paid in convenience for some closing off of possible cyberspace(s), but all important defense decisions involve choice, so what is novel about that? There is nothing new about accepting some limitations on utility as a price worth paying for security.¶ 3. Intelligence is critically important, but informa - tion should not be overvalued. The strategic history of cyber over the past decade confirms what we could know already from the science and technology of this new domain for conflict. Specifically, cyber power is not technically forgiving of user error. Cyber warriors seeking criminal or military benefit require precise information if their intended exploits are to succeed. Lucky guesses should not stumble upon passwords, while efforts to disrupt electronic Supervisory Con - trol and Data Acquisition (SCADA) systems ought to be unable to achieve widespread harmful effects. But obviously there are practical limits to the air-gap op - tion, given that control (and command) systems need to be networks for communication. However, Internet connection needs to be treated as a potential source of serious danger.¶ It is one thing to be able to be an electronic nuisance, to annoy, disrupt, and perhaps delay. But it is quite another to be capable of inflicting real persisting harm on the fighting power of an enemy. Critically important military computer networks are, of course, accessible neither to the inspired amateur outsider, nor to the malignant political enemy. Easy passing reference to a hypothetical “cyber Pearl Harbor” reflects both poor history and ignorance of contemporary military common sense. Critical potential military (and other) targets for cyber attack are extremely hard to access and influence (I believe and certainly hope), and the technical knowledge, skills, and effort required to do serious harm to national security is forbiddingly high. This is not to claim, foolishly, that cyber means absolutely could not secure near-catastrophic results. However, it is to say that such a scenario is extremely improbable. Cyber defense is advancing all the time, as is cyber offense, of course. But so discretionary in vital detail can one be in the making of cyberspace, that confidence—real confidence—in cyber attack could not plausibly be high. It should be noted that I am confining this particular discussion to what rather idly tends to be called cyber war. In political and strategic practice, it is unlikely that war would or, more importantly, ever could be restricted to the EMS. Somewhat rhetorically, one should pose the question: Is it likely (almost anything, strictly, is possible) that cyber war with the potential to inflict catastrophic damage would be allowed to stand unsupported in and by action in the other four geographical domains of war? I believe not.¶ Because we have told ourselves that ours uniquely is the Information Age, we have become unduly respectful of the potency of this rather slippery catch-all term. As usual, it is helpful to contextualize the al - legedly magical ingredient, information, by locating it properly in strategic history as just one important element contributing to net strategic effectiveness. This mild caveat is supported usefully by recognizing the general contemporary rule that information per se harms nothing and nobody. The electrons in cyber - ized conflict have to be interpreted and acted upon by physical forces (including agency by physical human beings). As one might say, intelligence (alone) sinks no ship; only men and machines can sink ships! That said, there is no doubt that if friendly cyber action can infiltrate and misinform the electronic informa - tion on which advisory weaponry and other machines depend, considerable warfighting advantage could be gained. I do not intend to join Clausewitz in his dis - dain for intelligence, but I will argue that in strategic affairs, intelligence usually is somewhat uncertain. 59 Detailed up-to-date intelligence literally is essential for successful cyber offense, but it can be healthily sobering to appreciate that the strategic rewards of intelligence often are considerably exaggerated. The basic reason is not hard to recognize. Strategic success is a complex endeavor that requires adequate perfor - mances by many necessary contributors at every level of conflict (from the political to the tactical). ¶ When thoroughly reliable intelligence on the en - emy is in short supply, which usually is the case, the strategist finds ways to compensate as best he or she can. The IT-led RMA of the past 2 decades was fueled in part by the prospect of a quality of military effec - tiveness that was believed to flow from “dominant battle space knowledge,” to deploy a familiar con - cept. 60 While there is much to be said in praise of this idea, it is not unreasonable to ask why it has been that our ever-improving battle space knowledge has been compatible with so troubled a course of events in the 2000s in Iraq and Afghanistan. What we might have misunderstood is not the value of knowledge, or of the information from which knowledge is quarried, or even the merit in the IT that passed information and knowledge around. Instead, we may well have failed to grasp and grip understanding of the whole context of war and strategy for which battle space knowledge unquestionably is vital. One must say “vital” rather than strictly essential, because relatively ignorant armies can and have fought and won despite their ig - norance. History requires only that one’s net strategic performance is superior to that of the enemy. One is not required to be deeply well informed about the en - emy. It is historically quite commonplace for armies to fight in a condition of more-than-marginal reciprocal and strategic cultural ignorance. Intelligence is king in electronic warfare, but such warfare is unlikely to be solely, or even close to solely, sovereign in war and its warfare, considered overall as they should be.¶ 4. Why the sky will not fall. More accurately, one should say that the sky will not fall because of hostile action against us in cyberspace unless we are improb - ably careless and foolish. David J. Betz and Tim Ste vens strike the right note when they conclude that “[i]f cyberspace is not quite the hoped-for Garden of Eden, it is also not quite the pestilential swamp of the imagination of the cyber-alarmists.” 61 Our understanding of cyber is high at the technical and tactical level, but re - mains distinctly rudimentary as one ascends through operations to the more rarified altitudes of strategy and policy. Nonetheless, our scientific, technological, and tactical knowledge and understanding clearly indicates that the sky is not falling and is unlikely to fall in the future as a result of hostile cyber action. This analysis has weighed the more technical and tactical literature on cyber and concludes, not simply on balance, that cyber alarmism has little basis save in the imagination of the alarmists. There is military and civil peril in the hostile use of cyber, which is why we must take cyber security seriously, even to the point of buying redundant capabilities for a range of command and control systems. 62 So seriously should we regard cyber danger that it is only prudent to as - sume that we will be the target for hostile cyber action in future conflicts, and that some of that action will promote disruption and uncertainty in the damage it will cause.¶ That granted, this analysis recommends strongly that the U.S. Army, and indeed the whole of the U.S. Government, should strive to comprehend cyber in context. Approached in isolation as a new technol - ogy, it is not unduly hard to be over impressed with its potential both for good and harm. But if we see networked computing as just the latest RMA in an episodic succession of revolutionary changes in the way information is packaged and communicated, the computer-led IT revolution is set where it belongs, in historical context. In modern strategic history, there has been only one truly game-changing basket of tech - nologies, those pertaining to the creation and deliv - ery of nuclear weapons. Everything else has altered the tools with which conflict has been supported and waged, but has not changed the game. The nuclear revolution alone raised still-unanswered questions about the viability of interstate armed conflict. How - ever, it would be accurate to claim that since 1945, methods have been found to pursue fairly traditional political ends in ways that accommodate nonuse of nuclear means, notwithstanding the permanent pres - ence of those means.¶ The light cast by general strategic theory reveals what requires revealing strategically about networked computers. Once one sheds some of the sheer wonder at the seeming miracle of cyber’s ubiquity, instanta - neity, and (near) anonymity, one realizes that cyber is just another operational domain, though certainly one very different from the others in its nonphysi - cality in direct agency. Having placed cyber where it belongs, as a domain of war, next it is essential to recognize that its nonphysicality compels that cyber should be treated as an enabler of joint action, rather than as an agent of military action capable of behav - ing independently for useful coercive strategic effect. There are stand-alone possibilities for cyber action, but they are not convincing as attractive options either for or in opposition to a great power, let alone a superpower. No matter how intriguing the scenario design for cyber war strictly or for cyber warfare, the logic of grand and military strategy and a common sense fueled by understanding of the course of strategic history, require one so to contextualize cyber war that its independence is seen as too close to absurd to merit much concern.

