# UGA FB – Quarters

## 1NC

### Off 1

#### Interpretation – OCO includes only cyberattacks – that excludes exploitation and active defense – key to precision

Lorber 13 (Eric, J.D. Candidate, University of Pennsylvania Law School, Ph.D Candidate, Duke University Department of Political Science, "COMMENT: Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?," 15 U. Pa. J. Const. L. 961, lexis)

Cyberattacks are "efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them ... [,] encompassing activities that range in target (military versus civilian, public versus private), consequences (minor versus major, direct versus indirect), and duration (temporary versus long-term)." n83 While this definition provides broad [\*977] guidance as to what may constitute a cyberattack, for the purposes of applying existing legal structures, the definition must be conceptualized in a way that usefully fits into those preexisting regimes. Because of the complexity and great number of potential means of cyberattack, this Comment groups such attacks based on employment, i.e., the way in which they are utilized and their intended purposes. Such an approach provides greater clarity as to which U.S. domestic legal regime will likely govern their employment. The following section proceeds by first discussing some of the technical details of cyberattacks and then moves into understanding how they have been - and likely will be - employed in future conflicts.¶ Before moving to a discussion of what cyberattacks are, it is important to note what they are not. They are not cyberexploitation, that is, "the use of actions and operations ... to obtain information that would otherwise be kept confidential ... . Cyberexploitations are usually clandestine and conducted with the smallest possible intervention that still allows extraction of the information sought." n84 The core difference between attack and exploitation is in the cyber operation's purpose; cyberattacks are meant to be destructive whereas cyberexploitation acquires information nondestructively. n85 While the term offensive cyber operations usually encompasses both attack and exploitative elements, here "OCO" refers only to attacks. n86

#### Vote neg -

#### Limits – explodes the number of Affs because they could read a ton of different defensive policies in order to solve.

#### Brightline – sets the clearest distinction – either they restrict an attack or they do not – key to neg preparation and predictability

### Off 2

#### Text: The executive branch of the United States should issue and enforce an executive order implementing, via the appropriate administrative agencies, restricting the war powers authority of the President of the United States in the area of offensive cyber operations

#### Executive orders concerning war powers are common, have the same effect as the plan, and withstand judicial scrutiny

Duncan 10 (John C. – Associate Professor of Law, College of Law, Florida A & M University; Ph.D., Stanford University; J.D., Yale Law School, “A CRITICAL CONSIDERATION OF EXECUTIVE ORDERS: GLIMMERINGS OF AUTOPOIESIS IN THE EXECUTIVE ROLE”, Vermont Law Review, 35 Vt. L. Rev. 333, lexis)

Executive orders make "legally binding pronouncements" in fields of authority generally conceded to the President. n92 A prominent example of this use is in the area of security classifications. n93 President Franklin Roosevelt issued an executive order to establish the system of security classification in use today. n94 Subsequent administrations followed the President's lead, issuing their own executive orders on the subject. n95 In 1994, Congress specifically required "presidential issuance of an executive order on classification," by way of an "amendment to the National Security Act of 1947 . . . ." n96 The other areas in which Congress concedes broad power to the President "include ongoing governance of civil servants, foreign service and consular activities, operation and discipline in the military, controls on government contracting, and, until recently, the management and control of public lands." n97 Although there are also statutes that address these areas, most basic policy comes from executive orders. n98 Executive orders commonly address matters "concerning military personnel" n99 and foreign policy. n100 "[D]uring periods of heightened national security activity," executive orders regularly authorize the transfer of responsibilities, personnel, or resources from selected parts of the government to the military or vice versa. n101 Many executive orders have also guided the management of public lands, such as orders creating, expanding, or decommissioning military installations, and creating reservations for sovereign Native American communities. n102 [\*347] Executive orders serve to implement both regulations and congressional regulatory programs. n103 Regulatory orders may target specific businesses and people, or may be designed for general applicability. n104 Many executive orders have constituted "delegations of authority originally conferred on the president by statute" and concerning specific agencies or executive-branch officers. n105 Congress may confer to the President, within the statutory language, broad delegatory authority to subordinate officials, while nevertheless expecting the President to "retain[] ultimate responsibility for the manner in which ." n106 "[I]t is common today for [the President] to cite this provision of law . . . as the authority to support an order." n107 Many presidents, especially after World War II, used executive orders-with or without congressional approval-to create new agencies, eliminate existing organizations, and reorganize others. n108 Orders in this category include President Kennedy's creation of the Peace Corps, n109 and President Nixon's establishment of the Cabinet Committee on Environmental Quality, the Council on Environmental Policy, and reorganization of the Office of the President. n110 At the core of this reorganization was the creation of the Office of Management and Budget. n111 President Clinton continued the practice of creating agencies, including the National Economic Council, with the issuance of his second executive order. n112 President Clinton also used an executive order "to cut one hundred thousand positions from the federal service" a decision which would have merited no congressional review, despite its impact. n113 President George W. Bush created the Office of Homeland Security as his key organizational reaction to the terrorist attacks of September 11, 2001, despite the fact that [\*348] Congress at the time appeared willing to enact whatever legislation he sought. n114 President Obama created several positions of Special Advisor to the President on specific issues of concern, for which there is often already a cabinet or agency position. n115 Other executive orders have served "to alter pay grades, address regulation of the behavior of civil servants, outline disciplinary actions for conduct on and off the job, and establish days off, as in the closing of federal offices." n116 Executive orders have often served "to exempt named individuals from mandatory retirement, to create individual exceptions to policies governing pay grades and classifications, and to provide for temporary reassignment of personnel in times of war or national emergency." n117 Orders can authorize "exceptions from normal operations" or announce temporary or permanent appointments. n118 Many orders have also addressed the management of public lands, although the affected lands are frequently parts of military reservations. n119 The fact that an executive order has the effect of a statute makes it a law of the land in the same manner as congressional legislation or a judicial decision. n120 In fact, an executive order that establishes the precise rules and regulations for governing the execution of a federal statute has the same effect as if those details had formed a part of the original act itself. n121 However, if there is no constitutional or congressional authorization, an executive order may have no legal effect. n122 Importantly, executive orders designed to carry a statute into effect are invalid if they are inconsistent [\*349] with the statute itself, for any other construction would permit the executive branch to overturn congressional legislation capriciously. n123 The application of this rule allows the President to create an order under the presumption that it is within the power of the executive branch to do so. Indeed, a contestant carries the burden of proving that an executive action exceeds the President's authority. n124 That is, as a practical matter, the burden of persuasion with respect to an executive order's invalidity is firmly upon anyone who tries to question it. n125 The President thus has great discretion in issuing regulations. n126 An executive order, with proper congressional authorization enjoys a strong presumption of validity, and the judiciary is likely to interpret it broadly. n127 If Congress appropriates funds for a President to carry out a directive, this constitutes congressional ratification thereof. n128 Alternatively, Congress may simply refer to a presidential directive in later legislation and thereby retroactively shield it from any future challenge. n1

### Off 3

#### 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.

### Off 4

#### Yellen will likely be confirmed this month despite increasing GOP opposition

NASDAQ 10/30/13 ("GOP Senators Threaten to Delay Yellen Nomination," http://www.nasdaq.com/article/gop-senators-threaten-to-delay-yellen-nomination-20131030-01719)

Ms. Yellen, Mr. Obama's pick to become the first chairwoman of the central bank, is expected to secure the support of nearly all Democrats, but a handful of opponents among Senate Republicans have surfaced recently. Sens. Graham and McCain threatened this week to put a "hold" on Ms. Yellen's nomination in an effort to pressure the White House to release more information about the Benghazi attacks on Sept. 11, 2012.¶ "That's the only way we get their attention," Mr. McCain said in an interview Wednesday evening. "It's the only way we get any response." Mr. Graham's office confirmed he would also hold up Ms. Yellen's nomination to press for more information about the Benghazi attacks.¶ The lawmakers are pushing the White House to make the attack's survivors available to Congress and to release the statements they gave to the Federal Bureau of Investigation within 48 hours of the attack, an aide said. Earlier this year, Mr. Graham had cited concerns over Benghazi in his efforts to delay confirmation of Defense Secretary Chuck Hagel.¶ Democrats have expressed confidence that Ms. Yellen, currently the vice chairwoman of the Fed's Board of Governors, will be confirmed. Only a handful of GOP lawmakers have said they plan to try to delay the Senate from voting on her nomination later this fall and none have aimed their criticism at Ms. Yellen herself. Mr. McCain noted Wednesday that he was pushing only to delay the nomination and said that didn't indicate he would ultimately oppose Ms. Yellen.¶ Last week, Sen. Rand Paul (R., Ky.) said he would put a hold on Ms. Yellen's nomination unless the Senate votes on his bill to increase congressional scrutiny of the central bank.¶ A hold is a procedural tactic that prevents the Senate from moving unanimously to approve a nominee, forcing a series of floor votes instead. However, Senate aides said they always expected to hold full roll-call votes for a high-profile position such as the chairwoman of the central bank. A hold can be overcome if at least 60 senators support Ms. Yellen in a procedural vote. Then, just a majority of the 100-member Senate would be needed to approve the nomination. There will be 55 senators in the chamber's Democratic caucus Thursday, when Democratic New Jersey Senator-elect Cory Booker is sworn in. The Republican caucus has 45.¶ Ms. Yellen is expected to begin meeting this week with lawmakers on the Senate Banking Committee, which is expected to hold her confirmation hearing in November.

#### Obama fights the plan – strongly supports war powers

Rana 11 (Aziz – Assistant Professor of Law, Cornell Law School, “TEN QUESTIONS: RESPONSES TO THE TEN QUESTIONS”, 2011, 37 Wm. Mitchell L. Rev. 5099, lexis)

Thus, for many legal critics of executive power, the election of Barack Obama as President appeared to herald a new approach to security concerns and even the possibility of a fundamental break from Bush-era policies. These hopes were immediately stoked by Obama's decision before taking office to close the Guantanamo Bay prison. n4 Over two years later, however, not only does Guantanamo remain open, but through a recent executive order Obama has formalized a system of indefinite detention for those held there and also has stated that new military commission trials will begin for Guantanamo detainees. n5 More important, in ways small and large, the new administration remains committed to core elements of the previous constitutional vision of national security. Just as their predecessors, Obama officials continue to defend expansive executive detention and war powers and to promote the centrality of state secrecy to national security.

#### Presidential war power battles expend capital – it’s immediate and forces a trade-off

O’Neil 7 (David – Adjunct Associate Professor of Law, Fordham Law School, “The Political Safeguards of Executive Privilege”, 2007, 60 Vand. L. Rev. 1079, lexis)

a. Conscious Pursuit of Institutional Prerogatives The first such assumption is belied both by first-hand accounts of information battles and by the conclusions of experts who study them. Participants in such battles report that short-term political calculations consistently trump the constitutional interests at stake. One veteran of the first Bush White House, for example, has explained that rational-choice theory predicts what he in fact experienced: The rewards for a consistent and forceful defense of the legal interests of the office of the presidency would be largely abstract, since they would consist primarily of fidelity to a certain theory of the Constitution... . The costs of pursuing a serious defense of the presidency, however, would tend to be immediate and tangible. These costs would include the expenditure of political capital that might have been used for more pressing purposes, [and] the unpleasantness of increased friction with congressional barons and their allies. n182 Louis Fisher, one of the leading defenders of the political branches' competence and authority to interpret the Constitution independently of the courts, n183 acknowledges that politics and "practical considerations" typically override the legal and constitutional principles implicated in information disputes. n184 In his view, although debate about congressional access and executive privilege "usually proceeds in terms of constitutional doctrine, it is the messy political realities of the moment that usually decide the issue." n185 Indeed, Professor Peter Shane, who has extensively studied such conflicts, concludes that their successful resolution in fact depends upon the parties focusing only on short-term political [\*1123] considerations. n186 When the participants "get institutional," Shane observes, non-judicial resolution "becomes vastly more difficult." n187

#### Capital key to securing the new Fed chair

Collier 9/30/13 (Sustainable Wealth Management, "Perspectives: Four Challenges Facing the Markets This Fall," http://webcache.googleusercontent.com/search?q=cache:mVzW9cxQi5YJ:www.collierswm.com/blog/perspectives-four-challenges-facing-markets-fall+&cd=15&hl=en&ct=clnk&gl=us)

Current Fed Chairman, Ben Bernanke, will step down from his position in January and his replacement will be named soon. Rumors about President Obama’s nomination are flying and we can expect a contentious confirmation process by the Senate, filled with horse-trading and negotiations. The new Fed chairman will have the responsibility of managing the tapering process and ending the Fed’s unprecedented quantitative easing programs while keeping the economy on track.[iii]

#### Yellen confirmation is key to the global economy – she’s key to managing multiple threats to growth

Crutsinger and Wiseman 10/9/13 (Martin and Paul, AP Economics Writers, "As Fed chair, Yellen would face tough challenges," http://www.dallasnews.com/business/headlines/20131009-as-fed-chair-yellen-would-face-tough-challenges.ece?nclick\_check=1)

Yellen would also take over the Fed at a critical time for China, the world's No. 2 economy after the United States, and other developing nations.¶ The International Monetary Fund, citing slower growth in China, India and Brazil, downgraded its forecast this week for global economic growth to 2.9 percent this year and 3.6 percent in 2014. Both are 0.2 percentage point weaker than the IMF's previous forecast in July.¶ Investors have been pulling money out of developing markets, partly to take advantage of rising interest rates in the United States. The Fed might be called upon to help calm worldwide financial volatility.¶ "The role of the Fed chair is so critical," said Greg McBride, senior financial analyst at Bankrate.com. "We're not just talking about the U.S. economy. We're talking about the global economy."¶ Yellen will also have to establish herself as chair at a time when the Fed is experiencing unusual turnover. When Bernanke leaves Jan. 31, but there could be up to four vacancies that Obama would need to fill on the seven-member Fed board.¶ One board member, Elizabeth Duke, left in August. Another, Sarah Bloom Raskin, has been nominated by Obama to become deputy Treasury secretary. The term of a third, Jerome Powell, will be up Jan. 31, though he can remain on the board until a successor is confirmed by the Senate.¶ And Sandra Pianalto, president of the Federal Reserve Bank of Cleveland, has announced that she will leave early next year.¶ Most analysts say they're confident Yellen can handle the many challenges.¶ "By temperament, by mannerism and by extensive experience, I think she is better prepared for that job than almost anybody on the face of the earth," says Alan Blinder, a Princeton University economist and former Fed vice chairman who served with Yellen at the Fed in the 1990s.

