# 1NC

## 1NC

#### Interpretation:

#### Increase requires pre-existing entities.

**Brown**, US District Judge, 7-17-200**3**

[Anna J., UNITED STATES DISTRICT COURT FOR THE DISTRICT OF OREGON, 275 F. Supp. 2d 1307; 2003 U.S. Dist. LEXIS 13355, l/n, accessed 8-1-10, mss]

The Fair Credit Reporting Act does not define the term "increase." The plain and ordinary meaning of the verb "to increase" is to make something greater or larger. The "something" that is increased in 15 U.S.C.S. § 1681a(k)(1)(B)(i) is the "charge for any insurance." The plain and common meaning of the noun "charge" is the price demanded for something. Thus, the statute plainly means an insurer takes adverse action if the insurer makes greater (i.e., larger) the price demanded for insurance. **An insurer cannot "make greater" something that did not exist previously.** The statutory definition of adverse action, therefore, clearly anticipates an insurer must have made an **initial** charge or demand for payment **before the insurer can increase that charge**. In other words, an insurer cannot increase the charge for insurance unless the insurer previously set and demanded payment of the premium for that insured's insurance coverage at a lower price.

#### War powers authority is derived from congressional statute - restrictions are increased via statutory or judicial prohibitions on the source.

**Bradley, 10** - \* Richard A. Horvitz Professor of Law and Professor of Public Policy Studies, Duke Law School (Curtis, “CLEAR STATEMENT RULES AND EXECUTIVE WAR POWERS” <http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2730&context=faculty_scholarship>)

The scope of the President’s independent war powers is notoriously unclear, and courts are understandably reluctant to issue constitutional rulings that might deprive the federal government as a whole of the flexibility needed to respond to crises. As a result, courts often look for signs that Congress has either supported or opposed the President’s actions and rest their decisions on statutory grounds. This is essentially the approach outlined by Justice Jackson in his concurrence in Youngstown.1

For the most part, the Supreme Court has also followed this approach in deciding executive power issues relating to the war on terror. In Hamdi v. Rumsfeld, for example, Justice O’Connor based her plurality decision, which allowed for military detention of a U.S. citizen captured in Afghanistan, on Congress’s September 18, 2001, Authorization for Use of Military Force (AUMF).2 Similarly, in Hamdan v. Rumsfeld, the Court grounded its disallowance of the Bush Administration’s military commission system on what it found to be congressionally imposed restrictions.3

The Court’s decision in Boumediene v. Bush4 might seem an aberration in this regard, but it is not. Although the Court in Boumediene did rely on the Constitution in holding that the detainees at Guantanamo have a right to seek habeas corpus re‐ view in U.S. courts, it did not impose any specific restrictions on the executive’s detention, treatment, or trial of the detainees.5 In other words, Boumediene was more about preserving a role for the courts than about prohibiting the executive from exercising statutorily conferred authority.

#### Voting issue for limits and ground---they explode mechanisms that are not grounded in the status quo literature base which makes it not predictable---doubles our research burden makes specific strategy impossible.

#### Pleas for reasonability just warrant precision – only check on bi-directionality and Commander-in-Chief affs

Colby P. Horowitz 2013 “CREATING A MORE MEANINGFUL DETENTION STATUTE: LESSONS LEARNED FROM HEDGES V. OBAMA,” FORDHAM L.R. Vol. 81, http://fordhamlawreview.org/assets/pdfs/Vol\_81/Horowitz\_April.pdf

Thus, there at least two ways to interpret section 1021 under Justice Jackson’s framework. The government believes that section 1021 places the executive firmly in Zone 1. It has argued on appeal in Hedges that section 1021 is “an essentially verbatim affirmation by Congress of the Executive Branch’s interpretation of the AUMF.”335 This is supported by the government’s 2009 brief to the D.C. District Court, which is almost identical to the description of detention authority in section 1021.336 If section 1021 places the President in Zone 1, he has clear statutory authorization and does not need to rely on his general Commander-in-Chief powers (which courts view more narrowly).337 Additionally, in Zone 1, any ambiguities or vague terms in the statute might actually expand the President’s authority.338 338. See Chesney, supra note 33, at 792–93 (explaining that some observers view ambiguities in detention statutes as constituting “an implied delegation of authority to the executive to provide whatever further criteria may be required”).