#### Diminishing marginal returns means there’s no impact

Martin C. Libicki 9, Senior Management Scientist @ RAND and adjunct fellow @ Georgetown’s Center for Security Studies, “Cyberdeterrence and Cyberwar,” RAND, <http://www.rand.org/pubs/monographs/MG877.html>

Strategic Cyberwar Is Unlikely to Be Decisive ¶ No one knows how destructive any one strategic cyberwar attack would be. Estimates of the damage from today’s cyberattacks within the United States range from hundreds of billions of dollars to just a few billion dollars per year. ¶ The higher dollar figures suggest that cyberattacks on enemy civilian infrastructures—strategic cyberwar—may be rationalized as a way to assist military efforts or as a way to coerce the other side to yield to prevent further suffering. But can strategic cyberwar induce political compliance the way, say, strategic airpower would? Airpower tends to succeed when societies are convinced that matters will only get worse. With cyberattacks, the opposite is more likely. As systems are attacked, vulnerabilities are revealed and repaired or routed around. As systems become more hardened, societies become less vulnerable and are likely to become more, rather than less, resistant to further coercion.

### AT: Impact

#### Cyberattacks won’t result in nuclear war --- airgapping solves

Green 2 – editor of The Washington Monthly (Joshua, 11/11, The Myth of Cyberterrorism, http://www.washingtonmonthly.com/features/2001/0211.green.html)

There's just one problem: There is no such thing as cyberterrorism--no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer. Nor is there compelling evidence that al Qaeda or any other terrorist organization has resorted to computers for any sort of serious destructive activity. What's more, outside of a Tom Clancy novel, computer security specialists believe it is virtually impossible to use the Internet to inflict death on a large scale, and many scoff at the notion that terrorists would bother trying. "I don't lie awake at night worrying about cyberattacks ruining my life," says Dorothy Denning, a computer science professor at Georgetown University and one of the country's foremost cybersecurity experts. "Not only does [cyberterrorism] not rank alongside chemical, biological, or nuclear weapons, but it is not anywhere near as serious as other potential physical threats like car bombs or suicide bombers." Which is not to say that cybersecurity isn't a serious problem--it's just not one that involves terrorists. Interviews with terrorism and computer security experts, and current and former government and military officials, yielded near unanimous agreement that the real danger is from the criminals and other hackers who did $15 billion in damage to the global economy last year using viruses, worms, and other readily available tools. That figure is sure to balloon if more isn't done to protect vulnerable computer systems, the vast majority of which are in the private sector. Yet when it comes to imposing the tough measures on business necessary to protect against the real cyberthreats, the Bush administration has balked. Crushing BlackBerrys When ordinary people imagine cyberterrorism, they tend to think along Hollywood plot lines, doomsday scenarios in which terrorists hijack nuclear weapons, airliners, or military computers from halfway around the world. Given the colorful history of federal boondoggles--billion-dollar weapons systems that misfire, $600 toilet seats--that's an understandable concern. But, with few exceptions, it's not one that applies to preparedness for a cyberattack. "The government is miles ahead of the private sector when it comes to cybersecurity," says Michael Cheek, director of intelligence for iDefense, a Virginia-based computer security company with government and private-sector clients. "Particularly the most sensitive military systems." Serious effort and plain good fortune have combined to bring this about. Take nuclear weapons. The biggest fallacy about their vulnerability, promoted in action thrillers like WarGames, is that they're designed for remote operation. "[The movie] is premised on the assumption that there's a modem bank hanging on the side of the computer that controls the missiles," says Martin Libicki, a defense analyst at the RAND Corporation. "I assure you, there isn't." Rather, nuclear weapons and other sensitive military systems enjoy the most basic form of Internet security: they're "air-gapped," meaning that they're not physically connected to the Internet and are therefore inaccessible to outside hackers. (Nuclear weapons also contain "permissive action links," mechanisms to prevent weapons from being armed without inputting codes carried by the president.) A retired military official was somewhat indignant at the mere suggestion: "As a general principle, we've been looking at this thing for 20 years. What cave have you been living in if you haven't considered this [threat]?" When it comes to cyberthreats, the Defense Department has been particularly vigilant to protect key systems by isolating them from the Net and even from the Pentagon's internal network. All new software must be submitted to the National Security Agency for security testing. "Terrorists could not gain control of our spacecraft, nuclear weapons, or any other type of high-consequence asset," says Air Force Chief Information Officer John Gilligan. For more than a year, Pentagon CIO John Stenbit has enforced a moratorium on new wireless networks, which are often easy to hack into, as well as common wireless devices such as PDAs, BlackBerrys, and even wireless or infrared copiers and faxes. The September 11 hijackings led to an outcry that airliners are particularly susceptible to cyberterrorism. Earlier this year, for instance, Sen. Charles Schumer (D-N.Y.) described "the absolute havoc and devastation that would result if cyberterrorists suddenly shut down our air traffic control system, with thousands of planes in mid-flight." In fact, cybersecurity experts give some of their highest marks to the FAA, which reasonably separates its administrative and air traffic control systems and strictly air-gaps the latter. And there's a reason the 9/11 hijackers used box-cutters instead of keyboards: It's impossible to hijack a plane remotely, which eliminates the possibility of a high-tech 9/11 scenario in which planes are used as weapons. Another source of concern is terrorist infiltration of our intelligence agencies. But here, too, the risk is slim. The CIA's classified computers are also air-gapped, as is the FBI's entire computer system. "They've been paranoid about this forever," says Libicki, adding that paranoia is a sound governing principle when it comes to cybersecurity. Such concerns are manifesting themselves in broader policy terms as well. One notable characteristic of last year's Quadrennial Defense Review was how strongly it focused on protecting information systems.

## Alliances

### 1NC A2/AD

#### New military doctrine means no A2AD threat

Jonathan Greenert 12, Chief of Naval Operations, 5/10/12, “Projecting Power, Assuring Access,” http://cno.navylive.dodlive.mil/2012/05/10/projecting-power-assuring-access/

There’s been attention recently about closing an international strait using, among other means, mines, fast boats, cruise missiles and mini-subs. These weapons are all elements of what we call an “Anti-Access /Area Denial (A2AD)” strategy. Keeping with my tenet of “Warfighting First,” I want to highlight for you how the Navy and Air Force have been planning to deal with A2AD threats like this today and into the future.¶ A goal of an A2AD strategy is to make others believe it can close off international airspace or waterways and that U.S. military forces will not be able (or willing to pay the cost) to reopen those areas or come to the aid of our allies and partners. In peacetime, this gives the country with the A2AD weapons leverage over their neighbors and reduces U.S. influence. In wartime, A2AD capabilities can make U.S. power projection more difficult. The areas where A2AD threats are most consequential are what I call “strategic maritime crossroads.” These include areas around the Straits of Hormuz and Gibraltar, Suez Canal, Panama Canal or Malacca Strait – but strategic crossroads can also exist in the air, on land, and in cyberspace.¶ To counter these strategies and assure U.S. freedom of action, Navy and Air Force spearheaded a comprehensive study, which included Army and Marine Corps participation, to bring forward a concept called Air Sea Battle (ASB). This concept identifies how we will defeat A2AD capabilities such as cyber attack, mines, submarines, cruise and ballistic missiles, and air defense systems and, where applicable, “natural access denial” such as weather, pollution, natural disaster, etc. The concept also describes what we will need to do these operations, especially as the threats improve due to technological advancements.¶ Air-Sea Battle relies on tightly coordinated operations across domains (air, land, maritime, undersea, space and cyberspace) to defeat A2AD capabilities, such as a submarine striking air defenses in support of Air Force bombers, Air Force stealth fighters destroying a radar site to prevent cruise missile attacks on Navy ships, or a Navy cryptologic technician (CT) confusing a radar system to allow an Air Force UAV to attack an enemy command center. This level of real-time coordination requires new approaches to developing systems, planning operations, and conducting command and control.¶ By working across domains, Air-Sea Battle takes advantage of unique U.S. advantages in global reach (long-range tankers, nuclear-powered carriers), and stealth above (F-22 and B-2) and below (SSN, SSGN) the sea. Putting Air Force and Navy capabilities together also creates new combinations of systems, or “kill-chains”, for warfighting operations that can add redundancy or make us more efficient. For example, a threat cruise missile could be detected by an Air Force E-3 AWACS or Navy E-2D Hawkeye, and if we invest in the right data links, either of them could cue an Air Force F-22, Aegis ship or Navy F/A-18 to engage the missile. This provides more “paths” we can follow to destroy the missile.¶ Using these integrated air and naval forces, the Air Sea Battle concept executes three main lines of effort:¶ Disrupt an adversary’s command, control, communications, computers and intelligence, surveillance and reconnaissance (C4ISR) – this reduces the adversary’s ability to find or target us with large raids; they will have to spread out their attacks to all our potential locations.¶ Destroy adversary weapons launch systems – To have sustained access to international seas and skies, we will eventually need to destroy the launchers on land, sea and in the air.¶ Defeat adversary weapons – until we destroy the launchers, our forces will kinetically or non-kinetically prevent the weapons launched at us from getting a hit.¶ We are using the Air Sea Battle concept to guide decisions in procurement, doctrine, organization, training, leadership, personnel and facilities. Our budgets for FY11, FY12 and now FY13 reflect hard choices that support Air-Sea Battle. In some cases we accepted reductions in capacity to ensure the needed capabilities were retained.