#### 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 Frontline – Deterrence

#### The plan is not a deterrent strategy – Kramer ev says we need to invest in new kinds of deterrent capabilities – that’s not the aff

#### No space war

Klein 12 – CDR John J. Klein, USN (BS, Georgia Institute of Technology; MS, Naval Postgraduate School; MA, Naval War College), is assistant air officer (“miniboss”) aboard the USS John C. Stennis (CVN 74). He has served as maintenance officer, Sea Control Squadron 24 (VS‑24); test and evaluation project officer, Naval Force Aircraft Test Squadron (VX-20); naval flight officer under instruction, US Naval Test Pilot School; tactical development and evaluation officer (VS-24); and maintenance branch officer, Sea Control Squadron 28 (VS‑28). Commander Klein is the author of several journal articles and the book Space Warfare: Strategy, Principles and Policy (London: Routledge, 2006). March 6th, 2012, Astropolitics: The International Journal of Space Politics & Policy, "The Influence of Technology on Space Strategy," [www.tandfonline.com/doi/pdf/10.1080/14777622.2012.651700](http://www.tandfonline.com/doi/pdf/10.1080/14777622.2012.651700)

Fourth, advanced space-based technology and weapons systems can have a stabilizing effect on the international community. As was the case with nuclear weapons during the Cold War, if a weapons system poses a large enough threat to two or more adversaries, its potential use can cause state leaders to avoid direct confrontation. This is not to suggest that future space-based weapons will eliminate tensions among competing states, nations, or groups, but **weapons can provide a stabilizing influence at times.**

#### No internal – Crossx proves they cant articulate the difference between escalatory cyber war and non-escalatory and who attacks

#### No risk of space weapons

Rosen 13 Armin Rosen, an Atlantic Media fellow, The Atlantic, January 16, 2013, "Give Peace a Chance—in Space", http://www.theatlantic.com/international/archive/2013/01/give-peace-a-chance-in-space/267223/

"The wars of the future will not be fought on the battlefield or at sea," a military academy commandant voiced by Willem Dafoe intones toward the end of a now-classic 1997 episode of The Simpsons. "They will be fought in space, or possibly on top of a very tall mountain." This was meant as a joke, but the latter half of that statement would soon prove eerily prescient when India and Pakistan battled over Kashmir's Siachen glacier -- a strategically irrelevant ice field sitting over 18,000 feet above sea level -- during the Kargil War in 1999. For now, the prospect of military conflict in outer space still resides in the realm of dystopia or absurdity, to the point that a White House petition demanding the construction of a Star Wars-style "Death Star" could be treated as a harmless prank. In rejecting the petition this week, the White House rightly wondered why a debt-strapped U.S. government would spend $850 quadrillion on a weapons system "with a fundamental flaw that can be exploited by a one-man starship." Thankfully, the prospect of an orbital space-to-earth battlestation doesn't even need to be treated seriously. But it wasn't always this way. In 1952, the eminent rocket scientist Werner Von Braun imagined that a future space station would function as an orbital nuclear platform. Space historians believe that Russia's Salyut 3 space station, which was launched in June of 1974, had a cannon on board, in case a craft or satellite from an enemy country attempted to disrupt its mission. The Soviet Union experimented with Fractional Orbital Bombardment Systems in the 1960s and 70s -- basically nuclear delivery systems that were capable of orbiting the earth. The U.S. even detonated a nuclear weapon over 200 miles above the Pacific Ocean in July of 1962, an incident known as Starfish Prime that, according to Harvard University astrophysicist Jonathan McDowell, halved the useful lifetime of all satellites then in orbit, knocked out power in Hawaii, created an artificial Van Allen Belt that persisted for five years, and released radiation into the atmosphere that wouldn't fully dissipate until the end of the decade. For a time, it was all but taken for granted that space would not only be militarized, but weaponized -- used as a venue or staging area for violent clashes between space-faring nations, or attacks on the surface of the earth. Space war wasn't a punch line, but a possibility that nuclear-armed powers didn't think they could afford to ignore. The results of the Starfish event hint at one reason why that changed. "This is a great weapon. It does a lot of damage -- but it also killed everything you had yourself," McDowell says of the results of the high-altitude nuclear test. War in space was sure to have a cataclysmic effect on the country with the most space assets, regardless of the end result. But what about war from space? For powerful space-faring countries, space-to-earth or earth-to-space combat is about as practical as it is desirable -- which is to say, not very. "Space is incredibly useful for the military for a lot of things," McDowell explains. "It's great for intelligence, communication and navigation. The natural thing is to ask, 'where are my X-Wing fighters?' The fact is that it's hard to find a rationale for them." Laura Grego, a senior scientist in the global security program at the Union of Concerned Scientists, explained why an orbital weapons platform -- the kind of big-ticket military asset that you might want a fleet of X-Wing-type vehicles to protect -- is impractical for attacking targets on earth. "Everything in space is moving at rapid speeds. At the same time, the earth is rotating underneath it....as it's going around, you can't hold [the weapon] above your target. You might be over one country for 15 minutes and then you're gone." This tiny orbital window is called the absentee ratio, and an ICBM, which can hit any target on earth within minutes, isn't constrained by one. McDowell added that in order to reach atmospheric velocity, a rocket needs to reach a breakneck seven kilometers-per-second, far faster than the four to five kilometers-per-second an ICBM must travel. From a purely strategic standpoint, orbiting a weapon for space-to-ground use is more expensive and far less useful than existing, more earth-bound capabilities. Simply orbiting a nuke, while possible, is good for little other than blackmail, or, at best, a Dr. Strangelove or Dead Hand-style insurance policy for a paranoid and heavily-armed space-faring state. The space nuke would be a means of ensuring that someone (or some thing) has the capability of effectively wiping out most or perhaps all of the 1,016 satellites that currently orbit the earth, while rendering their orbits so debris-strewn as to be totally and perhaps permanently useless. Such dangerous and cavalier behavior is the stuff of cinematic super-villainy -- not statecraft. But there's another, more idealistic reason humanity is safe from the scourge of space war. And ironically, it suggests that we might not be safe forever. The ban on Death Star-like orbital weaponry is one of the more robust norms in international law. A prohibition on stationing weapons of mass destruction in space, as well as the total demilitarization of the Moon, is enshrined in article 4 of the Outer Space Treaty of 1967, which 126 countries have signed. As University of Nebraska law professor and space law expert Frans von der Dunk notes, the treaty bans the stationing of weapons of mass destruction in space without banning their actual use in space. The stationing and use of kinetic or conventional weaponry is also allowed. Yet the most worrying aspect of the current legal regime is that the laws of war extend to the heavens as well. "The general international law on the law of force and the prohibition on the use of military force also applies in outer space," says von der Dunk. "If, as part of your self-defense you need your satellite to shoot down the satellite of your aggressor...that is perfectly allowed." Even so, the 1967 treaty demonstrates that in space, the peaceniks seem to be winning, at least for now. Joan Johnson-Freese of the Naval War College explained that there are two ways that, at the most schematic level, there are two ways the international legal regime could conceive of outer space: "On one end you put the view that space is a common heritage of mankind," she says. "The other end of the spectrum is that air, land and sea are all environments, and all those environments have been weaponized and therefore it's inevitable that space too will also become weaponized." The latter formulation raises a number of chilling possibilities: most people probably don't expect a war to break out in space, but the soldiers at Siachen probably didn't expect to be fighting atop an 18,000 mountain pass either. Humanity has proven willing to fight over literally anything, so long as the capability exists. Why should we assume space will be different? Space hasn't been weaponized, and the general anti-weaponization tilt of the 1967 treaty is part of the reason why. That tilt has gained the status of a respected legal norm, one arguably strengthened by the fact that the treaty itself was founded on a bedrock of mutual self-interest. "In the 1960s, the superpowers were able to agree that there was more of a benefit in keeping the other party from doing it than they saw a drawback in themselves being forced to abstain from it," von der Dunk says of the U.S. and Soviet Union's view towards stationing weapons of mass destruction in space. In other words, each side believed that preventing their opponent from weaponizing space was worth the potential strategic cost of foreclosing on their own ability to weaponize space. Even after the Cold War, the norm has endured.

#### No solvency – Kramer says we need to establish deterrent capability – also that failure to communicate *resolve* sparks the internal – that’s cross-x

#### 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.

#### No solvency – Healy and Wilson – it says congress has to check executive power – plan doesn’t specify binding consultation

#### No risk of cyber attack and even if it happens no impact

Douglas Birch 10-1, former foreign correspondent for the Associated Press and the Baltimore Sun who has written extensively on technology and public policy, 10/1/12, “Forget Revolution,” Foreign Policy, http://www.foreignpolicy.com/articles/2012/10/01/forget\_revolution?page=full

Government officials sometimes describe a kind of Hieronymus Bosch landscape when warning of the possibility of a cyber attack on the electric grid. Imagine, if you will, that the United States is blindsided by an epic hack that interrupts power for much of the Midwest and mid-Atlantic for more than a week, switching off the lights, traffic signals, computers, water pumps, and air conditioners in millions of homes, businesses, and government offices. Americans swelter in the dark. Chaos reigns! ¶ Here's another nightmare scenario: An electric grid that serves two-thirds of a billion people suddenly fails in a developing, nuclear-armed country with a rich history of ethnic and religious conflict. Rail transportation is shut down, cutting off travel to large swathes of the country, while many miners are trapped underground. ¶ Blackouts on this scale conjure images of civil unrest, overwhelmed police, crippled hospitals, darkened military bases, the gravely injured in the back of ambulances stuck in traffic jams. ¶ The specter of what Defense Secretary Leon Panetta has called a "digital Pearl Harbor" led to the creation of U.S. Cyber Command, which is tasked with developing both offensive and defensive cyber warfare capabilities, and prompted FBI Director Robert Mueller to warn in March that cyber attacks would soon be "the number one threat to our country." Similar concerns inspired both the Democrats and Republicans to sound the alarm about the cyber threat in their party platforms. ¶ But are cyber attacks really a clear and present danger to society's critical life support systems, capable of inflicting thousands of casualties? Or has fear of full-blown cybergeddon at the hands of America's enemies become just another feverish national obsession -- another of the long, dark shadows of the 9/11 attacks? ¶ Worries about a large-scale, devastating cyber attack on the United States date back several decades, but escalatedfollowing attacks on Estonian government and media websites during a diplomatic conflict with Russia in 2007. That digital ambush was followed by a cyber attack on Georgian websites a year later in the run-up to the brief shooting war between Tbilisi and Moscow, as well as allegations of a colossal, ongoing cyber espionage campaign against the United States by hackers linked to the Chinese army. ¶ Much of the concern has focused on potential attacks on the U.S. electrical grid. "If I were an attacker and I wanted to do strategic damage to the United States...I probably would sack electric power on the U.S. East Coast, maybe the West Coast, and attempt to cause a cascading effect," retired Admiral Mike McConnell said in a 2010 interview with CBS's 60 Minutes. ¶ But the scenarios sketched out above are not solely the realm of fantasy. This summer, the United States and India were hit by two massive electrical outages -- caused not by ninja cyber assault teams but by force majeure. And, for most people anyway, the results were less terrifying than imagined. ¶ First, the freak "derecho" storm that barreled across a heavily-populated swath of the eastern United States on the afternoon of June 29 knocked down trees that crushed cars, bashed holes in roofs, blocked roads, and sliced through power lines. ¶ According to an August report by the U.S. Department of Energy, 4.2 million homes and businesses lost power as a result of the storm, with the blackout stretching across 11 states and the District of Columbia. More than 1 million customers were still without power five days later, and in some areas power wasn't restored for 10 days. Reuters put the death tollat 23 people as of July 5, all killed by storms or heat stroke. ¶ The second incident occurred in late July, when 670 million people in northern India, or about 10 percent of the world's population, lost power in the largest blackout in history. The failure of this huge chunk of India's electric grid was attributed to higher-than-normal demand due to late monsoon rains, which led farmers to use more electricity in order to draw water from wells. Indian officials told the media there were no reports of deaths directly linked to the blackouts. ¶ But this cataclysmic event didn't cause widespread chaos in India -- indeed, for some, it didn't even interrupt their daily routine. "[M]any people in major cities barely noticed the disruption because localized blackouts are so common that many businesses, hospitals, offices and middle-class homes have backup diesel generators," the New York Timesreported. ¶ The most important thing about both events is what didn't happen. Planes didn't fall out of the sky. Governments didn't collapse. Thousands of people weren't killed. Despite disruption and delay, harried public officials, emergency workers, and beleaguered publics mostly muddled through. ¶ The summer's blackouts strongly suggest that a cyber weapon that took down an electric grid even for several days could turn out to be little more than a weapon of mass inconvenience.¶ That doesn't mean the United States can relax. James Lewis, director of the technology program at the Center for Strategic and International Studies, believes that hackers threaten the security of U.S. utilities and industries, and recently penned an op-ed for the New York Times calling the United States "defenseless" to a cyber-assault. But he told Foreign Policy the recent derecho showed that even a large-scale blackout would not necessarily have catastrophic consequences.