#### They’re independently not offensive cyber operations---Offensive operations must attempt to coerce, harm or degrade a rival---explodes host of defensive and information operations that kill predictability.

Belk and Noyes 12

[Robert and Matthew, Robert is, studying international and global affairs at the Harvard Kennedy School.. Following graduation, he is scheduled to report to the Naval Operations staff in the Pentagon to develop and execute Navy network and cybersecurity policy, Matthew studies international security policy and is a senior associate with the cybersecurity practice at Good Harbor Consulting.. He has a degree in Computer Science and Applied Computational Mathematics from the University of Washington. “On the Use of Offensive Cyber Capabilities A Policy Analysis on Offensive US Cyber Policy”, <http://belfercenter.ksg.harvard.edu/files/cybersecurity-pae-belk-noyes.pdf>, Accessed 9-1-13]jap-lkm

The objective of an operation can be offensive, defensive, or informational in nature. Offensive objectives are those seeking to coerce rival action, impose harm, or degrade rival capabilities. Defensive objectives are those seeking to secure one’s own systems, and preserve freedom of operation. Informational objectives seek either to access or to expose information that is not generally, or publically, available. There exists some overlap between these three categories. For example, one may degrade rival capabilities as part of a counter-attack, giving an operation both an offensive and defensive characteristic. However, these categories are still useful for characterizing external cyber operations based on the nature of the objectives sought.

## 1NC

#### The President of the United States should issue an Executive Order committing the executive branch to Solicitor General Representation and advance consultation with the Office of Legal Counsel over decisions regarding a ban from enacting offensive cyber operations on civilians and civilian infrastructure. The Department of Justice officials involved should counsel against offensive cyber operations on civilians and civilian infrastructure. The Executive Order should also require written publication of Office of Legal Counsel opinions.

#### Executive pre-commitment to DOJ advice solves the aff- avoids ptx and flex

Pillard 5 JD from Harvard, Faculty Director of Supreme Court Institute at Georgetown University Law Center, former Deputy Assistant Attorney General in the DOJ, February, Cornelia T., Michigan Law Review, 103.4, “The Unfulfilled Promise of the Constitution in Executive Hands”, 103 Mich. L. Rev. 676-758, <http://scholarship.law.georgetown.edu/facpub/189/>

V. ENABLING EXECUTIVE CONSTITUTIONALISM¶ The courts indisputably do not and cannot fully assure our enjoyment of our constitutional rights, and it is equally clear that the federal executive has an independent constitutional duty to fulfill the Constitution's promise. Executive constitutionalism seems ripe with promise. Yet, it is striking how limited and court-centered the executive's normative and institutional approaches to constitutional questions remain.¶ One conceivable way to avoid the pitfalls of court-centric executive lawyering on one hand and constitutional decisions warped by political expedience on the other would be to make the Solicitor General and Office of Legal Counsel - or perhaps the entire Department of Justice - as structurally independent as an independent counsel or independent agency.207 Making the SG and OLC independent in order to insulate them from politics presumably would alleviate the "majoritarian difficulty" resulting from their service to elected clients. Promoting fuller independence in that sense does not, however, appear to be clearly normatively attractive, constitutionally permissible, nor particularly feasible. In all the criticism of our current constitutionalism, there is little call for an SG or OLC that would act, in effect, as a fully insulated and jurisprudentially autonomous constitutional court within the executive branch, operating with even less transparency and accountability than the Supreme Court. Moreover, as a practical matter it would be complex and problematic to increase the independence of the SG and OLC. The federal government faces Article II obstacles to formally insulating executive lawyers from politics and institutional pressures, and the president and his administration likely would be less amenable to guidance from such unaccountable lawyers.208¶ The challenge, rather, is to draw forth from the executive a constitutional consciousness and practice that helps the government actively to seek to fulfill the commitments of the Constitution and its Bill of Rights, interpreted by the executive as guiding principles for government. Adjustments to executive branch constitutional process and culture should be favored if they encourage the executive to use its experience and capacities to fulfill its distinctive role in effectuating constitutional guarantees. There is transformative potential in measures that break ingrained executive branch habits of looking to the Constitution only as it is mediated through the courts, and of reflexively seeking, where there is no clear doctrinal answer, to minimize constitutional constraint. It is difficult fully to imagine what kinds of changes would best prompt executive lawyers and officials to pick up constitutional analysis where the courts leave off, and to rely on the Constitution as an affirmative, guiding mandate for government action; what follows are not worked-out proposals, but are meant to be merely suggestive.¶ A. Correcting the Bias Against Constitutional Constraint¶ As we have seen, the SG's and OLC's default interpretive approach to individual rights and other forms of constitutional constraints on government is to follow what clear judicial precedents there are and, where precedents are not squarely to the contrary, to favor interpretations that minimize constitutional rights or other constitutional obligations on federal actors. Those court-centered and narrowly self-serving executive traditions produce a systematic skew against individual rights.¶ 1. Encourage Express Presidential Articulation of Commitment to Constitutional Rights¶ To the extent that a president articulates his own rights-protective constitutional vision with any specificity, he ameliorates the tension his constitutional lawyers otherwise face between advancing individual rights and serving their boss's presumed interest in maximum governing flexibility. Case or controversy requirements and restrictions against courts issuing advisory opinions do not, of course, apply to the executive's internal constitutional decisionmaking, and presidents can better serve individual rights to the extent that they expressly stake out their constitutional commitments in general and in advance of any concrete controversy."° When the president takes a stand for advancing abortion rights, property rights, disability rights, "charitable choice," a right to bear arms, or full remediation of race and sex discrimination, he signals to his lawyers that they should, in those areas, set aside their default bias in favor of preserving executive prerogative, even if it requires extra executive effort or restraint to do so.¶ If presented in a concrete setting with a choice between interpreting and applying the Constitution in fully rights-protective ways or sparing themselves the effort where Supreme Court precedent can be read not to require it, government officials typically default to the latter course without considering whether they might thereby be giving short shrift to a constitutional duty. A president's stated commitment to protection of particular rights, however, flips the default position with respect to those rights, acting as a spur to executive-branch lawyers and other personnel to work to give effect to constitutional rights even where, for a range of institutional reasons, the courts would not. A president is thus uniquely situated to facilitate full executive-branch constitutional compliance by precommitting himself to a rights-protective constitutional vision, and thereby making clear that respect for constitutional rights is part of the executive's interest, not counter to it.