#### U.S. can adapt to A2/AD

James Dobbins 12, directs the International Security and Defense Policy Center at the RAND Corporation, previously served as American Ambassador to the European Community and Assistant Secretary of State, August/September 2012, “War with China,” Survival, Vol. 54, No. 4, p. 7-24

The increasing difficulty in ensuring direct defence could be consequential even if Sino-American hostilities are unlikely, for they could stimulate Chinese risk-taking, increase US inhibitions, and weaken the resolve of US allies and China’s neighbours to withstand greater Chinese insistence on sett ling disputes on Beijing’s terms. These trends are the result of underlying general technological progress; sustainable growth in military spending, reform and doctrinal adaptation within the People’s Liberation Army; and geographic distances for China and the United States. On the other hand, most of China’s neighbours are growing both economically and in technological sophistication, and some may choose to keep pace in quality (if not quantity) with Chinese advances in the military field.

Barring unforeseen technological developments that assure survivability for US forces and C4ISR capabilities, it will not be possible or affordable for the United States to buck these trends. As the defence of Taiwan is already becoming problematic for US forces (including for its carriers and nearby air bases), so will US operational options in the event of a confrontation with China over a North Korean collapse or a crisis in Southeast Asia. Over time, the United States is likely to become increasingly reliant on its more distant and less vulnerable capabilities. As US forward-operating survivability declines, strike range must increase. US military-operational emphasis in the Western Pacific will thus shift from geographically limited direct defence to more escalatory responses, and eventually, when even these will not suffice, from deterrence based on denial to deterrence based on the threat of punishment, with the speed of the shift likely to be more swift in Taiwan, followed by Northeast Asia and then Southeast Asia at a somewhat later date.

### 1NC South Korea Cyber Coop High

#### Cyber and military coop with South Korea is high—common interests

Kim 13 Eun-jung, Yonhap News Agency, 4/1/13, “S. Korean military to prepare with U.S. for cyber warfare scenarios,” http://english.yonhapnews.co.kr/national/2013/04/01/20/0301000000AEN20130401004000315F.HTML

In light of the massive attacks on the websites of major broadcasters and banks, South Korea's defense ministry said Monday it will increase cyber warfare forces and develop various deterrence scenarios in cooperation with the United States to better deal with emerging threats.¶ The ministry briefed President Park Geun-hye on the 2013 policy plan along with other security goals and assessments of North Korea's threats. Tensions on the peninsula have come to a boiling point in the wake of Pyongyang's saber-rattling over joint military drills held in the South.¶ The ministry said it will develop deterrence methods in response to various cyber attacks to enhance preparedness against an unprovoked attack both in times of war and peace. ¶ Calls to step up cyber warfare forces have risen, as recent attacks on broadcasters and banks -- the largest attack in two years -- brought fresh attention to potential cyber attacks in South Korea. The identity of the person or group behind the attacks is still under investigation, but military officials had speculated about possible links with North Korea, as it has repeatedly threatened to launch various attacks on Seoul in light of annual joint drills with the U.S. and new sanctions for its nuclear test.¶ "We will cooperate with the U.S. to prepare measures in cyber policy, technology and information," a senior ministry official said.¶ South Korea has about 400 personnel under the Cyber Command, a special unit launched in early 2010. The North is known to be running a cyber warfare unit composed of 3,000 elite hackers who are trained to break into other computer networks for information and spread computer viruses.¶ With the rising threat posed by the communist country, South Korean and U.S. forces will draft a customized deterrence strategy as early as July to test and review during the next joint drills, which kick off in late August. Militaries of the two nations will sign the plan in October, when their defense chiefs have an annual meeting called a Security Consultative Meeting (SCM) scheduled in October in Seoul, officials said.¶ Bilateral consultations have been underway to come up with a strengthened nuclear deterrence plan since last year, but Pyongyang's third nuclear test in February has brought new urgency to prepare a tailored strategy to counter the defiant communist state under its young leader Kim Jong-un.¶ South Korean military leaders had said they were considering destroying the North's nuclear facilities in advance in case of an imminent nuclear attack against South Korea.¶ The ministry also reaffirmed its commitment to develop an alternative joint operation structure to replace the Combined Forces Command, which is expected to be dissolved when Seoul regains its wartime operational command (OPCON) at the end of 2015.¶ "The ministry will prepare the OPCON transition to meet the December 2015 deadline and establish a new joint operation body," the ministry said in a statement.¶ The two sides will sign an alternative operation body in a meeting of military chiefs slated to meet in Washington next month, which will be finalized in the SCM.¶ In addition, the ministry vowed to speed up its planned deployment of ballistic missiles as well as an advanced missile interception system -- the so-called "kill chain" -- which is designed to detect, target and destroy missiles.¶ South Korea has been putting forth efforts to develop longer-range missiles after Seoul and Washington in October of last year agreed to nearly triple its missile range to 800 kilometers to better deter North Korean threats.¶ In addition, the military will push to adopt military spy satellites to keep closer tabs on the communist country and integrate its own missile defense shield program, dubbed the Korean Air and Missile Defense (KAMD).¶ South Korea currently operates Arirang-3, a multipurpose satellite, which provides geographical information on the Korean Peninsula, including North Korea's missile and nuclear test sites. However, it still relies on the U.S. for much of its intelligence due to the commercial satellite's limited vision and longer rotation period.¶ With adding reconnaissance satellites to its monitoring capabilities, the military hopes to increase its surveillance of major North Korean military facilities to better anticipate aggressive actions by the communist state.