#### You’re not the deliberation of your solvency ev - griffin

#### 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.

#### 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.

### 1NC Frontline – China

#### If china modeled the plan the one party system in china would just approve the cyber attacks, so the impact is inevitable

#### Mutual mistrust means no modeling, but any conflict won’t escalate

Inociendo, 13 (Ramy – CNN, with Jaime Florcruz, 7/11. “Will we really see the dawn of a "new chapter" in U.S.-China relations?” http://www.cnn.com/2013/07/11/business/us-china-relations-new-chapter/)

In addition to IP theft, U.S.-China cyber security issues have come to the fore in the past month after NSA leak Edward Snowden alleged U.S. intelligence agents have been hacking hundreds of Chinese computers since at least 2009. China claimed Snowden's revelations would "test developing Sino-US ties" and exacerbate an already "soured relationship" on cybersecurity. Snowden's assertions, on top of alleged Chinese hacking of U.S. firms, depict a clear degree of mutual mistrust. The majority of headlines in China since then have referenced "strain," "tension," and even "anger" between the U.S. and China. The potential and ease for cyber attacks between the U.S. and China will continue to grow, says Andy Mok, managing director of Beijing-based Red Pagoda and former technology researcher for RAND Corporation. "When every physical object has an IP address ... the return on malicious behavior becomes much higher. So on both sides -- China and the U.S. -- the targets are increasingly attractive." National electrical grids and transportation networks are some of the most attractive marks in each country, adds Mok. "That said, the sky is not falling and I don't believe we are weeks or months away from a cyberwar with China that will leave the U.S. power grid in tatters and the whole country sitting in the dark for months or years." The chances of direct conflict are low, agree analysts. Economic, military, and technological disparity between the U.S. and China is too great. China is not ready for a clash to occur. And the U.S. -- still on the mend from the 2008 financial crisis -- is unlikely to instigate a conflict with China because of its own fiscal binds to China.

#### NO solvency – 1AC dycus ev – it assumes congress lays down guidelines and then the prez follows them – that’s not the aff

#### Can’t solve norms

**Lewis 11, Senior Fellow at CSIS** (James Andrew, Confidence-building and international agreement in cybersecurity, citizenlab.org/cybernorms2012/Lewis2011.pdf)

Obstacles to reaching a multilateral agreement

The immense utility of cyber action will shape any international agreement on cybersecurity. ¶ States will not give up this new tool for state power. Cyber attack is cheap and offers strategic ¶ advantage. First, the importance of information superiority in warfare and the ability to gain ¶ real military advantage from the use of information assets makes digital infrastructures too ¶ valuable a target to be declared off limits or for cyber attacks to be renounced. The necessary ¶ technologies are either commercial or easily derived from widely available commercial ¶ products—a laptop computer, an internet connection and a few computer programs. We ¶ cannot control the “precursors” for assembling these “weapons”. They are cheap, small, ¶ portable, easy to conceal and, for sophisticated programmers in or out of government, easy ¶ to construct. Special purpose tools for cyber attack are widely available on thriving cybercrime ¶ black markets. It is unlikely that any state will renounce the use of cyber attacks. ¶ Nor would a treaty that excludes certain targets from cyber attack make sense. Existing laws ¶ of war already define safeguards and limitations on (but do not ban) attacks on civilian targets. ¶ We cannot expect more for cyberspace. An alternate approach could be based on nonproliferation, where states developed multilateral norms that define responsible behaviour. ¶ The simplest norm would extend existing law and practice to say that a state is responsible for ¶ the behaviour of those on its territory—this would constrain the use of proxies and “patriotic” ¶ hackers.¶ Second, action in cyberspace has been an immense boon to espionage. The close linkage ¶ to espionage makes states reluctant to discuss or even admit they possess cyber capabilities, ¶ and this linkage also makes it unlikely that they will agree to “ban” first use. A “no first use” ¶ commitment could require states to renounce cyber espionage—something they are unlikely ¶ to do. Since the techniques of attack and espionage are similar, asking for a commitment ¶ not to develop or use cyber tools for penetration of opponent networks is really asking for a ¶ commitment not to spy. A “no first use” commitment could even be destabilizing if a victim ¶ were to misinterpret an instance of cyber espionage as an attack. four l 2011¶ 58¶ Confronting cyberconflict¶ The perceived difficulty of attribution of an attack may encourage some states to believe that ¶ they can successfully engage in covert cyber action while evading responsibility. A covert ¶ attack where the identity of the attacker is unknown has much less political risk. In addition, ¶ mercenaries (usually cybercriminals recruited by a state) can launch sophisticated attacks, ¶ providing an additional degree of deniability. The difficulty of attribution is often overstated, ¶ as it is increasingly possible in many cyber incidents to determine who is responsible using ¶ forensic techniques or active intelligence measures, but the perceived attribution problem ¶ increases the temptation to use cyber attack.¶ These problems mean that approaches that seek to limit cyber attack through multilateral ¶ agreement on technological constraints face intrinsic and potentially insurmountable ¶ difficulties. Cyber attack is a behaviour rather than a technology. Cyberconflict is shaped ¶ by covertness, ease of acquisition and uncertainty, and a legally binding convention that ¶ depends upon renouncing use, restricting technology, or upon verification of compliance is ¶ an unworkable approach for reducing the risk to international security from cyber attacks. An ¶ effort to secure an overarching cybersecurity agreement or treaty that attempted to address ¶ the full range of cybersecurity issues would be impractical. ¶ An incremental approach¶ Agreements to reduce the possibility of misinterpretation, escalation or unintended ¶ consequences in cyberconflict are a legitimate subject for international agreement and would ¶ improve international security. Just as states feel a degree of constraint from norms and ¶ agreements on non-proliferation, establishing explicit international norms for behaviour in ¶ cyberspace would affect political decisions on the potential risks and costs of cyber attack. The ¶ effect of globalization—the deep economic interconnection among states—has if anything ¶ increased the need for cooperation among states. ¶ The creation of norms for responsible state behaviour in cyberspace, the expansion of ¶ common understandings on the application of international law to cyberconflict, and the ¶ development of assurances on the use of cyber attacks would increase stability and reduce ¶ the risks of miscalculation or escalation. The single most important norm for multilateral ¶ agreement might be a norm that establishes state responsibility for the actions of its private ¶ citizens—such a norm could make it more difficult for states to tacitly encourage proxies by ¶ ignoring them or denying involvement with their actions. ¶ However, even simple norms face serious opposition. Conflicting political agendas, covert ¶ military actions, espionage and competition for global influence form the context for ¶ international discussion of cybersecurity. While there is little or no support for the idea of a ¶ treaty, and while international efforts now focus on a norms-based approach, the level of ¶ distrust among powerful states is too high for easy agreement on norms. 59¶ Confidence-building and international agreement in cybersecurity¶ Disparate values and deep distrust shape the environment for negotiation. Fundamental ¶ differences over values, despite formal acceptance of universal human rights, means that ¶ the initial set of norms likely to be acceptable to many states is limited. Ultimately, increased ¶ stability and security in cyberspace will require common understandings among states on ¶ their national responsibilities, on how the laws of war apply, where restraint in the use of the ¶ new military capability is possible, and where red lines or thresholds for escalation might exist. ¶ But there is too much distrust among competitors to move immediately towards global norms ¶ for cybersecurity.

#### No internal link – Sanger says china has refused to stop cyber espionage because of US policy – plan doesn’t stop US cyber espionage and it’s not reverse causal

#### 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

#### No Taiwan war

**Saunders and Kastner 2009** – \*Senior Research Fellow at the Institute for National Strategic Studies at the National Defense University, \*Assistant Professor in the Department of Government and Politics at the University of Maryland and former China Security Fellow at the Institute for National Strategic Studies (Phillip and Scott, International Security, 33.4, “Bridge over troubled water? Envisioning a China-Taiwan peace agreement”, http://www.mitpressjournals.org/doi/pdf/10.1162/isec.2009.33.4.87, WEA)

Most observers agree that the issue of Taiwan’s status is not ripe for resolution. China remains committed to the ultimate goal of unification and refuses to renounce the use of force to prevent Taiwan independence. Former President Jiang Zemin emphasized the goal of unification, and China’s policies sometimes implied a timetable for achievement of that objective.2 China’s policy toward the Taiwan issue, however, has undergone a significant shift under President Hu Jintao, who has emphasized the short-to-medium-term goal of deterring Taiwan independence, postponing unification into the indefinite future.3

On Taiwan, public opinion polls consistently show strong (more than 75 percent) public support for maintaining the status quo. Only a small percentage favors either immediate independence or immediate unification with China.4 Although this polling reflects conditional preferences that factor in the likelihood of China using force if Taiwan were to declare independence,5 it accurately reflects the widespread view on Taiwan that permanent resolution of the issue of Taiwan’s status is not presently possible. While the Democratic Progressive Party (DPP) has sought to mobilize voters by highlighting Taiwan’s separate identity and sought ways to emphasize Taiwan’s sovereignty during President Chen Shui-bian’s term in office, the KMT has adjusted the emphasis in its cross-strait policy to more closely match the views of mainstream Taiwan voters. In the 2008 presidential campaign, KMT candidate (and eventual victor) Ma Ying-jeou articulated “three nos” that would govern policy toward China in his administration. These were a pledge that there would be no pursuit of de jure independence, no negotiations with the mainland about unification, and no use of force.6 President Ma reiterated these points in his May 20, 2008, inaugural address.

Collectively, these positions suggest that China and Taiwan may be prepared to defer the issue of Taiwan’s status for resolution at some point in the future. **Both sides have expressed the desire to improve relations, expand cross-strait contacts, and negotiate a peace agreement** between Taipei and Beijing. These goals were articulated in the joint press communiqué issued following KMT Chairman Lien Chan’s April 2005 meeting with Chinese President Hu Jintao.7 Hu Jintao reiterated China’s willingness to negotiate a peace agreement with Taiwan in his statements at the October 2007 17th Party Congress: “On the basis of the one-China principle, let us discuss a formal end to the state of hostility between the two sides, reach a peace agreement, construct a framework for peaceful development of cross-straits relations, and thus usher in a new phase of peaceful development.”8 Both candidates in Taiwan’s 2008 presidential election called for negotiation of a peace agreement with Beijing, and President Ma repeated the call in his inaugural address.9 Upon assuming office, Ma moved quickly to restart dialogue between Taiwan’s Straits Exchange Foundation (SEF) and the PRC’s Association for Relations Across the Taiwan Straits (ARATS), the semiofficial bodies that previously served as vehicles for cross-strait dialogue.10

#### 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.**

#### Economic ties lead to MAD with China.

Shor 12 (Francis, Professor of History – Wayne State, “Declining US Hegemony and Rising Chinese Power: A Formula for Conflict?”, Perspectives on Global Development and Technology, 11(1), pp. 157-167)

While the United States no longer dominates the global economy as it did during the first two decades after WWII, it still is the leading economic power in the world. However, over the last few decades China, with all its internal contradictions, has made enormous leaps until it now occupies the number two spot. In fact, the IMF recently projected that the Chinese economy would become the world's largest in 2016. In manufacturing China has displaced the US in so many areas, including becoming the number one producer of steel and exporter of four-fifths of all of the textile products in the world and two-thirds of the world's copy machines, DVD players, and microwaves ovens. Yet, a significant portion of this manufacturing is still owned by foreign companies, including U.S. firms like General Motors. [5] On the other hand, China is also the largest holder of U.S. foreign reserves, e.g. treasury bonds. This may be one of the reasons mitigating full-blown conflict with the U.S. now, since China has such a large stake in the U.S. economy, both as a holder of bonds and as the leading exporter of goods to the U.S. Nonetheless, "the U.S. has blocked several large scale Chinese investments and buyouts of oil companies, technology firms, and other enterprises." [6] In effect, there are still clear nation-centric responses to China's rising economic power, especially as an expression of the U.S. governing elite's ideological commitment to national security.