## 1NC

#### Text: The President of the United States should issue a National Security Directive requiring the Department of Defense include in its Quadrennial Defense Review a recommendation to ban the President from enacting offensive cyber operations on civilians and civilian infrastructure. The President should not de-classify information regarding this National Security Directive.

#### QDR solves- reduces war powers

Parsons, National Defense Magazine Staff Writer, 2013,

(Dan, "Analyst: 2014 Defense Review Offers Opportunity for Real Reform", National Defense Magazine, 6-17, PAS) [www.nationaldefensemagazine.org/blog/lists/posts/post.aspx?ID=1182](http://www.nationaldefensemagazine.org/blog/lists/posts/post.aspx?ID=1182) 9-2-13

Instead of shoehorning its current force structure within a confined budget, the U.S. military should decide what it wants to be able to accomplish in the future and then design an affordable force to achieve those goals, a new study on the upcoming Quadrennial Defense Review contends. ¶ ¶ “We have a very capable force today. But the QDR is supposed to look out into the future, 20 years in the future and detect trends in the threats, trends in technology and where we should put our resources to be prepared for those future threats.,” Mark Gunzinger, author of “Shaping America’s Military: Toward a New Force Planning Construct, said June 13 during a presentation of the report. ¶ ¶ “We need to decide what capabilities we need for the future, before we decide what cuts we’re going to make today,” added Gunzinger, a senior fellow at the Center for Strategic and Budgetary Assessments, the Washington, D.C.-based think tank that published the report. ¶ ¶ Gunzinger’s concern is that the QDR that is scheduled to be published in 2014 will simply cut the current military down to a size that is affordable based on the current constrained fiscal environment. Mandated by law, next year’s QDR is the first in 11 years that will be drafted without a seemingly endless pot of money to fund its objectives. In fact, this and the next QDR fall squarely into a timeframe when Pentagon officials can count on shrinking budgets.¶ ¶ “The QDR could become another budget-dominated drill, which could lead the U.S. military to cut force structure, personnel and programs resulting in a force structure that is a smaller version of what we have today — a force structure that is, frankly, best prepared for fading threats,” Gunzinger said. “You should invest in the future first, before you balance the budget.”¶