### 1NC Allied Coop High

#### Allied cyber coop high

John Reed 12, national security reporter for Foreign Policy, 9/10, “U.S. swapping cyber notes with allies,” http://killerapps.foreignpolicy.com/posts/2012/09/10/us\_now\_swapping\_notes\_on\_cyber\_attacks\_with\_closest\_allies

The Defense Department has reached what Pentagon officials describe a key agreement with some of the United States' closest international allies to share information in the cyber realm.¶ The agreement allows the Pentagon to quickly share broad amounts of information on cyber attacks with the four other members of the so-called Five Eyes intelligence-sharing group (formally known as the UKUSA Agreement): the United Kingdom, Canada, Australia, and New Zealand.¶ "We have far more ability to share, particularly in relation to network defense and information assurance, than we've ever had previously. That's very positive," said Marine Corps Maj. Gen. George Allen, director of plans and policy for U.S. Cyber Command said on August 16. "I think you'll see a far better partnership with our coalition partners than you've ever seen" as the Five Eyes countries integrate the information into their exercises and planning.¶ "At this point it's not a full treaty because it's more an operational type cooperation; it's through a policy type memorandum of understanding," Eric Rosenbach, deputy assistant secretary of defense for cyber policy told Killer Apps during a Sept. 4 interview while discussing how the U.S. shares cyber information with its closest allies. The cyber information-sharing agreement falls under a 2003 MOU on general information sharing between the Five Eyes, according to a DoD spokesman.¶ The agreement will speed up information sharing, which is crucial in cyber, Allen said: "It's extremely important because you may see a certain threat in the U.K. that we haven't yet seen in the U.S. and you want to be able to try to bolster your defenses by seeing that before it hits us. We still have a long way to go on near real time information sharing but the technology is there."¶ Agreements like the one between the Five Eyes are being reached as a result of a National Disclosure Policy regarding the sharing of sensitive cyber information that was enacted "just a couple of months ago," said Allen.¶ The new policy also allows less extensive information sharing with other U.S. allies around the globe, according to Allen.¶ "In some cases [info-sharing agreements are part of] a bilateral relationship, depending upon the country, in other cases we have agreements with groups of countries that come together," such as the Five Eyes, explained DoD's Chief Information Officer, Teri Takai to Killer Apps during a Sept. 4 interview.¶ Defense officials say that information sharing partnerships like this one are badly needed to defeat cyber attacks since the cyber domain transcends national borders. Not only can attacks originate abroad, hackers in one country going after networks in another can often disguise their attacks to appear as if they are emanating from servers in a third nation. Furthermore, not all countries have the ability to detect cyber threats and attacks quickly. This means that a country whose servers are hijacked may not even know that it is hosting an attack.¶ "The more we can build a solid relationship with a partner, the more we're going to be able to crack the code in rapid information sharing, indications, and warnings with those partners," said Army Maj. Gen. John Davis, the military's top advisor for cyber to the undersecretary of defense for policy on August 15.¶ "If we can do that, we can get these partners to rapidly react to [cyber attacks] that we may be seeing that they may not see. We may be able to tip and cue them so that they can take action. If some of their equipment is being hijacked, we can inform them, and if we have good working relationships we can leverage that to get them to take action rather than relying on any type of U.S. government activity because then you run into issues of sovereignty and that can be very complex," he said.¶ To that end, the Five Eyes countries are already sharing lessons learned on how to defend networks, according to Davis.¶ "We are able to leverage lessons from across the five eyes, and in fact, where we find some of these nations that have particular skill or abilities in one area or another, may lead a common forum to develop that and share it with the rest of the group," said Davis.

### AT: Taiwan

#### China wants a peaceful rise---any threats are just saber rattling---US also deters

Vu Duc ‘13 "Khanh Vu Duc is a Vietnamese-Canadian lawyer who researches on Vietnamese politics, international relations and international law. He is a frequent contributor to Asia Sentinel and BBC Vietnamese Service, "Who's Bluffing Whom in the South China Sea?" www.asiasentinel.com/index.php?option=com\_content&task=view&id=5237&Itemid=171

Nevertheless, **it remains unlikely that any conflict** between China and Japan, Philippines, or Vietnam will **amount to more than saber rattling and harsh words.** Even a "small" police action against the Philippines or Vietnam over the Spratly Islands, however successful for China, would have severe consequences. Any Chinese use of force **would realize the fears of every state** in the region. Moreover, **Beijing's hope for a peaceful rise would be immediately set back, if not ruined**.

Presently, tensions are already running high; however, any clear displays of Chinese aggression would simply add fuel to the fire. Countries such as the Philippines and Vietnam would then be able to turn some of their neighbours—previously skeptical, if not cautious, about standing in opposition to China—and convince these states to protest openly. Any goodwill China possessed among some of these countries would evaporate as the Philippines and/or Vietnam make their case.

However, of all the scenarios of a conflict involving China, what can be certain is the potential for an immediate American intervention. While it is questionable that the US would directly intervene in any skirmish between nations, it is likely that Washington would use the conflict as an excuse for deploying a larger, if not more permanent, security force in Asia-Pacific. Although an increased American footprint would not be welcomed by all in the region, **the US would prove to be an appropriate balance against China.**

# Block

## CP

### 2NC Guidelines Solve/Aff Fails

#### Congress should set guidelines—that solves while preserving flex

Stephen Dycus—1AC Author—10, Professor, Vermont Law School, 8/11/10, “Congress’s Role in Cyber Warfare,” <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>

Congress accordingly needs to work closely with the executive branch in the development of a policy for this new kind of conflict. Such a policy ought to reflect the distinctive technology and strategy of digital warfare, and it should be reviewed constantly as the technology evolves. Like other regulations dealing with dynamic subjects, this policy should include general approaches that reflect this nation’s broad strategic concerns and fundamental values. But the policy must also be crafted with enough flexibility to allow those charged with its execution to deal with future developments that cannot now be predicted. And it should set out a procedure for such adaptive use by identifying, for example, who must be consulted under what circumstances, and who will make the final critical decisions. ¶ It is at least theoretically possible that Congress could play an active, real-time role in the implementation of whatever cyber warfare policy is adopted. The policy might, for example, like the War Powers Resolution, require consultation “in every possible circumstance.”50 But it seems more likely that a digital war would begin and end before any notice could ever reach Capitol Hill. Congress therefore needs to lay down clear guidelines, with as much flexibility as prudence requires, for executive branch officials to follow if consultation is not reasonably possible. And Congress should require a prompt and full account of every significant use of cyber weapons.

### Consult Kills Rapid Response

#### Consultation kills rapid response

Stephen Dycus—1AC Author—10, Professor, Vermont Law School, 8/11/10, “Congress’s Role in Cyber Warfare,” <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>

8. Require consultation with the designated congressional committees in every possible instance before any significant use of cyber weapons.(Footnote 64 Begins) ¶ 64 . A National Research Council study suggests possible advance congressional approval of some offensive uses of cyber weaponry based on, inter alia, the scale of a contemplated attack, the target, and other circumstances. NATIONAL RESEARCH COUNCIL, supra note 3, at 56. Because of the possible need for immediate action, advance approval is not recommended here. Possible criteria for determining when a contemplated use is “significant” for these purposes are suggested supra note 31.

## Cp 2

### AT: Russia Add-on

#### Transparent cyber cooperation with Russia high—answers their internal specifically

Amber Corrin 6/19/13, a staff writer covering defense and national security, “U.S. teams with unexpected new cyber ally,” http://fcw.com/articles/2013/06/19/russia-cybersecurity-cooperation.aspx

The United States is pushing forward in bilateral cooperation efforts with Russia that build on Cold War-era strategies and, officials hope, strengthen the countries' global cybersecurity stances. But will the renewed, digital-era alliance have broader implications?¶ News of the U.S.-Russian agreement came out of the recent G-8 summit held in Northern Ireland, where President Barack Obama and Russian President Vladimir Putin notably disagreed on the conflict in Syria and other high-profile issues. The two did, however, establish plans to improve cyber collaboration and foster trust between the two countries, according to a June 18 White House fact sheet.¶ "Our two nations now are leading the way in extending traditional transparency and confidence-building measures to reduce the mutual danger we face from cyber threats," the fact sheet notes. "These kinds of exchanges are important to ensuring that as we develop defense policy in this dynamic domain, we do so with a full understanding of one another's perspectives."¶ The information and communications technology security cooperation agreement involves an emphasis on increased dialog between senior officials. It includes the creation of a new working group between the two countries that will focus on identifying information and communication technology threats and coming up with potential solutions. The group is set to begin work within 30 days.¶ Other plans include steps in confidence-building "designed to increase transparency and reduce the possibility that a misunderstood cyber incident could create instability or a crisis in our bilateral relationship," according to the fact sheet.¶ Among the steps are the formation of links between the U.S. Computer Emergency Response Team and its Russian counterpart to exchange cybersecurity information. The two governments additionally are reviving Nuclear Risk Reduction Center links created in 1987 between the United States and the former Soviet Union that will allow access to each other's authorities on potential cyber incidents.¶ Another Cold War-era relic making a digital-era comeback is the so-called nuclear hotline, an already established direct communications system to be used in case of a security crisis.¶ "There have been ongoing efforts to apply concepts leftover from the nuclear era, transferring them to this era. For the most part it's led to mistakes, bad policy decisions and confusion – such as [the strategy of] deterrence being applied from the nuclear age to the cyber age," said Scott Borg, director and chief economist of U.S. Cyber Consequences Unit, an independent research firm. "In this case, ironically, it works."