#### China won’t model – too much mistrust over cybersecurity issues

IGCC, 12 – University of California Institute on Global Conflict and Cooperation (April, “China and Cybersecurity: Political, Economic, and Strategic Dimensions.” http://igcc.ucsd.edu/assets/001/503568.pdf)

Cybersecurity and Mistrust in U.S.–China Relations

In recent years the security of global information systems has become a contentious issue in U.S.–China relations. U.S. government sources allege that Chinese intrusions targeting proprie- tary economic data and sensitive national security information are on the rise. At the same time, a large proportion of malicious activity globally originates from computer hosts located in the United States. Both the U.S. Department of Defense and the Chinese People’s Liberation Army (PLA) view cyberspace as a new domain of conflict, and they eye each other warily. Nationalist “hacktivism,” in the form of website defacements, service denials, and network exploitation, flows both ways across the Pacific. This unfortunate situation exacerbates mistrust and raises suspicions in both countries regarding the others’ motives and activities. Cybersecurity as a Political Economy Problem There has been growing appreciation in the United States that cybersecurity, while superficially a technical issue, is actually a profoundly economic and political problem. The private sector ac- tors who generate risks often lack incentives to mitigate them, and the public sector has been unable to coordinate policy responses across government agencies with differing priorities. However, Western audiences have had little exposure to empirical research on the corresponding domestic policies, governing organizations, and economic tradeoffs in China. Failure to appreci- ate China’s domestic economy and politics can lead to a profound misunderstanding of its inter- national activities. It is especially important to understand the domestic civilian context of cyber- security given that the majority of day-to-day insecurity in cyberspace is economically motivated and risks of all types involve civilian information technologies.

#### China won’t model – sees itself as structurally disadvantaged so they have no incentive to adopt a defensive posture even if the US does

Segal, 12 – the Ira A. Lipman Senior Fellow for Counterterrorism and National Security Studies at the Council on Foreign Relations (Adam, 4/7. “Understanding China’s Cyber Policy.” http://thediplomat.com/china-power/understanding-chinas-cyber-policy/)

Linking cyber and technology policy is a form of techno nationalism that’s widely and deeply held by Chinese policymakers. The objectives are clear: China doesn’t want to depend on other countries for critical technologies, the United States and Japan in particular. The 2006 Medium to Long Term Plan on Science and Technology (MLP) puts it plainly: “Facts have proved that, in areas critical to the national economy and security, core technologies cannot be purchased.” The Chinese tend to see the current system as, if not unfair, then stacked against them, and so commentaries often focus on competitors’ unfair advantages (U.S. firms dominate hardware and software sectors, 10 of the 13 root servers in U.S.) and China’s victimization (China is the biggest victim of cybercrime). With both cyber and technology, outside observers have a tendency to overstate how driven by the center China really is. Yes, the MLP sets the goal of China becoming an “innovative nation” by 2020 and a “global scientific power” by 2050. Not surprising given Chinese history and national security concerns. But the document is of two minds about how to move up the value chain, including both a top-down, big-science and technology policy, as well as a bottom-up, entrepreneurial innovation strategy. In cyber, we tend to see China pursuing a coherent cyber strategy that involves pushing an Information Security Code of Conduct at the United Nations, the use of patriotic hackers, information war, and tight Internet control. Chinese analysts see the opposite, complaining that the U.S. – with the standing up of Cyber Command and promotion of the Internet Freedom agenda – has put China on the defensive and that Beijing is falling behind in cyberspace. There’s also a question of how strategically China can implement. The world of technology policy is one of sectoral and regional differentiation, with industries and provinces interpreting national regulations to serve their own interests. Ministries, universities, and government research institutes behave similarly, and Chinese firms often identify more with their Western competitors than with their local bureaucratic partners. It’s hard to imagine that the Ministry of Public Security, Ministry of State Security, PLA, and Ministry of Industry and Information Technology play any nicer together in the sand box of cyber policy. The prolific rate of cyber espionage – what Cyber Command head General Alexander called “the greatest transfer of wealth in history” – raises questions of China’s absorptive capacity. With technology imports, Chinese firms historically spent much less than Japanese and Korean companies did for diffusion and absorption. What is China doing with all of the IPR it’s allegedly stealing, and shouldn’t we start to see it paying off in more competitive Chinese firms? Not much public evidence exists that it’s helping Chinese companies move up the value chain (most evidence in the public domain is old-fashioned theft, see DuPont, Motorola, and American Semiconductor). Finally, technology policy may tell us something about what might work for cyber, although progress, especially in protecting intellectual property rights, has been glacially slow and uneven. The issue must be raised at the highest level, including by the President and Vice President, something that it’s not clear has happened yet. Multilateral pressure should also be applied. China backed down from the compulsory introduction of WAPI, an alternative to WiFi, after the U.S. government, supported by Japan and the EU, threatened to take a case to the WTO. Given the current state of the U.S.-China relationship in cyber, glacially slow and uneven might be an improvement.

## DA

### 2NC AT: Umbrella

#### Power over OCOs provides the president with flexibility in war powers – Congressional checks fail

Lorber 13 (Eric, JD Candidate, University of Pennsylvania Law School, PhD Candidate, Duke University Department of Political Science, "Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legilsation Successfully Constrain Presidential Power?", January, University of Pennsylvania Journal of Constitutional Law, 15, 961, Lexis)

Based on analysis of the War Powers Resolution, the lack of oversight for OCOs does not radically shift the balance between the legislative and executive branches' war-making authority. Most notably, because the War Powers Resolution itself has proven ineffective in providing Congress with a powerful tool to govern presidential use of force, bringing OCOs under the War Powers Resolution's statutory umbrella likely would not provide the possibility of such oversight. However, insofar as the President has increasingly turned to covert action since the passage of the War Powers Resolution to avoid its reporting requirements, [n233](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.909948.2817417112&target=results_DocumentContent&returnToKey=20_T18162626997&parent=docview&rand=1379362776915&reloadEntirePage=true" \l "n233) offensive cyber operations [\*1001] provide the President another means by which to continue this trend. OCOs therefore may give the President substantially more flexibility than he already has under the War Powers Resolution by adding what will become an increasingly frequent tool of warfare to his option-set.¶ The lack of congressional oversight of offensive cyber operations under the Intelligence Authorization Act also likely does not seriously shift the balance between congressional and executive war-making powers. The reason is inherent in the limitations of the legislation itself: the Intelligence Authorization Act specifies reporting requirements, but does not require the non-use or withdrawal of forces. [n234](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.909948.2817417112&target=results_DocumentContent&returnToKey=20_T18162626997&parent=docview&rand=1379362776915&reloadEntirePage=true" \l "n234) Further, these reports must be made in a "timely" fashion (the definition of which is undefined) and only to a small number of Congressmen (at most eight). [n235](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.909948.2817417112&target=results_DocumentContent&returnToKey=20_T18162626997&parent=docview&rand=1379362776915&reloadEntirePage=true" \l "n235) Thus even if the President had to report offensive cyber operations to Congress, it is unclear he would have to do so in a way that gave Congress an effective check, as these reports would be made only to a small group of Congressmen (who would not be able to share the information, because of its classified nature, with other members of the legislature) and could be done well after the employment of these capabilities. The resulting picture is one of increased presidential flexibility**;** the War Powers Resolution and the Intelligence Authorization Act - while arguably ineffective in many circumstances - provide increased congressional oversight of presidential war-making actions such as troop deployments and covert actions. Yet these statutes do not cover offensive cyber operations, giving the President an increasingly powerful foreign policy tool outside congressional reach.¶ Should these statutes be adjusted (or new ones created) that give Congress additional oversight in this area? Two competing desiderata suggest that oversight should be increased, but only to a limited extent. On the one hand, policymakers have suggested that developing strict rules and limitations on the use of offensive cyber operations will handicap the military's ability to quickly and effectively employ these tools in critical situations, such as cyber warfare against adversarial states. [n236](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.909948.2817417112&target=results_DocumentContent&returnToKey=20_T18162626997&parent=docview&rand=1379362776915&reloadEntirePage=true" \l "n236) According to these arguments, developing red lines that proscribe the use of these capabilities will create reluctance and trepidation among strategists and will lead to disadvantages in combat situations. [n237](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-20.909948.2817417112&target=results_DocumentContent&returnToKey=20_T18162626997&parent=docview&rand=1379362776915&reloadEntirePage=true" \l "n237) On the other hand, developing some legal rules is necessary to ensure that, as these cyber [\*1002] capabilities continue to develop, the President does not gain sufficient leverage to substantially tilt the balance between the President and Congress. Moreover, because these capabilities are still developing at a fast rate, understanding how they should and should not be employed is an important goal and having senior members of Congress and their staffs - professional staff members on the intelligence committees, who likely have substantial experience in these areas - provide input would be useful in developing this understanding.

### 2NC AT: Single Issues

#### Issues can’t be taken in isolation – each one invites other countries to take advantage of us

Talent 13

[Jim, National Review, Edward Snowden and the Consequences of Leading From Behind, 6/25/13, <http://www.nationalreview.com/corner/352010/edward-snowden-and-consequences-leading-behind-jim-talent>]

And why shouldn’t they stick their fingers in our eye? Over the last few years, the United States has repudiated the strategic principles which have underpinned its foreign policy since World War II. The Obama Administration has moved America away from the forefront of world events, preferring to “lead from behind” – which of course means not leading at all. It has neglected traditional alliances with Britain, Israel, and Eastern Europe and failed to build new ones. It has eschewed the tools of soft power, pointedly failing to recognize, much less support (even rhetorically) those fighting for human rights in places like Russia, China, or Iran. Worst of all, the government is systematically dismantling America’s hard power. Over the last four years, American defense budgets have been cut by almost 1.5 trillion dollars — far more than any other part of the budget. The last round of cuts embodied in the sequester are eating into readiness. The force is “hollowing,” sacrificing the training and maintenance that are essential for the military to operate on a day-to-day basis. Training has been curtailed for 80% of the Army; one third of America’s fighters and bombers have stood down; and two thirds of the Navy will, by year’s end, not be ready for combat. The hollowing out of America’s military is the worst thing that could happen for our national security. America’s power is what gives efficacy to the rest of our foreign policy. Without it, nothing that we do is likely to work. Our rights will be disregarded; our warnings will be ignored; our initiatives for peace will be taken as signs of weakness; our allies will distance themselves from us, and our enemies will increase their provocations. The insult America has suffered in the Snowden matter is by itself a small thing. But it cannot be taken in isolation. America is a wealthy nation with traditions that not only recognize but enshrine the principle of human dignity. For those reasons, the United States will always be a target fo

r governments and movements that covet what we have and fear what we believe. In the context of other recent events — the threats from North Korea, the aggressiveness of the Chinese in the South and East China Seas, the intervention by the Russians in Syria – the Snowden case is **another sign that the power of the United States is no longer taken seriously**. As long as that is the case, the provocations will continue, until they escalate into confrontations which cannot be ignored and which America does not have the power to control.

### 2NC Link

#### 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.

#### 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.

#### Congress moderating the president causes a power imbalance

Yoo 08

[John, Law Professor at University of California, Berkeley and Visiting Scholar at the American Enterprise Institute Deputy Assistant U.S. Attorney General in the Office of Legal Counsel, Department of Justice (OLC), during the George W. Bush administration, Deputy Assistant U.S. Attorney General in the Office of Legal Counsel, Department of Justice (OLC), during the George W. Bush administration, On Presidential Power, 2008, <http://www.writersreps.com/feature.aspx?FeatureID=152>]

The idea behind the “executive power,” which traces its origins from Alexander Hamilton and the first Washington administration, to thinkers such as Machiavelli, Locke, Montesquieu, and Blackstone, requires the perspectives of many disciplines: law, history, and political science. In the 20th century, the idea of presidential power has taken full advantage of the broad language of the Constitution and expanded to include management of the agencies and other powers inherently “executive” in nature—in contrast with the Constitution’s grant of specified, or "enumerated," powers to Congress. Presidential power also grew through the development of the President as party leader. Lastly, it grew in response to pressing challenges to the nation through its history. **Claims of an out-of-control executive have been much bandied about lately**. Most are overblown, aimed at a campaign season and audience. The Bush administration went to Congress twice for authorization for foreign combat. Congress has always has full power to cut off or roll back any military operations it chooses—however, it often does not so choose, and this fact makes no headlines. The political effort to curb the President's power over judicial appointments today has been heated: filibusters withholding Senate approval, for example, have proliferated to the point of judicial system paralysis. Judicial nominees are kept in limbo or subjected to smear campaigns, and this, at least theoretically, encourages a talent deficit in the judiciary. The national interest requires executive and legislative branches to cooperate politically. Congress can be eager to micromanage the executive branch, but whenever it addresses difficult subjects on which there is no consensus, it tends to pass ambiguous laws—sometimes bad law, incorporating contradictory goals—in its effort to placate warring interest groups and to seem to be doing good. I believe there is a current power imbalance that checks presidential action in matters of national security that were misguidedly enacted during the nation's over-reaction to Watergate and Vietnam and which have, ever since, hindered the executive branch's ability to do its job effectively—including to address dangers from terrorist networks about which many workers in government knew, as these individuals have since disclosed in scores of books. Many sensed the need to prevent the nation from attacks such as that which occurred on 9/11, but were paralyzed into inaction due to legal concerns that were sometimes overdrawn.