## Alliances

### AT: SCS

#### No SCS war

VOA 12 – Voice of America News, 9/4/12, “Will South China Sea Disputes Lead to War?,” http://www.voanews.com/content/south-china-sea-war-unlikely/1501780.html

“A minor military clash in the South China Sea is, rather worryingly, a distinct and growing possibility,” according to Ian Storey from the Institute of Southeast Asian Studies in Singapore. ¶ Storey, an expert on Asia Pacific maritime security, goes even further. He envisions the possibility of differences over fishing rights or energy exploration turning into a military clash. ¶ “Caused by miscalculation, misperception or miscommunication, it’s just a question of time before one these skirmishes results in loss of life,” Storey said. ¶ A South China Sea War is Unlikely¶But that doesn’t mean a war. Storey said an escalation into full-blown conflict is unlikely.¶ “It is in no country’s interests to spill blood or treasure over this issue – the costs far outweigh the benefits,” Storey said. ¶ Other experts agree.¶ James Holmes of the U.S. Naval War College says admires how China has been able to get its way in spreading it claims of sovereignty without becoming a bully.¶ “[China] gradually consolidated the nation's maritime claims while staying well under the threshold for triggering outside -most likely American -intervention,” said Holmes.¶ “Is war about to break out over bare rocks? I don't think so.” writes Robert D. Kaplan, Chief Political Strategist for the geopolitical analysis group Stratfor.¶ Kaplan, however, doesn’t give much hope for negotiations. “The issues involved are too complex, and the power imbalance between China and its individual neighbors is too great,” he said. For that reason, Kaplan says China holds all the cards.¶ Kaplan doesn’t look for Chinese military aggression against other claimants. That, he says, would be counterproductive for its goals in the region.¶ “It would completely undermine its carefully crafted ‘peaceful rise’ thesis and push Southeast Asian countries into closer strategic alignment with the US,” said Kaplan.

### AT: NoKo Collapse

#### Zero risk of great power war and Kim’s death makes it inev

Barnett 9 – Thomas P. M. Barnett, visiting scholar at the University of Tennessee's Howard Baker Center, March 23, 2009, “Threat of Great Power War Recedes,” online: http://www.koreatimes.co.kr/www/news/opinon/2009/03/137\_41779.html

As for Kim Jong-il's North Korea, that fake state won't long survive the Dear Leader's death, made all the more imminent by a recent stroke that Pyongyang strenuously denied.

Whatever the timetable, the key point here is that none of the concerned great powers expects North Korea's collapse will trigger war among them. Their long-standing multilateral talks have demystified that dire scenario.

#### No Korean war---laundry list---(rational regime, empirics, military inferiority, and it’s all just domestic propaganda)

Fisher ‘13 Max, Foreign Policy Writer @ Washington Post & Former Editor at the Atlantic, “Why North Korea loves to threaten World War III (but probably won’t follow through)” http://www.washingtonpost.com/blogs/worldviews/wp/2013/03/12/why-north-korea-loves-to-threaten-world-war-iii-but-probably-wont-follow-through/

North Korea is indeed a dangerous rogue state that has, in the recent past, staged small-scale but deadly attacks on South Korea without provocation. In March 2010, a South Korean navy ship was attacked by a ship of unknown origin, killing 46 on board; though North Korea denied responsibility, an investigation concluded it was likely responsible. A few months later, North Korea fired over 100 artillery shells at Yeonpyeong Island, killing two civilians and wounding 19.

But is North Korea really an irrational nation on the brink of launching “all-out war,” a mad dog of East Asia? Is Pyongyang ready to sacrifice it all? Probably not. The North Korean regime, for all its cruelty, has also shown itself to be **shrewd, calculating, and single-mindedly obsessed with its own self-preservation**. The regime’s past behavior **suggests pretty strongly** that these **threats are empty**. But they still matter.

**For years**, North Korea has threatened the worst and, despite all of its apparent readiness, never gone through with it. So why does it keep going through these macabre performances? We can’t read Kim Jong Eun’s mind, but the most plausible explanation has to do with internal North Korean politics, with trying to set the tone for regional politics, and with forcing other countries (including the United States) to bear the costs of preventing its outbursts from sparking an unwanted war.

Starting World War III or a second Korean War would not serve any of Pyongyang’s interests. Whether or not it deploys its small but legitimately scary nuclear arsenal, North Korea could indeed cause substantial mayhem in the South, whose capital is mere miles from the border. But the North Korean military is antiquated and inferior; it wouldn’t last long against a U.S.-led counterattack. No matter how badly such a war would go for South Korea or the United States, it would almost **certainly end with the regime’s total destruction**.

Still, provocations and threats do serve Pyongyang’s interests, even if no one takes those threats very seriously. It helps to rally North Koreans, particularly the all-important military, behind the leader who has done so much to impoverish them. It also helps Pyongyang to control the regional politics that should otherwise be so hostile to its interests. Howard French, a former New York Times bureau chief for Northeast Asia whom I had the pleasure of editing at The Atlantic, explained on Kim Jong Il’s death that Kim had made up for North Korea’s weakness with canny belligerence:

The shtick of apparent madness flowed from his country’s fundamental weakness as he, like a master poker player, resolved to bluff and bluff big. Kim adopted a game of brinkmanship with the South, threatening repeatedly to turn Seoul into a “sea of flames.” And while this may have sharply raised the threat of war, for the North, it steadily won concessions: fuel oil deliveries, food aid, nuclear reactor construction, hard cash-earning tourist enclaves and investment zones.

At the risk of insulting Kim Jong Eun, it helps to think of North Korea’s provocations as somewhat akin to a child throwing a temper tantrum. He might do lots of shouting, make some over-the-top declarations (“I hate my sister,” “I’m never going back to school again”) and even throw a punch or two. Still, you give the child the attention he craves and maybe even a toy, **not because you think the threats are real** or because he deserves it, but because you want the tantrum to stop.

## Solvency

### Squo Solves

#### Squo solves --- new USFG cyber guidelines

Tim Stevens 12, Associate for the Centre for Science and Security Studies and an Associate Fellow of the International Centre for the Study of Radicalisation and Political Violence, PhD candidate @ King’s College London, MA in War Studies, “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace,” Contemporary Security Policy, Vol. 33, Iss. 1, Apr. 13, Taylor and Francis Online

In May 2011, the US International Strategy for Cyberspace answered the President's call and was the first US policy document to provide, in Secretary Clinton's introductory words, ‘an approach that unifies our engagement with international partners on the full range of cyber issues’.82 Norms are promoted in the context of ‘applying the broad expectations of peaceful and just interstate conduct to cyberspace’ in order to effect ‘stability’, as obtains in ‘other spheres of international relations’.83 The document stresses the collaborative and cooperative aspects of global normative change whilst reiterating states' rights to self-defence consistent with the UN Charter. Norms extended not only to technical issues of network functionality but also to ‘upholding fundamental freedoms’ consistent with several high-profile speeches by Secretary Clinton on this topic,84 and a range of other responsibilities of states to the privacy of their citizens and so on. Importantly, the document stated, ‘[a]dherence to such norms brings predictability to state conduct, helping prevent the misunderstandings that could lead to conflict’.85 Norms are therefore principally, although not exclusively, to be understood as regulative norms concerned with preventing inter-state conflict, and can be framed as a form of norms-based deterrence.