### 2NC AT: Heg Defense

#### Most probable – history and statistics prove

**Barnett 11** – Thomas P.M. Barnett is Former Senior Strategic Researcher and Professor in the Warfare Analysis & Research Department, Center for Naval Warfare Studies, U.S. Naval War College American military geostrategist and Chief Analyst at Wikistrat., worked as the Assistant for Strategic Futures in the Office of Force Transformation in the Department of Defense, March 7th, 2011, “The New Rules: Leadership Fatigue Puts U.S., and Globalization, at Crossroads,” http://www.worldpoliticsreview.com/articles/8099/the-new-rules-leadership-fatigue-puts-u-s-and-globalization-at-crossroads

It is worth first examining the larger picture: We live in a time of arguably the greatest structural change in the global order yet endured, with this historical moment's most amazing feature being its relative and absolute lack of mass violence. That is something to consider when Americans contemplate military intervention in Libya, because if we do take the step to prevent larger-scale killing by engaging in some killing of our own, we will not be adding to some fantastically imagined global death count stemming from the ongoing "megalomania" and "evil" of American "empire." We'll be engaging in the same sort of system-administering activity that has marked our stunningly successful stewardship of global order since World War II. Let me be more blunt: As the guardian of globalization, the U.S. military has been the greatest force for peace the world has ever known. Had America been removed from the global dynamics that governed the 20th century, the mass murder never would have ended. Indeed, it's entirely conceivable there would now be no identifiable human civilization left, once nuclear weapons entered the killing equation. But the world did not keep sliding down that path of perpetual war. Instead, America stepped up and changed everything by ushering in our now-perpetual great-power peace. We introduced the international liberal trade order known as globalization and played loyal Leviathan over its spread. What resulted was the collapse of empires, an explosion of democracy, the persistent spread of human rights, the liberation of women, the doubling of life expectancy, a roughly 10-fold increase in adjusted global GDP and a profound and persistent reduction in battle deaths from state-based conflicts. That is what American "hubris" actually delivered. Please remember that the next time some TV pundit sells you the image of "unbridled" American military power as the cause of global disorder instead of its cure. With self-deprecation bordering on self-loathing, we now imagine a post-American world that is anything but. Just watch who scatters and who steps up as the Facebook revolutions erupt across the Arab world. While we might imagine ourselves the status quo power, we remain the world's most vigorously revisionist force. ¶ As for the sheer "evil" that is our military-industrial complex, again, let's examine what the world looked like before that establishment reared its ugly head. The last great period of global structural change was the first half of the 20th century, a period that saw a death toll of about 100 million across two world wars. That comes to an average of 2 million deaths a year in a world of approximately 2 billion souls. Today, with far more comprehensive worldwide reporting, researchers report an average of less than 100,000 battle deaths annually in a world fast approaching 7 billion people. Though admittedly crude, these calculations suggest a 90 percent absolute drop and a 99 percent relative drop in deaths due to war. We are clearly headed for a world order characterized by multipolarity, something the American-birthed system was designed to both encourage and accommodate. But given how things turned out the last time we collectively faced such a fluid structure, we would do well to keep U.S. power, in all of its forms, deeply embedded in the geometry to come.

## China

### 2NC Solvency

#### VornDick evidence = Chinese leaders don’t know what is going on with the strategy

One crucial point lost amid the backdrop of the new digitized battlefield is the lack of Chinese leadership experience both military and political in utilizing key principles of the laws of armed conflict

#### Austin and Grady advocate a direct policy engagement with China

Austin & Gady 12 (Greg Austin – phD in International Relations, Vice President for the Worldwide Security Initiative, including a leadership role in the institute's work on cybersecurity, is now a Professorial Fellow. Greg has a 30-year career in international affairs, including senior posts in academia and government., Franz Stefan Gady -- M.A. in Strategic Studies/International Economics from the School of Advanced International Studies, Johns Hopkins University., “CYBER DETENTE BETWEEN THE U.S. AND CHINA: Shaping the Agenda, http://www.ewi.info/system/files/detente.pdf)

There are three proposals that the authors feel warrant immediate attention and may produce benefits in a reasonable time frame. First, the United States and China should agree on a joint public study on the interdependence of their respective critical information infrastructures in terms of likely economic effects of criminal attacks with strategic impacts. This could be done under the framework of the United States- China Strategic and Economic Dialogue. This may not be welcome by some private operators. Yet the need for such a study exists on a political level. It is a consequence of the strategic impact of private ownership of critical infrastructure. As much as such a study might intrude on narrowly defined private sector interests, leading ICT businesses need a deeper understanding of the military implications of the intermingled, even tangled, character of U.S. and Chinese operations in cyberspace. Second, the United States should work to include China in the existing infrastructure of the 24/7 Network of Contacts for High-Tech Crime of the G8. This might be accompanied by an effort to set up bilateral cooperation between the two countries on emergency response that go beyond the current capacity of the Comput

**MARKED**

er Emergency Response Teams (CERT) of the two countries. Third, cyber espionage, especially against intellectual property and critical infrastructure, is now too big a problem to ignore or to dismiss as a necessary evil. The U.S. and China need to take stock of the negative impacts and establish some limits. Both countries need some common understanding of the limits of cyber espionage.

#### Dycus says we need a more specific legislative approach

Dycus 10 your 1ac author (Professor Stephen Dycus is an internationally recognized authority on national security law and environmental law. The courses he has taught at Vermont Law School include Public International Law, National Security Law, Estates, Property, and Water Law. He was founding chair of the National Security Law Section of the Association of American Law Schools. He is the lead author of "National Security Law" (the field's leading casebook) and "Counterterrorism Law", and he was founding co-editor in chief of the Journal of National Security Law & Policy. (Stephen, "Congress' Role in Cyber Warfare," National Security Journal, Volume 4, Issue 155, 2010 http://jnslp.com/wp-content/uploads/2010/08/11\_Dycus.pdf)

Set out below are some steps that Congress might take to create an appropriate partnership. Some of these steps involve changes in congressional committees and responsibilities. Others would require coordination of cybersecurity functions within the executive branch. Still others would direct the President to keep Congress fully informed about anticipated and actual uses of cyber weapons. Several would restrict potential executive branch actions that seem – as a matter of policy – particularly unwise. 1. Designate a single committee in each House with primary responsibility for cyber warfare in order to develop a coherent and consistent legislative approach.60 2. Charge the designated committees with the development of broad policy and oversight of its implementation for both offensive and defensive uses of cyber weapons, given the close, perhaps indistinguishable, connection between the two uses. 3. Make the designated committees responsible for oversight of the relevant activities of the White House and every government agency concerned with cyber warfare, including the Defense Department, and their contractors, whether overt, clandestine, or covert. 4. Designate a lead federal agency to coordinate ongoing planning among agencies.61 The congressional committees would then have a principal point of contact for the collaborative development of policy. 5. Designate a lead agency to execute the cybersecurity plan.62 6. Order the preparation of a National Cybersecurity Strategy at prescribed intervals.63 This document should be declassified to the greatest extent possible, in order to inform every member of Congress and the public about the basic elements of U.S. cyber policy. 7. Require frequent, periodic briefings of the congressional committees, to enable serious consultation and advice in both directions as cyber policy evolves over time. These briefings should include information about rules of engagement, procedures for deciding to use cyber weapons, and any delegations of authority for such use. 8. Require consultation with the designated congressional committees in every possible instance before any significant use of cyber weapons.64 9. Require a written finding by the President, in advance of any significant use of cyber weapons whenever reasonably possible, or within a day or two afterward, that such use is or was necessary to the national security of the United States, that such use is or was as limited in scope as possible and consistent with the laws of armed conflict, and that Congress was consulted or could not be consulted because of the urgency of the threat. 10. Require immediate reports to the designated committees of any significant use of cyber weapons, either offensive or defensive. 11. Expressly forbid any withholding of information from the committees based on classification or for other reasons of secrecy. 12. Direct that all required reports be delivered to the designated committees as a whole, not merely to selected members.65 13. Expressly forbid automated offensive responses to actual or threatened cyber attacks on the United States under any circumstances. Given the potential for misperception or misinterpretation of an enemy attack, the difficulty of identifying the attacker and of assessing any resulting damage, and the risk of inadvertent escalation, any such response should be directed by a sentient human hand, informed by as much consultation with various government officials as the circumstances will permit.66 14. Create a government structure to coordinate assistance to private entities that come under cyber attack, so that such entities do not take matters into their own hands.67

### 2NC China/Taiwan

#### The Taiwan war wouldn’t escalate at all – China wouldn’t let it.

Austin & Gady 12 (Greg Austin – phD in International Relations, Vice President for the Worldwide Security Initiative, including a leadership role in the institute's work on cybersecurity, is now a Professorial Fellow. Greg has a 30-year career in international affairs, including senior posts in academia and government., Franz Stefan Gady -- M.A. in Strategic Studies/International Economics from the School of Advanced International Studies, Johns Hopkins University., “CYBER DETENTE BETWEEN THE U.S. AND CHINA: Shaping the Agenda, http://www.ewi.info/system/files/detente.pdf)

The type of war that China would want to fight over Taiwan, if forced to, would not be an all-out massive attack on Taiwanese and United States forces. Instead, it would prefer a carefully designed strategy of political, economic and military gambits intended to weaken the capacity or will of the United States to deliver overwhelming military power in the Taiwan region and to weaken the capacity of the Taiwan government to control the civil affairs of the island. A partial economic blockade or sanctions are more likely tools of choice for China than heavy reliance on cyber weapons for strategic impact, though such weapons could be used for operational and tactical effects.

--Where Emory’s card starts—

In sum, China is probably engaged in cyber warfare planning for operations against the United States on a very serious level, and possibly more so than for naval or air combat operations against it. At least in relative terms, China’s cyber warfare capability is probably far more powerful but less lethal than its conventional military capabilities. That suits China enormously in both respects. China’s military strategy is highly defensive, but to defend against U.S. operations against China over Taiwan, China has to rely mainly on unconventional operations, and these include cyber operations as well as psy-ops of the classic kind, including through fifth- column policies.

### 2NC China War

#### Shor evidence = mutually assured economic ties that prevent solvency

#### No military aggression

Goldstein 11—Professor and Director of the China Maritime Studies Institute @ US Naval War College [Dr. Lyle J. Goldstein, “Resetting the US–China Security Relationship,” Survival | vol. 53 no. 2 | April–May 2011 | pp. 89–116]

Weighed in the aggregate, China’s rise remains a peaceful process, and the record to date should engender significant confidence. Beijing has not resorted to a significant use of force against another state in more than three decades. Its deployments of troops as UN peacekeepers to hot spots such as Lebanon and the Democratic Republic of the Congo have played a helpful role, as have the counter-piracy operations of its fleet in the Gulf of Aden. When dealing with weak and occasionally unstable states on its borders, such as Kyrgyzstan or Tajikistan, Beijing has not resorted to military intervention, nor even flexed its military muscles to gain advantage. Chinese maritime claims, whether in the South or the East China seas, are generally being enforced by unarmed patrol cutters, a clear signal that Beijing does not seek escalation to a major crisis on these matters. Contrary to the perception that China’s senior military officers are all irreconcilable hawks, one influential People’s Liberation Army Navy (PLAN) admiral recently said in an interview, with reference to lessons learned from recent border negotiations on China’s periphery: ‘If there are never any concessions or compromises, there is simply no possibility of reaching a breakthrough in border negotiations.’2 pg. 90

#### No catching up anyway

**Zenko and Cohen 12** (Micah Zenko, Fellow in the Center for Preventive Action at the Council on Foreign Relations, and MIchael Cohen, Senior Fellow at the American Security Project, serves on the board of the National Security Network and has taught at Columbia University’s School of International and Public Affairs, served in the U.S. Department of State, former Senior Vice President at the strategic communications firm of Robinson, Lerer and Montgomery, bachelor’s degree in international relations from American University and a master’s degree from Columbia University, 3/14/2012, "Clear and Present Safety", yaleglobal.yale.edu/content/clear-and-present-safety)

As the threat from transnational terrorist groups dwindles, the United States also faces few risks from other states. China is the most obvious potential rival to the United States, and there is little doubt that China’s rise will pose a challenge to U.S. economic interests. Moreover, there is an unresolved debate among Chinese political and military leaders about China’s proper global role, and the lack of transparency from China’s senior leadership about its long-term foreign policy objectives is a cause for concern. However, the present security threat to the U.S. mainland is practically nonexistent and will remain so. Even as China tries to modernize its military, its defense spending is still approximately one-ninth that of the United States. In 2012, the Pentagon will spend roughly as much on military research and development alone as China will spend on its entire military. While China clumsily flexes its muscles in the Far East by threatening to deny access to disputed maritime resources, a recent Pentagon report noted that China’s military ambitions remain dominated by “regional contingencies” and that the People’s Liberation Army has made little progress in developing capabilities that “extend global reach or power projection.” In the coming years, China will enlarge its regional role, but this growth will only threaten U.S. interests if Washington attempts to dominate East Asia and fails to consider China’s legitimate regional interests. It is true that China’s neighbors sometimes fear that China will not resolve its disputes peacefully, but this has compelled Asian countries to cooperate with the United States, maintaining bilateral alliances that together form a strong security architecture and limit China’s room to maneuver. The strongest arguments made by those warning of Chinese influence revolve around economic policy. The list of complaints includes a host of Chinese policies, from intellectual property theft and currency manipulation to economic espionage and domestic subsidies. Yet none of those is likely to lead to direct conflict with the United States beyond the competition inherent in international trade, which does not produce zero-sum outcomes and is constrained by dispute-resolution mechanisms, such as those of the World Trade Organization. If anything, China’s export-driven economic strategy, along with its large reserves of U.S. Treasury bonds, suggests that Beijing will continue to prefer a strong United States to a weak one.

## Deterrence

### A2: Stein

1 – Stein has a bachelors degree and is a green builder. Not sure why he knows all the things about nuclear plants

2 – we have at least a week to get cooling systems running again – that’s the unhighlighted part

3 – 1NC Birch is a direct response to this impact – empirically blackouts don’t cause any of these impacts and attacks wouldn’t be on nuclear sources

More evidence

**No risk of attacks – newest evidence**

**NEI ’12** [Nuclear Energy Institute, “Myths & Facts About Safety”, January 2012, <http://www.nei.org/newsandevents/nei-backgrounders/myths--facts-about-nuclear-energy/myths--facts-about-safety>]

Myth: Nuclear power plants are likely targets for terrorism. Fact: With protective measures similar to high-security military installations, U.S. nuclear plants are among the most **highly protected facilities** in the nation’s industrial infrastructure. It is because of their fortifications and multiple layers of security that nuclear plants present a strong deterrent to potential threats. Myth: A nuclear power plant cannot withstand a terrorist attack. Fact: With protective measures similar to high-security military installations, U.S. nuclear plants are among the most highly protected facilities in the nation’s industrial infrastructure. Nuclear power plants are protected 24/7 by professional security personnel armed with automatic weapons prepared to repel ground and airborne terrorist attacks. It is because of their fortifications and multiple layers of security that nuclear plants are **far less likely** to be targets of terrorism than the thousands of far more vulnerable potential targets across the nation. Anti-terrorism measures are regularly tested and closely coordinated with local, state and federal authorities. Myth: A nuclear power plant cannot withstand the impact of a jetliner. Fact: Following the terrorist attacks of Sept. 11, 2001, sophisticated computer modeling by some of the world’s leading structural engineers showed that nuclear power facilities that contain radioactive material **can withstand a jetliner** impact without releasing radiation. Likewise, all new nuclear power plants are required to withstand the direct impact of a fully fueled commercial jetliner. Myth: Nuclear plants are vulnerable to cyber attacks. Fact: There has never been a successful cyber attack at any U.S. nuclear plant. Unlike industries for which two-way data flow is critical (e.g. banking), nuclear power plants do not require incoming data flow.None of a plant’s safety and control systems are connected to the Internet. Any additional computers utilized in a nuclear plants are strictly controlled with their content, use and possession monitored by security personnel. Nuclear plants are protected from grid instability and are able to safely shut down in a variety of ways without computer controls under any condition including a total loss of off-site power.

4 – your ev is about one reactor melting down and assumes that somehow escalates wildly – empirically denied

#### Meltdowns don’t cause extinction (empirics)

**WNA 12**(World nuclear association members are responsible for 95% of the world's nuclear power outside of the U.S., as well as the vast majority of world uranium, conversion and enrichment production, “Safety of Nuclear Power Reactors”, March 2012, WNA, <http://www.world-nuclear.org/info/inf06.html>, Chetan)

In the 1950s attention turned to harnessing the power of the atom in a controlled way, as demonstrated at Chicago in 1942 and subsequently for military research, and applying the steady heat yield to generate electricity. This naturally gave rise to concerns about accidents and their possible effects. However, with nuclear power safety depends on much the same factors as in any comparable industry: intelligent planning, proper design with conservative margins and back-up systems, high-quality components and a well-developed safety culture in operations. A particular nuclear scenario was loss of cooling which resulted in melting of the nuclear reactor core, and this motivated studies on both the physical and chemical possibilities as well as the biological effects of any dispersed radioactivity. Those responsible for nuclear power technology in the West devoted extraordinary effort to ensuring that a meltdown of the reactor core would not take place, since it was assumed that a meltdown of the core would create a major public hazard, and if uncontained, a tragic accident with likely multiple fatalities. In avoiding such accidents the industry has been very successful. In over 14,500 cumulative reactor-years of commercial operation in 32 countries, there have been only three major accidents to nuclear power plants - Three Mile Island, Chernobyl, and Fukushima - the second being of little relevance to reactor design outside the old Soviet bloc. It was not until the late 1970s that detailed analyses and large-scale testing, followed by the 1979 meltdown of the Three Mile Island reactor, began to make clear that even the worst possible accident in a conventional western nuclear power plant or its fuel would not be likely to cause dramatic public harm. The industry still works hard to minimize the probability of a meltdown accident, but it is now clear that no-one need fear a potential public health catastrophe simply because a fuel meltdown happens. Fukushima has made that clear, with a triple meltdown causing no fatalities or serious radiation doses to anyone, while over two hundred people continued working on the site to mitigate the accident's effects. The decades-long test and analysis program showed that less radioactivity escapes from molten fuel than initially assumed, and that most of this radioactive material is not readily mobilized beyond the immediate internal structure. Thus, even if the containment structure that surrounds all modern nuclear plants were ruptured, as it has been with at least one of the Fukushima reactors, it is still very effective in preventing escape of most radioactivity. It is the laws of physics and the properties of materials that mitigate disaster, more than the required actions by safety equipment or personnel. In fact, licensing approval for new plants now requires that the effects of any core-melt accident must be confined to the plant itself, without the need to evacuate nearby residents. The three significant accidents in the 50-year history of civil nuclear power generation are: Three Mile Island (USA 1979) where the reactor was severely damaged but radiation was contained and there were no adverse health or environmental consequences Chernobyl (Ukraine 1986) where the destruction of the reactor by steam explosion and fire killed 31 people and had significant health and environmental consequences. The death toll has since increased to about 5 Fukushima (Japan 2011) where three old reactors (together with a fourth) were written off and the effects of loss of cooling due to a huge tsunami were inadequately contained. A table showing all reactor accidents, and a table listing some energy-related accidents with multiple fatalities are appended. These three significant accidents occurred during more than 14,000 reactor-years of civil operation. Of all the accidents and incidents, only the Chernobyl and Fukushima accidents resulted in radiation doses to the public greater than those resulting from the exposure to natural sources. The Fukushima accident resulted in some radiation exposure of workers at the plant, but not such as to threaten their health, unlike Chernobyl. Other incidents (and one 'accident') have been completely confined to the plant. Apart from Chernobyl, no nuclear workers or members of the public have ever died as a result of exposure to radiation due to a commercial nuclear reactor incident. Most of the serious radiological injuries and deaths that occur each year (2-4 deaths and many more exposures above regulatory limits) are the result of large uncontrolled radiation sources, such as abandoned medical or industrial equipment. (There have also been a number of accidents in experimental reactors and in one military plutonium-producing pile - at Windscale, UK, in 1957, but none of these resulted in loss of life outside the actual plant, or long-term environmental contamination.) See also Table 2 in Appendix.

### Grid 2NC

**No black-outs in the US**

**Wood 12** -- Senior Communications Advisor at Business Roundtable (Carter, 8/2/12, "The grid: After India, America? No, but still…" http://businessroundtable.org/blog/the-grid-after-india-america-no-but-still/)

**A blackout of such scale could not happen in the U**nited **S**tates. For one thing, we don't have 600 million people. And America's electrical grid is certainly much more resilient than the one in India, a still-developing country with ineffective governments. Still, as The Washington Post reports today, "Aging power grid on overload as U.S. demands more electricity." At CNBC, Jim Cramer asked Thomas F. Farrell II, Chairman, President & CEO of Dominion Resources, about India. Could the same thing happen in the United States? Farrell responded: Our system has **a lot more rigor** to it and partly because we have reserve margins, meaning we have more power stations than we need to run at any particular moment in time, so that **if a power station goes out, there's a back-up** to help keep the grid stable. They don't have that much excess power in India, and when they get to the root cause, they'll probably find that was somewhere in there.

**US grid stable – frequency can be maintained by new technologies**

**Lamonica 12** -- senior writer covering green tech and cutting-edge technologies, contributor @ Technology Review (Martin, 8/2/12, "Outage in India Could Be a Harbinger for the Rest of the World," http://www.technologyreview.com/news/428685/outage-in-india-could-be-a-harbinger-for-the-rest/)

The primary function of grid operators is to anticipate load and to maintain a steady balance between power supply and demand. The grid signal operates at a set frequency—60 hertz in the U.S. and 50 hertz in India—and when supply and demand fall out of sync, the frequency will either dip or rise. In the U.S., grid operators have "hot" generators on standby to ramp up power in order to keep a close-to-steady frequency, but that's not the case when generators are routinely maxed out. "In a developing world country, it's tough to keep 10 percent of the generation capacity on contingency when you may use it once in a lifetime," Mansoor says. "You're not using the generator, but you still pay for it. That's tough to do." More technologies to keep that frequency steady are emerging. Sensors called phasor measurement units are designed for real-time measurement of grid frequency, and can **flag potential problems**. Grid operators in the United States are increasingly using automation to manage demand-response programs that lower consumption at big power users at peak times. These types of technologies as well as microgrids (see "Microgrids Keeps the Power Local, Cheap, and Reliable") stand to make electricity grids more reliable as more renewable resources come online and weather-related events, such as heat waves, strain generating resources.

### 2NC Space War

#### 1NC Klein – space weapons not only don’t escalate they have a *stabilizing effect* – this is a conceded warrant by the 2AC – leaders will avoid wars because of the chilling effect of the possession

#### No escalation and no war

**Weston 09** – Major, attending Joint Military Attaché School en route to serve as the assistant air attaché to the Republic of the Philippines (Scott A, Spring 2009, "Examining Space Warfare: Scenarios, Risks, and US Policy Implications," Proquest, RG)

In the first scenario, the United States deploys to defend Taiwan against China’s attempt to subdue the island forcibly. As in the RAND study, China would likely refrain from attacking US space assets to preserve its own space ISR capability, which it needs to monitor the US buildup. The United States would also delay full counterspace operations until fully deployed in order to prepare for retaliation with assets in place instead of in transit, where space disruption would cause much more confusion. With the United States almost fully deployed, China would do well to utilize any counterspace weapons it possesses before the United States targets them. Given its limited ASAT capability, China would likely target US military communication and reconnaissance satellites, avoiding permanent damage to dual-use commercial satellites to preserve its global reputation and protect its own third-party commercial space contracts. The Chinese would use kinetic attacks and any rapidly deployed ASAT lasers against low-altitude satellites, such as those performing reconnaissance, while likely attacking high-altitude communication satellites by jamming or feeding them malicious code. In addition to hitting space assets, China would probably deploy high-powered GPS and other signal jamming throughout the theater to degrade US bombing accuracy and complicate navigation. US doctrine, which places priority on air and space superiority, suggests that the first US attack would target China’s ground-based counterspace capability, using the full range of joint-attack forces and munitions. This first wave of ground attacks would also combine with counterspace offensive operations of a nondestructive nature, as highlighted in the Schriever war games, to temporarily blind Chinese ISR satellites and jam communication and signal-collection satellites. A few political caveats attach to this doctrine-directed target list, however. China’s launch facilities are far inland, thus raising the possibility that it would consider strikes in these areas a significant escalation, just as the United States would consider Chinese attacks on US launch facilities at Cape Canaveral, Florida, and Vandenberg AFB, California, provocative. The United States would also have to avoid targeting ground-based missile-launch-detection capabilities, which China might interpret as preparation for a nuclear first strike. As mentioned in the RAND war-game scenario, China would be far less affected than the United States by the loss of most space assets at this point because its air-breathing ISR assets could cover the immediate theater and short-range ground communications that do not rely upon satellites.37 Conversely, once US forces have deployed, they would rely heavily upon space assets. In a limited military engagement such as this, it is unlikely that the United States would attempt to facilitate ISR flights by establishing air superiority over all of China. US forces would thus remain highly reliant upon satellites for ISR over mainland China and for communication with the homeland and between deployed units. The RAND study also pointed out that China would likely contract commercial third-party space assets to provide needed capabilities, complicating repercussions from US attacks. All told, counterspace operations would probably prove as discriminate as possible to prevent strategic escalation. Both sides would hesitate to utilize kinetic-kill ASATs against anything but very low-altitude satellites for fear of incurring international condemnation and increasing debris hazards for their own resources.38 In all likelihood, the United States would not use its kinetic ASAT capability, preferring to utilize its limited number of sea-based Standard Missile 3s for ABM defense of forward-deployed forces. Thus, the number of satellites destroyed or permanently disabled would be very low. As limited as this scenario appears, it bears out realistic actions taken under current policy and doctrine, given the resources available to each side. In this case, it is difficult to see how even one of our most capable space adversaries would have either the capability or the motivation to attempt a surprise attack on US space assets that would rise to the level of a space Pearl Harbor. It is also difficult to understand how the cost of deploying hundreds or even thousands of US weapon satellites to ensure space dominance would greatly affect the outcome of this scenario. Even a deployed space-based missile-defense shield probably would not encourage the United States to intentionally escalate a limited regional conflict with another nuclear power to a full nuclear exchange if there were any risk of nuclear warheads reaching US soil.