## DA

### Speed

#### The structure of Congress inherently favors delay and inaction --- that’s awful for crisis response

John Yoo 4, Emanuel S. Heller Professor of Law @ UC-Berkeley Law, visiting scholar @ the American Enterprise Institute, former Fulbright Distinguished Chair in Law @ the University of Trento, served as a deputy assistant attorney general in the Office of Legal Council at the U.S. Department of Justice between 2001 and 2003, received his J.D. from Yale and his undergraduate degree from Harvard, “War, Responsibility, and the Age of Terrorism,” UC-Berkeley Public Law and Legal Theory Research Paper Series, http://works.bepress.com/cgi/viewcontent.cgi?article=1015&context=johnyoo

In order to weigh the advantages of the Congress-first approach, it is also important to understand its potential costs. The costs may not be obvious, since grounding the use of force in ex ante congressional consent bears a close resemblance to the process for enacting legislation. The legislative process increases the costs of government action. It is heavily slanted against the enactment of legislation by requiring the concurrence not just of the popularly elected House but also the state-representing Senate and the President. This raises decision costs by increasing the delay needed to get legislative concurrence, requiring an effort to coordinate between executive and legislature, and demanding an open, public discussion of potentially sensitive information. Decision costs are not encapsulated merely in the time-worn hypotheticals that ask whether the President must go to Congress for permissions to launch a preemptive strike against a nation about to launch its own nuclear attack. Rather, these decision costs might arise from delay in using force that misses a window of opportunity, or one in which legislative discussion alerts an enemy to a possible attack, or the uncertainty over whether congressional authorization will be forthcoming.

#### Congress is too slow to respond to 21st century threats --- executive deference is critical

Andrew Rudalevige 6, the Thomas Brackett Reed Professor of Government @ Bowdoin College, “The New Imperial Presidency,” UMich-Ann Arbor Press, Book, p. 264-67

That fragmentation is most obvious at the other end of Pennsylvania Avenue. Despite common grammatical usage, including in this book, Congress is not an “it” but a “they.” That is, Congress is not singular but plural and a fractious plural at that. The geographic basis of House representation— the “territorial imperative”—means that no two House members share identical interests.6 The distinctive constituencies and terms of the House and Senate generate few overlapping sympathies across the chambers. Sequential majorities and supermajorities are required for action, but only a small minority for inaction. This became even more true after the application of reforms in the 1970s designed to apply the openness and decentralization aimed at the executive branch to Congress itself. The reforms enhanced the power of subcommittees and gave party rank-and-‹le more power to override seniority in selecting committee chairs. What nineteenth-century observers like Woodrow Wilson condemned as “committee government” often atomized further into “subcommittee government” instead. As a result, one scholar noted, members of Congress can make laws “only with sweat patience, and a remarkable skill in the handling of creaking machinery.” But stopping laws is a feat “they perform daily, with ease and infinite variety.”7¶ Thus even an alert and aggressive Congress has endemic weaknesses.8 Its large size and relative lack of hierarchy hamper quick decision making. The specialized jurisdictions inherent in the committee system, so necessary for dividing labor, also divide issues and make their comprehensive consideration across functional lines nearly impossible. (Nor do House members’ two-year terms give much incentive for long-term planning.) For similar reasons Congress has difficulty in planning and agenda setting. The ready acceptance of the idea of a presidential legislative program after World War II was partly a question of legislative convenience, a way to weed through innumerable proposals and provide a focus for limited floor time. Finally, with so many members, each seeking press attention, Congress also finds it hard to keep a secret. As President George H. W. Bush’s counsel, Boyden Gray, put it, “any time you notify Congress, it’s like putting an ad in the Washington Post. Notification is tantamount to declaration.”9¶ In short, Congress has the problems inherent to any body of individuals that must take collective action. The decisions that are rational for a single member—especially those aimed at gaining particular benefits for his or her district—are not always good decisions for the body as a whole.10 James Madison wrote as early as 1791 that whenever a question of “general. . . advantage to the Union was before the House . . . [members] commonly resorted to local views.” Then, as now, coalition building had to overcome decentralized inertia, with the result that governing often comes down to, in the words of LBJ budget official Charles Schultze, “a lot of boodle being handed out in large numbers of small boodle.”11¶ Worse, fragmentation is not limited to the legislative branch. After all, Congress created most of the executive branch as well—and in its own image. The “politics of bureaucratic structure” result in a bureaucracy far different than what organization theorists would draw up on a blank page, one rarely aligned along functional lines or with clear lines of executive authority. Legislative majorities hope to institutionalize their own interests in government agencies and to structurally insulate those preferences against future majorities seeking to meddle. They hope to gain access to the bureaucratic decision-making process and to influence it whenever desirable. They hope to gain points with constituents for fixing the errors agencies make, perhaps to the point of structuring agencies that cannot help but make errors. If nothing else, the historical pattern of executive branch development has spurred a particular array of legislative committees—and organized special interests linked to both.12¶ As the size and scope of the national government grew, its organizational inefficiencies became more obvious and more meaningful. This in turn focused increased attention on the need for direction and coordination— for a chief executive who could actually manage the executive branch. The areas of homeland security and intelligence analysis are only the most recent cases where failures of communication or analysis within the bureaucracy have magnified the need for those qualities.¶ Globalization in some ways highlights the continuing limits of the presidency’s authority: its incumbent is not, after all, president of the world. Yet the practical advantages of presidential leadership vis-à-vis the legislature, at least, are further magnified in an era where rapid transportation, instantaneous communication, and huge flows of trade have changed the context of governance in ways that play to presidential strengths. Both opportunities and threats arise quickly and demand immediate response. Their resolution requires a broad national view, not territorialism; resident expertise, not the give-and-take of log-rolling compromise. Further, if, as Richard Neustadt suggested, the cold war’s omnipresent fear of nuclear war made the president for a time the “final arbiter” in the balance of power, the rise of rogue states and nonstate actors with access to similar weaponry ups the ante again. In this one sense at least the “modern presidency” described earlier may have given way to a “postmodern” one.13 As the Bush administration argued to the Supreme Court on behalf of the president’s power to designate enemy combatants,¶ The court of appeals’ attempt to cabin the Commander-in-Chief authority to the conduct of combat operations on a traditional battlefield is particularly ill-considered in the context of the current conflict. . . . The September 11 attacks not only struck targets on United States soil; they also were launched from inside the Nation’s borders. The “full power to repel and defeat the enemy” thus necessarily embraces determining what measures to take against enemy combatants found within the United States. As the September 11 attacks make manifestly clear, moreover, al Qaeda eschews conventional battlefield combat, yet indiicts damage that, if anything, is more devastating.14

### Cred

#### Plan allows Congress to vocally oppose crisis intervention --- or they literally don’t solve anything--- that destroys international perception of U.S. resolve

Waxman 8/25/13 Matthew Waxman, Professor of Law @ Columbia and Adjunct Senior Fellow for Law and Foreign Policy @ CFR, citing William Howell, Sydney Stein Professor in American Politics @ U-Chicago, and Jon Pevehouse, Professor of Political Science @ U-Wisconsin-Madison, “The Constitutional Power to Threaten War,” Forthcoming in Yale Law Journal, vol. 123, August 25, 2013, SSRN

When members of Congress vocally oppose a use of force, they undermine the president’s ability to convince foreign states that he will see a fight through to the end. Sensing hesitation on the part of the United States, allies may be reluctant to contribute to a military campaign, and adversaries are likely to fight harder and longer when conflict erupts— thereby raising the costs of the military campaign, decreasing the president’s ability to negotiate a satisfactory resolution, and increasing the probability that American lives are lost along the way. Facing a limited band of allies willing to participate in a military venture and an enemy emboldened by domestic critics, presidents may choose to curtail, and even abandon, those military operations that do not involve vital strategic interests.145

#### 

### Link---Congress---Secrecy

#### Secrecy is key to effective cyber deterrence and response

John Mowchan 11, Lt Col, October, “Don’t Draw the (Red) Line,” http://www.usni.org/magazines/proceedings/2011-10/dont-draw-red-line

Those arguing for establishing red lines fail to comprehend the complexity of the digital domain, in which adaptation and anonymity are the norm. The United States is better served in the long run by not establishing such thresholds, for four reasons. First, not doing so allows government leaders the latitude to tailor response options

based on a hostile act, its physical and digital effects, and how it relates to the current state of affairs in the international system. As retired Air Force General Kevin Chilton remarked in 2009 as commander, U.S. Strategic Command, “I don’t think you take anything off the table when you provide [response] options to the president to decide. Why would we constrain ourselves on how we would respond [to hostile acts in cyberspace]?” 15¶ Such an approach does not differ from the way the United States addresses hostile acts in other domains. If red lines are established, we will be compelled to respond to each threat that crosses the line, which is unrealistic, given that our computer networks are subjected to millions of probes, scans, and attacks on a daily basis. Even if red lines are narrowly focused (e.g., employing military force if a cyber attack results in the deaths of U.S. citizens), the first time the United States fails to respond accordingly, it will undermine the credibility and deterrence effect of our other capabilities.¶ A second reason in favor of ambiguity is that if our adversaries know our response to such acts, they will adjust accordingly. Because neither the national nor the defense strategy explicitly defines a hostile act in cyberspace or exactly how the United States will respond, this leaves it open to interpretation. As one military official remarked, “If you shut down our power grid, maybe we will put a missile down one of your smokestacks.” 16 In addition, hostile actors may perceive a green light for certain acts that do not cross a particular response threshold. While one such act below this threshold may not be harmful to U.S. interests, what if 100 million are? Again, maintaining ambiguity concerning when, how, and to what extent to respond gives the United States greater latitude.¶ Third, because cyberspace is a global domain that emphasizes open access, the free flow of information, and anonymity, it is extremely difficult to determine where the threat or attack originated. For example, U.S. military networks are probed more than six million times a day by assailants operating in one corner of the world using computer networks or servers in another corner. Most perpetrators are never identified, except for a computer Internet protocol address or a one-time user alias. Army General Keith Alexander, commander of U.S. Cyber Command and Director, National Security Agency, emphasized this challenge, saying, “Too often, the military discovers through forensics that network probes have been successful [and] as a consequence, response becomes policing up after the fact versus mitigating it real time.” 17 If red lines demand a timely response and there is no one to pin responsibility on, then how can a response be implemented?¶ Finally, even if the source of the attacks is determined in a timely manner, automatic triggers for a response, particularly those that employ military force, could create negative second- and third-order effects that make a bad situation even worse. Given that nation states pose the greatest threat to U.S. networks, red lines that automatically result in a response could escalate an already volatile situation.¶ For example, in 2009 individuals in China and Russia penetrated computer networks operating parts of the U.S. electrical power grid. 18 They reportedly inserted malware that could destroy infrastructure components. Although their identities or associations with the Russian and Chinese governments were not disclosed, it validates the point that response options must be tailored. If Russia or China, two nuclear powers, were responsible, a U.S. response would be markedly different than if they had they been conducted by a non-nuclear state. Clearly the diplomatic, information, and economic instruments of national power versus military force would receive more emphasis with China or Russia for what could be considered a hostile act in cyberspace.¶ Given the complex and indeterminate 21st century international system and the multitude of current threats, U.S. interests will be better served by not establishing clear thresholds. Ambiguity is a powerful tool to shape our adversaries’ actions in all domains and allows us the maneuverability to respond where, when, and how we choose. Red-line advocates must understand that thresholds only constrain our actions and could undermine credibility and the power to effectively deter our adversaries.

### Link---AT: Plan Doesn’t Affect Retaliation

#### Retaliatory OCOs are offensive, not defense --- prefer military statements

Derek Klobucher 13, journalist for SAP, the world’s leading provider of business software, “U.S. Prepares Counterstrike Against Cyber-Attack,” 3/15, Forbes, http://www.forbes.com/sites/sap/2013/03/15/u-s-prepares-counterstrike-against-cyber-attack/

In a departure for Alexander, the general not only discussed U.S. defense against cyber-attacks, but its offensive capacity, The New York Times reported Tuesday. Cyber Command will have 13 teams of digital warriors would counter-cyber-strike any nation to launch a major attack on American networks.¶ “This team, this defend-the-nation team, is not a defensive team,” Alexander told the House Armed Services Committee. “This is an offensive team that the Defense Department would use to defend the nation if it were attacked in cyberspace.”

## T

### Overview

#### There's a clear brightline---restrictions require a floor and a ceiling---oversight is a floor but doesn't set a cap on the President's potential actions

USCA 77, UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT, 564 F.2d 292, 1977 U.S. App. LEXIS 10899,. 1978 Fire & Casualty Cases (CCH) P317

Continental argues that even if the Aetna and Continental policies provide coverage for the Cattuzzo accident, that coverage should [\*\*8] be limited to a total of $300,000 because Atlas agreed to procure "not less than" $300,000 coverage. The District Court properly found that the subcontract language does not support a restriction on the terms of Continental's policy because the subcontract only sets a floor, not a ceiling, for coverage.

### AT: We Meet

#### They don’t meet --- they don’t ban an area of flexibility since covert OCOs are still an option – their evidence is terrible – it’s in the context of the Arms Control Treaty, not war powers

Gaul 8, Matthew J. Gaul is a partner in Steptoe’s New York office.  A former insurance regulator and securities enforcement attorney for the state of New York, Mr. Gaul represents insurance companies and other financial institutions in government investigations and complex regulatory matters, <http://faculty.lls.edu/manheim/ns/gaul2.htm>