#### No arms race

Lopez 12 – Laura Delgado Lopez, expert at the Institute for Global Environmental Studies, Arlington, Virginia, master's degree in international science and technology from George Washington University, 2009 Truman Scholar and a Northrop Grumman Fellow at GWU's Space Policy Institute, bachelor's in political science, March 6th, 2012, "Predicting an Arms Race in Space: Problematic Assumptions for Space Arms Control" [www.tandfonline.com/doi/pdf/10.1080/14777622.2012.647391](http://www.tandfonline.com/doi/pdf/10.1080/14777622.2012.647391)

**Referring to the history of the nuclear arms race, as space doves often do, is misleading**. The Soviet Union and the United States did race to build up their nuclear arsenals, but that was because they could, both technologically and economically. Interestingly, while both lawful 43 and potentially illegal transfers of nuclear technology have taken place, the list of countries with known or suspected nuclear technology is still relatively small. 44 Moreover, it would be open to debate whether those countries that possess the knowledge of how to build nuclear weapons are currently immersed in a race to build up their arsenals in response to that of other countries. It is probable that limited proliferation may be a sign of the success of an efficient arms control regime, but it is nevertheless evident that adequate resources are a necessary prerequisite for an arms race**.**¶ **In the case of** space weapons**, the** conditions are even harsher**.** The incredible cost not only to develop and launch these systems, but to maintain them has been a major impediment to their development. Brilliant Pebbles, arguably the most cost-effective U.S. space-based missile defense program, which would also amount to an ASAT weapon, still amounted to a price tag of between $11 and $16 billion, expended over a 20-year period. 45 Would a country such as Pakistan, which ranks twenty-eighth in the U.S. Central Intelligence Agency’s World Factbook Gross Domestic Product comparison, be able to raise the kind of resources necessary for racing other countries in space? It is more probable that countries such as China and Russia would be able to compete if they so chose, 46 but **the idea of a worldwide space arms race can still not be sustained**. And therein lies the biggest issue that space doves fail to address in their arguments about an inevitable space race: resources. The perception of a threat and the political will to meet it are not enough to warrant the kind of worldwide conditions they are so quick to describe.¶ When space doves bring up the question of resources, they point to ‘‘asymmetric challenges from those who could not afford to be participants in the race itself.’’ 47 This situation might encourage, for instance, nuclear proliferation or the build-up of chemical or biological weapons. In fact, Nancy Gallagher argues that the United States rightly denies the existence of an arms race in space ‘‘only in the narrow sense that there is not, and probably will not be, a Cold War style ‘space arms race,’ i.e., an action-reaction dynamic between peer competitors,’’ but that doing so ignores the danger of ‘‘asymmetric reactions.’’ 48¶ Space doves thus seem to acknowledge that measures to regain or sustain stability in the international system do not always manifest themselves in the same way because power can take many forms. In proposing his concept of ‘‘soft power’’ as a legitimate tool for the United States to exert international influence, Joseph Nye explained that in a world of increased political complexity, the traditional ways to employ force are too costly, and thus ‘‘other instruments such as communications. . . and manipulation of interdependence have become more important.’’ 49¶ But this contention clearly **invalidates the inevitability of an arms race in space**. If countries do not respond in kind, then there is no race to speak of, and the inevitability argument breaks down. Gallagher’s statement thus seems contradictory: if a space race is not an ‘‘action-reaction dynamic between peer-competitors,’’ then what do space doves mean with an arms race? Why must it be avoided?¶ **This issue also raises a more** important problem: causality. **Unless other countries explicitly state that their asymmetric build-up is a direct response to U.S. deployment of space weapons, then** this link cannot be established**.** Even considering the timing sequence of deployment and the projected build-up—which would be difficult considering it takes years to develop, launch, and deploy space systems—**it would be simplistic to assume that other motivators for international behavior are not at work.**

### 2NC Miscalc

**No accidental or miscalc escalation**

– history and disaster behavior studies prove

**Mueller ’10** [John Mueller – Woody Hayes Chair of National Security Studies, Mershon Center, and professor of Political Science, at Ohio State University, Atomic Obsession: Nuclear Alarmism from Hiroshima to Al-Qaeda, p. 100

However, even if a bomb, or a few bombs, were to go off, it does not necessarily follow that war would result. For that to happen, it is usually assumed, the accident would have to take place at a time of high war- readiness, as during a crisis, when both sides are poised for action and when one side could perhaps be triggered—or panicked—into major action by an explosion mistakenly taken to be part of, or the prelude to, a full attack." This means that the unlikely happening—a nuclear accident—would have to coincide precisely with an event, a militarized international crisis, something that is rare to begin with, became more so as the cold war progressed, and has become even less likely since its demise. Furthermore, even if the accident takes place during a crisis, it does not follow that escalation or hasty response is inevitable, or even very likely. As Bernard Brodie points out, escalation scenarios essentially impute to both sides "a well-nigh limitless concern with saving face" and/or "a great deal of ground-in automaticity of response and counterresponse." None of this was in evidence during the Cuban missile crisis when there were accidents galore. An American spy plane was shot down over Cuba, probably without authorization, and another accidentally went off course and flew threateningly over the Soviet Union. As if that weren't enough, a Soviet military officer spying for the West sent a message, apparently on a whim, warning that the Soviets were about to attack." **None of these remarkable events triggered anything in the way of precipitous response**. They were duly evaluated and then ignored. Robert Jervis points out that "when critics talk of the impact of irrationality, they imply that all such deviations will be in the direction of emotional impulsiveness, of launching an attack, or of taking actions that are terribly risky. Bu**t irrationality could** also **lead a state to passive acquiescence:"** In moments of high stress and threat, people can be said to have three psychological alternatives: (1) to remain calm and rational, (2) to refuse to believe that the threat is imminent or significant, or (3) to panic, lashing out frantically and incoherently at the threat. Generally, people react in one of the first two ways. In her classic study of disaster behavior, Martha Wolfenstein concludes, "The usual reaction is one of being unworried."32 In addition, **the historical record suggests that wars simply do not begin by accident**. In his extensive survey of wars that have occurred since 1400, diplomat-historian Evan Luard concludes, "It is impossible to identify a single case in which it can be said that a war started accidentally; in which it was not, at the time the war broke out, the deliberate intention of at least one party that war should take place." Geoffrey Blainey, after similar study, very much agrees: although many have discussed "accidental" or "unintentional" wars, "it is difficult," he concludes, "to find a war which on investigation fits this description." Or, as Henry Kissinger has put it dryly, "Despite popular myths, large military units do not fight by accident.""

### 2NC Cyber Inevitable

#### 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.

### 2NC Cyberwar

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

**MARKED**

**MARKED**

ial 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.

Cyberattacks nearly impossible – empirics and defenses solve

**Rid 12** (Thomas Rid, reader in war studies at King's College London, is author of "Cyber War Will Not Take Place" and co-author of "Cyber-Weapons.", March/April 2012, “Think Again: Cyberwar”, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full)

"Cyberwar Is Already Upon Us." No way. "Cyberwar is coming!" John Arquilla and David Ronfeldt predicted in a celebrated Rand paper back in 1993. Since then, it seems to have arrived -- at least by the account of the U.S. military establishment, which is busy competing over who should get what share of the fight. Cyberspace is "a domain in which the Air Force flies and fights," Air Force Secretary Michael Wynne claimed in 2006. By 2012, William J. Lynn III, the deputy defense secretary at the time, was writing that cyberwar is "just as critical to military operations as land, sea, air, and space." In January, the Defense Department vowed to equip the U.S. armed forces for "conducting a combined arms campaign across all domains -- land, air, maritime, space, and cyberspace." Meanwhile, growing piles of books and articles explore the threats of cyberwarfare, cyberterrorism, and how to survive them. Time for a reality check: Cyberwar is still more hype than hazard. Consider the definition of an act of war: It has to be potentially violent, it has to be purposeful, and it has to be political. The cyberattacks we've seen so far, from Estonia to the Stuxnet virus, simply don't meet these criteria. Take the dubious story of a Soviet pipeline explosion back in 1982, much cited by cyberwar's true believers as the most destructive cyberattack ever. The account goes like this: In June 1982, a Siberian pipeline that the CIA had virtually booby-trapped with a so-called "logic bomb" exploded in a monumental fireball that could be seen from space. The U.S. Air Force estimated the explosion at 3 kilotons, equivalent to a small nuclear device. Targeting a Soviet pipeline linking gas fields in Siberia to European markets, the operation sabotaged the pipeline's control systems with software from a Canadian firm that the CIA had doctored with malicious code. No one died, according to Thomas Reed, a U.S. National Security Council aide at the time who revealed the incident in his 2004 book, At the Abyss; the only harm came to the Soviet economy. But did it really happen? After Reed's account came out, Vasily Pchelintsev, a former KGB head of the Tyumen region, where the alleged explosion supposedly took place, denied the story. There are also no media reports from 1982 that confirm such an explosion, though accidents and pipeline explosions in the Soviet Union were regularly reported in the early 1980s. Something likely did happen, but Reed's book is the only public mention of the incident and his account relied on a single document. Even after the CIA declassified a redacted version of Reed's source, a note on the so-called Farewell Dossier that describes the effort to provide the Soviet Union with defective technology, the agency did not confirm that such an explosion occurred. The available evidence on the Siberian pipeline blast is so thin that it shouldn't be counted as a proven case of a successful cyberattack. Most other commonly cited cases of cyberwar are even less remarkable. Take the attacks on Estonia in April 2007, which came in response to the controversial relocation of a Soviet war memorial, the Bronze Soldier. The well-wired country found itself at the receiving end of a massive distributed denial-of-service attack that emanated from up to 85,000 hijacked computers and lasted three weeks. The attacks reached a peak on May 9, when 58 Estonian websites were attacked at once and the online services of Estonia's largest bank were taken down. "What's the difference between a blockade of harbors or airports of sovereign states and the blockade of government institutions and newspaper websites?" asked Estonian Prime Minister Andrus Ansip. Despite his analogies, the attack was no act of war. It was certainly a nuisance and an emotional strike on the country, but the bank's actual network was not even penetrated; it went down for 90 minutes one day and two hours the next. The attack was not violent, it wasn't purposefully aimed at changing Estonia's behavior, and no political entity took credit for it. The same is true for the vast majority of cyberattacks on record. Indeed, there is no known cyberattack that has caused the loss of human life. No cyberoffense has ever injured a person or damaged a building. And if an act is not at least potentially violent, it's not an act of war. Separating war from physical violence makes it a metaphorical notion; it would mean that there is no way to distinguish between World War II, say, and the "wars" on obesity and cancer. Yet those ailments, unlike past examples of cyber "war," actually do kill people. "A Digital Pearl Harbor Is Only a Matter of Time." Keep waiting. U.S. Defense Secretary Leon Panetta delivered a stark warning last summer: "We could face a cyberattack that could be the equivalent of Pearl Harbor." Such alarmist predictions have been ricocheting inside the Beltway for the past two decades, and some scaremongers have even upped the ante by raising the alarm about a cyber 9/11. In his 2010 book, Cyber War, former White House counterterrorism czar Richard Clarke invokes the specter of nationwide power blackouts, planes falling out of the sky, trains derailing, refineries burning, pipelines exploding, poisonous gas clouds wafting, and satellites spinning out of orbit -- events that would make the 2001 attacks pale in comparison. But the empirical record is less hair-raising, even by the standards of the most drastic example available. Gen. Keith Alexander, head of U.S. Cyber Command (established in 2010 and now boasting a budget of more than $3 billion), shared his worst fears in an April 2011 speech at the University of Rhode Island: "What I'm concerned about are destructive attacks," Alexander said, "those that are coming." He then invoked a remarkable accident at Russia's Sayano-Shushenskaya hydroelectric plant to highlight the kind of damage a cyberattack might be able to cause. Shortly after midnight on Aug. 17, 2009, a 900-ton turbine was ripped out of its seat by a so-called "water hammer," a sudden surge in water pressure that then caused a transformer explosion. The turbine's unusually high vibrations had worn down the bolts that kept its cover in place, and an offline sensor failed to detect the malfunction. Seventy-five people died in the accident, energy prices in Russia rose, and rebuilding the plant is slated to cost $1.3 billion. Tough luck for the Russians, but here's what the head of Cyber Command didn't say: The ill-fated turbine had been malfunctioning for some time, and the plant's management was notoriously poor. On top of that, the key event that ultimately triggered the catastrophe seems to have been a fire at Bratsk power station, about 500 miles away. Because the energy supply from Bratsk dropped, authorities remotely increased the burden on the Sayano-Shushenskaya plant. The sudden spike overwhelmed the turbine, which was two months shy of reaching the end of its 30-year life cycle, sparking the catastrophe. If anything, the Sayano-Shushenskaya incident highlights how difficult a devastating attack would be to mount. The plant's washout was an accident at the end of a complicated and unique chain of events. Anticipating such vulnerabilities in advance is extraordinarily difficult even for insiders; creating comparable coincidences from cyberspace would be a daunting challenge at best for outsiders. If this is the most drastic incident Cyber Command can conjure up, perhaps it's time for everyone to take a deep breath. "Cyberattacks Are Becoming Easier." Just the opposite. U.S. Director of National Intelligence James R. Clapper warned last year that the volume of malicious software on American networks had more than tripled since 2009 and that more than 60,000 pieces of malware are now discovered every day. The United States, he said, is undergoing "a phenomenon known as 'convergence,' which amplifies the opportunity for disruptive cyberattacks, including against physical infrastructures." ("Digital convergence" is a snazzy term for a simple thing: more and more devices able to talk to each other, and formerly separate industries and activities able to work together.) Just because there's more malware, however, doesn't mean that attacks are becoming easier. In fact, potentially damaging or life-threatening cyberattacks should be more difficult to pull off. Why? Sensitive systems generally have built-in redundancy and safety systems, meaning an attacker's likely objective will not be to shut down a system, since merely forcing the shutdown of one control system, say a power plant, could trigger a backup and cause operators to start looking for the bug. To work as an effective weapon, malware would have to influence an active process -- but not bring it to a screeching halt. If the malicious activity extends over a lengthy period, it has to remain stealthy. That's a more difficult trick than hitting the virtual off-button. Take Stuxnet, the worm that sabotaged Iran's nuclear program in 2010. It didn't just crudely shut down the centrifuges at the Natanz nuclear facility; rather, the worm subtly manipulated the system. Stuxnet stealthily infiltrated the plant's networks, then hopped onto the protected control systems, intercepted input values from sensors, recorded these data, and then provided the legitimate controller code with pre-recorded fake input signals, according to researchers who have studied the worm. Its objective was not just to fool operators in a control room, but also to circumvent digital safety and monitoring systems so it could secretly manipulate the actual processes. Building and deploying Stuxnet required extremely detailed intelligence about the systems it was supposed to compromise, and the same will be true for other dangerous cyberweapons. Yes, "convergence," standardization, and sloppy defense of control-systems software could increase the risk of generic attacks, but the same trend has also caused defenses against the most coveted targets to improve steadily and has made reprogramming highly specific installations on legacy systems more complex, not less.