A. The Arms Export Control Act¶ The laws and regulations congress and the Department of State have created to deal with the independent military contracting industry are part of a larger regulatory scheme to regulate the export of American defense technology and services. The Arms Export Control Act76 under Title 22 of the United States Code is the key statute in this area. The statute authorizes the president "[i]n furtherance of world peace and the security and foreign policy of the United States," to control the import and export of arms and other defense articles and services.77 The president is given full authority to promulgate regulations for this purpose and to designate items as defense articles and defense services by placing them on the United States Munitions List.78 Any person or organization that manufactures, exports or imports the goods or services on the list must register with the United States government and receive a license.79 Criminal penalties can result from a failure to register properly. Congress has given the president broad power to determine not only registration and licensing procedures but also which goods and services fall under the regulations. ¶ A major inter-branch limitation on this executive regulatory power is a series of reporting and certification requirements. Basically, any license to export defense goods or services to a single nation or organization totaling more than $1 million must be reported to the Speaker of the House and the chair of the Senate Foreign Relations Committee on a quarterly basis.80 The report must include the items exported, the quantity of each item, the contract price, the name and address of the "ultimate user" of each item, and an estimate of the number of U.S. government employees in the territory to which the items will go.81 ¶ Furthermore, for any proposal to export defense articles or defense services worth $50 million or more, the president must provide the above information to the Speaker of the House and the chair of the Senate Foreign Relations Committee before the deal is completed or the license granted.82 The statute then specifies that congress has a 15 day83 or 30 day84 period in which to consider the proposed export. During the specified period congress may request additional information from the president including an estimate of the number of U.S. military personnel or contract personnel needed to carry out the proposed deal; an evaluation of whether and how the proposed export would contribute to an arms race, support international terrorism, increase the risk of an escalation or outbreak of armed conflict, prejudice the negotiation of arms controls, or adversely effect the arms control policy of the United States; the reasons why the proposed export is in the foreign policy interests of the United States; an analysis of the effect of the sale on the military capabilities of the buying country or organization; and an analysis of the how the proposed sale would effect the military balance of power in the given region.85 During the review period congress may then act to block the proposed export by joint resolution.86 If congress does not act within the given period the president may issue the license at his discretion. ¶ **\*\*CAL’S CARD STARTS\*\***¶The president may circumvent the specified waiting period by stating in his certification that a state of emergency exists which requires immediate approval of the exports.87 The emergency certification must also set forth "a detailed justification for his determination, including a description of the emergency circumstances which necessitate the immediate issuance of the export license and a discussion of the national security interests involved."88¶ The final check on presidential regulatory power in this area was added in 1996. The new provision requires the president to publish the above certifications in the federal register upon transmittal to the Speaker of the House and Chair of the Foreign Relations Committee.89 This public notification requirement only applies to major arms licenses for export deals totaling $50 million or more.¶ **\*\*CAL’S CARD ENDS\*\***

#### Contextual definitions bad – intent to define outweighs

Eric Kupferbreg 87, University of Kentucky, Senior Assistant Dean, Academic & Faculty Affairs at Northeastern University, College of Professional Studies Associate Director, Trust Initiative at Harvard School of Public Health 1987 “Limits - The Essence of Topicality” http://groups.wfu.edu/debate/MiscSites/DRGArticles/Kupferberg1987LatAmer.htm

Often, field contextual definitions are too broad or too narrow for debate purposes. Definitions derived from the agricultural sector necessarily incorporated financial and bureaucratic factors which are less relevant in considering a 'should' proposition. Often subject experts' definitions reflected administrative or political motives to expand or limit the relevant jurisdiction of certain actors. Moreover, field context is an insufficient criteria for choosing between competing definitions. A particularly broad field might have several subsets that invite restrictive and even exclusive definitions. (e.g., What is considered 'long-term' for the swine farmer might be significantly different than for the grain farmer.) Why would debaters accept definitions that are inappropriate for debate? If we admit that debate is a unique context, then additional considerations enter into our definitional analysis.

#### Authority is the exercise of power over others

OED 13 (http://www.oed.com/viewdictionaryentry/Entry/13349)

authority, n.

I. Power to enforce obedience.

a. Power or right to enforce obedience; moral or legal supremacy; the right to command, or give an ultimate decision.

b. in authority: in a position of power; in possession of power over others.

### Restrictions must be enforceable

#### Restrictions must be enforceable

Elizabeth Boalt 5, Professor of Law Emeritus, University of California, Berkeley, University of Arkansas at Little Rock School of Law The Journal of Appellate Practice and Process Fall, 20035 J. App. Prac. & Process 473, lexis

Four questions follow: (1) Are discouraging words "restrictions" on citation under Rule 32.1? (2) What difference, if any, does it make? (3) What is the risk of judicial resistance to [\*493] no-citation rules, through discouraging words or other means? and (4) Should discouraging words be forbidden?

1. Are Discouraging Words "Restrictions" under Rule 32.1?

The committee's statement notwithstanding, it is not clear that discouraging words have to be considered "restrictions" on citation under the proposed Rule 32.1. These words may be wholly admonitory - and unenforceable. The Fourth Circuit's rule, for example, states that citing unpublished opinions is "disfavored," but that it may be done "if counsel believes, nevertheless, that [an unpublished opinion] has precedential value in relation to a material issue in a case and that there is no published opinion that would serve as well." n129 On the question of what counsel "believes," surely counsel should be taken at her word; counsel's asserted belief that an unpublished opinion has precedential or persuasive value should not be considered a falsifiable fact. Hence no sanction should be available for violating the Fourth Circuit's rule, and the rule's discouraging language in turn would not be a "prohibition or restriction" that was barred by Rule 32.1 as presently drafted.

In the rules of some other circuits, however, the language disfavoring citation of unpublished opinions is unmoored from anyone's "belief" and arguably does impose an objective "prohibition or restriction" determinable by a court. n130 A court might find, for example, that the required "persuasive value with respect to a material issue that has not been addressed in a published opinion" n131 was not present, and hence that the citation was not permitted by the circuit rule.

With what result? It would follow, paradoxically, that the opinion could be cited - because the circuit rule would be struck down under Rule 32.1 as a forbidden "restriction" on citation.

The committee's double-negative drafting thus creates a Hall of Mirrors in which citation of an unpublished opinion [\*494] would be allowed either way. If the local rule's discouraging language is merely hortatory, it is not a "restriction" forbidden by Rule 32.1; but that doesn't matter, because such a rule does not bar the citation in the first place. If, on the other hand, the local rule's language has bite and is a "restriction," then Rule 32.1 strikes it down, and again the citation is permitted.

#### Their ev only defines "restrictions," not "restrictions on authority" - that kills predictability

J.A.D. Haneman 59, justice of the Superior Court of New Jersey, Appellate Division. “Russell S. Bertrand et al. v. Donald T. Jones et al.,” 58 NJ Super. 273; 156 A.2d 161; 1959 N.J. Super, Lexis

HN4 In ascertaining the meaning of the word "restrictions" as here employed, it must be considered in context with the entire clause in which it appears. It is to be noted that the exception concerns restrictions "which have been complied with." Plainly, this connotes a representation of compliance by the vendor with any restrictions upon the permitted uses of the subject property. The conclusion that "restrictions" refer solely to a limitation of the manner in which the vendor may [\*\*\*14] use his own lands is strengthened by the further provision found in said clause that the conveyance is "subject to the effect, [\*\*167] if any, of municipal zoning laws." Municipal zoning laws affect the use of property.¶ HN5 A familiar maxim to aid in the construction of contracts is noscitur a sociis. Simply stated, this means that a word is known from its associates. Words of general and specific import take color from each other when associated together, and thus the word of general significance is modified by its associates of restricted sense. 3 Corbin on Contracts, § 552, p. 110; cf. Ford Motor Co. v. New Jersey Department of Labor and Industry, 5 N.J. 494 (1950). The [\*284] word "restrictions," therefore, should be construed as being used in the same limited fashion as "zoning."

#### And, substantial requires an objective, absolute measurement--- there's no way to quantify the impact oversight has on War Powers which means that their interpretation has no coherent way to account for an entire word in the topic

Words & Phrases 64, 40 W&P 759

The words "outward, open, actual, risible, substantial, and exclusive," in connection with a change of possession, mean substantially the same thing. They mean not concealed; not bidden; exposed to view; free from concealment dissimulation, reserve, or disguise; in full existence; denoting that which not merely can be, but is opposed to potential, apparent, constructive, and imaginary; veritable; genuine; certain; absolute; real at present time, as a matter of fact, not merely nominal; opposed to form; actually existing; true; not including, admitting, or pertaining to any others; undivided; sole; opposed to inclusive. Bass v. Pease, 79 111. App. 308, 31R

#### They conflate management and restrictions

BEREC 12, Guidelines for quality of service in the scope of net neutrality, Body of European Regulators for Electronic Communications

The concept of “traffic management” is sometimes used as a synonym of “restrictions”, but in these guidelines BEREC seeks to avoid misunderstanding by using the term “restrictions” to refer to all limitations, including those which are contractually binding and/or technically implemented limitations.