**No impact to cyberwar - it's all hype - it's technically impossible and won't escalate**

**Rid 12** (Thomas, PhD, Reader in War Studies @ King's College London, Non-Resident Fellow at the Center for Transatlantic Relations in the School for Advanced International Studies at Johns Hopkins, "Think Again: Cyberwar," March/April, Foreign Policy, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,0,

Time for a reality check: Cyberwar is still more hype than hazard. Consider the definition of an act of war: It has to be potentially violent, it has to be purposeful, and it has to be political. The cyberattacks we've seen so far, from Estonia to the Stuxnet virus, simply don't meet these criteria. Take the dubious story of a Soviet pipeline explosion back in 1982, much cited by cyberwar's true believers as the most destructive cyberattack ever. The account goes like this: In June 1982, a Siberian pipeline that the CIA had virtually booby-trapped with a so-called "logic bomb" exploded in a monumental fireball that could be seen from space. The U.S. Air Force estimated the explosion at 3 kilotons, equivalent to a small nuclear device. Targeting a Soviet pipeline linking gas fields in Siberia to European markets, the operation sabotaged the pipeline's control systems with software from a Canadian firm that the CIA had doctored with malicious code. No one died, according to Thomas Reed, a U.S. National Security Council aide at the time who revealed the incident in his 2004 book, At the Abyss; the only harm came to the Soviet economy. But did it really happen? After Reed's account came out, Vasily Pchelintsev, a former KGB head of the Tyumen region, where the alleged explosion supposedly took place, denied the story. There are also no media reports from 1982 that confirm such an explosion, though accidents and pipeline explosions in the Soviet Union were regularly reported in the early 1980s. Something likely did happen, but Reed's book is the only public mention of the incident and his account relied on a single document. Even after the CIA declassified a redacted version of Reed's source, a note on the so-called Farewell Dossier that describes the effort to provide the Soviet Union with defective technology, the agency did not confirm that such an explosion occurred. The available evidence on the Siberian pipeline blast is so thin that it shouldn't be counted as a proven case of a successful cyberattack. Most other commonly cited cases of cyberwar are even less remarkable. Take the attacks on Estonia in April 2007, which came in response to the controversial relocation of a Soviet war memorial, the Bronze Soldier. The well-wired country found itself at the receiving end of a massive distributed denial-of-service attack that emanated from up to 85,000 hijacked computers and lasted three weeks. The attacks reached a peak on May 9, when 58 Estonian websites were attacked at once and the online services of Estonia's largest bank were taken down. "What's the difference between a blockade of harbors or airports of sovereign states and the blockade of government institutions and newspaper websites?" asked Estonian Prime Minister Andrus Ansip. Despite his analogies, the attack was no act of war. It was certainly a nuisance and an emotional strike on the country, but the bank's actual network was not even penetrated; it went down for 90 minutes one day and two hours the next. The attack was not violent, it wasn't purposefully aimed at changing Estonia's behavior, and no political entity took credit for it. The same is true for the vast majority of cyberattacks on record. Indeed, there is no known cyberattack that has caused the loss of human life. No cyberoffense has ever injured a person or damaged a building. And if an act is not at least potentially violent, it's not an act of war. Separating war from physical violence makes it a metaphorical notion; it would mean that there is no way to distinguish between World War II, say, and the "wars" on obesity and cancer. Yet those ailments, unlike past examples of cyber "war," actually do kill people. "A Digital Pearl Harbor Is Only a Matter of Time." Keep waiting. U.S. Defense Secretary Leon Panetta delivered a stark warning last summer: "We could face a cyberattack that could be the equivalent of Pearl Harbor." Such alarmist predictions have been ricocheting inside the Beltway for the past two decades, and some scaremongers have even upped the ante by raising the alarm about a cyber 9/11. In his 2010 book, Cyber War, former White House counterterrorism czar Richard Clarke invokes the specter of nationwide power blackouts, planes falling out of the sky, trains derailing, refineries burning, pipelines exploding, poisonous gas clouds wafting, and satellites spinning out of orbit -- events that would make the 2001 attacks pale in comparison. But the empirical record is less hair-raising, even by the standards of the most drastic example available. Gen. Keith Alexander, head of U.S. Cyber Command (established in 2010 and now boasting a budget of more than $3 billion), shared his worst fears in an April 2011 speech at the University of Rhode Island: "What I'm concerned about are destructive attacks," Alexander said, "those that are coming." He then invoked a remarkable accident at Russia's Sayano-Shushenskaya hydroelectric plant to highlight the kind of damage a cyberattack might be able to cause. Shortly after midnight on Aug. 17, 2009, a 900-ton turbine was ripped out of its seat by a so-called "water hammer," a sudden surge in water pressure that then caused a transformer explosion. The turbine's unusually high vibrations had worn down the bolts that kept its cover in place, and an offline sensor failed to detect the malfunction. Seventy-five people died in the accident, energy prices in Russia rose, and rebuilding the plant is slated to cost $1.3 billion. Tough luck for the Russians, but here's what the head of Cyber Command didn't say: The ill-fated turbine had been malfunctioning for some time, and the plant's management was notoriously poor. On top of that, the key event that ultimately triggered the catastrophe seems to have been a fire at Bratsk power station, about 500 miles away. Because the energy supply from Bratsk dropped, authorities remotely increased the burden on the Sayano-Shushenskaya plant. The sudden spike overwhelmed the turbine, which was two months shy of reaching the end of its 30-year life cycle, sparking the catastrophe. If anything, the Sayano-Shushenskaya incident highlights how difficult a devastating attack would be to mount. The plant's washout was an accident at the end of a complicated and unique chain of events. Anticipating such vulnerabilities in advance is extraordinarily difficult even for insiders; creating comparable coincidences from cyberspace would be a daunting challenge at best for outsiders. If this is the most drastic incident Cyber Command can conjure up, perhaps it's time for everyone to take a deep breath.

**Their evidence is flawed and should be rejected**

**Rahman ’10** (Arifeen Rahman, SEA National Security Intern, Scientist and Engineers for America, “Bringing Cybersecurity Back to Reality”, <http://www.sefora.org/2010/08/11/rahman_0811/>, August 11, 2010, LEQ)

The controversy over “cyber-rhetoric” is often reduced to a debate over the devastating magnitude of such possible scenarios versus the risks of framing them in such language. However, the truths in both positions do not inherently contradict each other, and can be reconciled. The great equalizer of these theories, therefore, lies in an analysis of predictions. The extent to which we can, or arguably should, take pre-emptive action to prevent cyber-attacks has its foundations in the determining the probability of these events. **Recent trends in the cyber security discussion have forgone an assessment of probability for a “possibilistic” worst case assessment. Most studies tend to sensationalize** the **threats** which cyberspace presents, **forecasting imminent scenarios of destruction. Not only have these predictions been categorically proven false over the last ten years, but have also brought into question the reliability of these assessments overall.**  Black Swan theory, coined by Nassim Nicholas Taleb, explains how **major catastrophes are low probability**, high impact scenarios which were impossible to predict, but seem inevitable when looked at retrospectively. Viewing cyber security through this lens allows for a separation of policy from threat inflation. Black Swan theory proves that **obsession over specific scenarios of cyber attack remain futile.** The scenario which is never considered, which is most unexpected, will occur. Therefore, the only logical way to maintain cyber security is to preserve defensive protection of critical infrastructure, and avoid hyping up new threats. […] Cyber security will remain a critical issue for the current and all following administrations. In order to create a safe and secure environment, critical vulnerabilities must be addressed without creating an atmosphere of fear and paranoia. **The “cyber-Armageddon” is not coming.** It’s time for the federal government to get its head out its science fiction novel, and get back to reality.

**Zero risk of cyber attack- new studies**

**Leyden ’11** (The ill-informed leading the ill-informed... By [John Leyden](http://forms.theregister.co.uk/mail_author/?story_url=/2011/01/17/cyberwar_hype_oecd_study/) • [Get more from this author](http://search.theregister.co.uk/?author=John%20Leyden) Posted in [Government](http://www.theregister.co.uk/public_sector/government/), [17th January 2011 11:23 GMT](http://www.theregister.co.uk/2011/01/17/)

**Cyberwar hype is inhibiting government attempts to develop an appropriate response to cybersecurity threats, say computer scientists. A heavyweight study by UK computer scientists** **for the** Organisation for Economic Cooperation and Development (**OECD) concludes that it is "highly unlikely" there will ever be a "pure cyber war”,** comparable with recent conflicts in Afghanistan or the Balkans. **Suggestions to the contrary are down to "heavy lobbying" by suppliers**, the report's authors – Professor Peter Sommer of the London School of Economics and Dr Ian Brown of the Oxford Internet Institute, University of Oxford – conclude. It is unlikely that there will ever be a true cyberwar**. The reasons are: many critical computer systems are protected against known exploits and malware so that designers of new cyberweapons have to identify new weaknesses and exploits; the effects of cyberattacks are difficult to predict** **– on the one hand they may be less powerful than hoped but may also have more extensive outcomes arising from the interconnectedness of systems, resulting in unwanted damage to perpetrators and their allies**. More importantly, there is no strategic reason why any aggressor would limit themselves to only one class of weaponry.

**At worst the impact will be contained**

**Rid 12** (Thomas, PhD, Reader in War Studies @ King's College London, Non-Resident Fellow at the Center for Transatlantic Relations in the School for Advanced International Studies at Johns Hopkins, "Think Again: Cyberwar," March/April, Foreign Policy, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,0,

"Cyberweapons Can Create Massive Collateral Damage." Very unlikely. When news of Stuxnet broke, the New York Times reported that the most striking aspect of the new weapon was the "collateral damage" it created. The malicious program was "splattered on thousands of computer systems around the world, and much of its impact has been on those systems, rather than on what appears to have been its intended target, Iranian equipment," the Times reported. Such descriptions encouraged the view that computer viruses are akin to highly contagious biological viruses that, once unleashed from the lab, will turn against all vulnerable systems, not just their intended targets. But this metaphor is deeply flawed. As the destructive potential of a cyberweapon grows, the likelihood that it could do far-reaching damage across many systems shrinks. Stuxnet did infect more than 100,000 computers -- mainly in Iran, Indonesia, and India, though also in Europe and the United States. But it was so specifically programmed that it didn't actually damage those machines, afflicting only Iran's centrifuges at Natanz. The worm's aggressive infection strategy was designed to maximize the likelihood that it would reach its intended target. Because that final target was not networked, "all the functionality required to sabotage a system was embedded directly in the Stuxnet executable," the security software company Symantec observed in its analysis of the worm's code. So yes, Stuxnet was "splattered" far and wide, but it only executed its damaging payload where it was supposed to. Collateral infection, in short, is not necessarily collateral damage. A sophisticated piece of malware may aggressively infect many systems, but if there is an intended target, the infection will likely have a distinct payload that will be harmless to most computers. Especially in the context of more sophisticated cyberweapons, the image of inadvertent collateral damage doesn't hold up. They're more like a flu virus that only makes one family sick.

**Defensive measures overwhelm**

**Rid 12** (Thomas, PhD, Reader in War Studies @ King's College London, Non-Resident Fellow at the Center for Transatlantic Relations in the School for Advanced International Studies at Johns Hopkins, "Think Again: Cyberwar," March/April, Foreign Policy, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,0,

"In Cyberspace, Offense Dominates Defense." Wrong again. The information age has "offense-dominant attributes," Arquilla and Ronfeldt wrote in their influential 1996 book, The Advent of Netwar. This view has spread through the American defense establishment like, well, a virus. A 2011 Pentagon report on cyberspace stressed "the advantage currently enjoyed by the offense in cyberwarfare." The intelligence community stressed the same point in its annual threat report to Congress last year, arguing that offensive tactics -- known as vulnerability discovery and exploitation -- are evolving more rapidly than the federal government and industry can adapt their defensive best practices. The conclusion seemed obvious: Cyberattackers have the advantage over cyberdefenders, "with the trend likely getting worse over the next five years." A closer examination of the record, however, reveals three factors that put the offense at a disadvantage. First is the high cost of developing a cyberweapon, in terms of time, talent, and target intelligence needed. Stuxnet, experts speculate, took a superb team and a lot of time. Second, the potential for generic offensive weapons may be far smaller than assumed for the same reasons, and significant investments in highly specific attack programs may be deployable only against a very limited target set. Third, once developed, an offensive tool is likely to have a far shorter half-life than the defensive measures put in place against it. Even worse, a weapon may only be able to strike a single time; once the exploits of a specialized piece of malware are discovered, the most critical systems will likely be patched and fixed quickly. And a weapon, even a potent one, is not much of a weapon if an attack cannot be repeated. Any political threat relies on the credible threat to attack or to replicate a successful attack. If that were in doubt, the coercive power of a cyberattack would be drastically reduced.