## 1NC

#### Presidential war powers high

Posner 13 President Ruthless, Eric Posner, professor at the University of Chicago Law School, May 23, 2013, http://www.slate.com/articles/news\_and\_politics/view\_from\_chicago/2013/05/obama\_s\_speech\_he\_s\_just\_like\_bush\_in\_pushing\_the\_limits\_of\_executive\_power.html

In his speech today about the future of American counterterrorism operations, President Obama said that he will order drone strikes less frequently and redouble efforts to transfer some detainees out of Guantánamo. He suggested a more focused approach to terrorist threats in light of the diminished capacity of al-Qaida. Yet he also maintained the administration’s long-standing legal approach. The speech thus may well confirm the view among Obama’s civil libertarian critics that he is the most lawless executive since, um, George Bush. They are right to see the continuity from one president to the next, but they are wrong to believe that Obama has violated the law.

#### Congressional restrictions undermine the executive- tanks heg

Yoo 6 Yoo, John, an American attorney, law professor, and author. He served as a political appointee, the Deputy Assistant U.S. Attorney General in the Office of Legal Counsel, Department of Justice (OLC), during the George W. Bush administration, "Exercising wartime powers: the need for a strong executive." Harvard International Review 28.1 (2006): 22+. Opposing Viewpoints In Context.

The Iraq is beginning to look like a rerun of the Vietnam War, and not just because critics are crying out that the United States has again fallen into a quagmire. War opponents argue that a wartime president has overstepped his constitutional bounds and that if Congress' constitutional role in deciding on war had been respected, the United States could have avoided trouble or at least have entered the war with broader popular support. According to Democratic Senator Edward Kennedy, the White House is improperly "abusing power, is excusing and authorizing torture, and is spying on American citizens." The terrorists would never have been harshly interrogated and intelligence surveillance never domestically expanded if only President George W. Bush had looked to Congress.¶ These war critics misread the Constitution's allocation of warmaking powers between the executive and legislative branches. Their interpretation is weakest where their case should be its strongest: who gets to decide whether to start a war. For much of the history of the nation, presidents and congresses have understood that the executive branch's constitutional authority includes the power to begin military hostilities abroad.¶ Energy in the Executive¶ During the last two centuries, neither the president nor Congress has ever acted under the belief that the Constitution requires a declaration of war before engaging in military hostilities abroad. Although the United States has used force abroad more than 100 times, it has declared war only five times: the War of 1812, the Mexican-American and Spanish-American wars, and World War I and II. Without declarations of war or any other congressional authorization, presidents have sent troops to oppose the Russian Revolution, intervene in Mexico, fight Chinese Communists in Korea, remove Manuel Noriega from power in Panama, and prevent human rights disasters in the Balkans. Other conflicts, such as both Persian Gulf Wars, received "authorization" from Congress but not declarations of war.¶ Critics of these conflicts want to upend long practice by appealing to an "original understanding" of the Constitution. But the text and structure of the Constitution, as well as its application over the last two centuries, confirm that the president can begin military hostilities without the approval of Congress. The Constitution does not establish a strict warmaking process because the Framers understood that war would require the speed, decisiveness, and secrecy that only the presidency could bring. "Energy in the executive," Alexander Hamilton argued in the Federalist Papers, "... is essential to the protection of the community against foreign attacks." He continued, "the direction of war most peculiarly demands those qualities which distinguish the exercise of power by a single hand."¶ Rather than imposing a fixed, step-by-step method for going to war, the Constitution allows the executive and legislative branches substantial flexibility in shaping the decision-making process for engaging in military hostilities. Given the increasing ability of rogue states to procure weapons of mass destruction (WMDs) and the rise of international terrorism, maintaining this flexibility is critical to preserving US national security.

#### Heg solves extinction

Brooks et al 13 Lean Forward: In Defense of American Engagement, Foreign Affairs, January 2013, Stephen G. Brooks, Associate Professor of Government at Dartmouth, G. John Ikenberry, Albert G. Milbank Professor of Politics and International Affairs at Princeton University, and William C. Wohlforth, Daniel Webster Professor in the Department of Government at Dartmouth, <http://mcfr.wildapricot.org/Resources/Documents/2013-05> 20%20Brooks%20Ikenberry%20FA%20Stay%20Engaged%201301.pdf

Since the end of World War II, the United States has pursued a single grand strategy: deep engagement. In an effort to protect its security and prosperity, the country has promoted a liberal economic order and established close defense ties with partners in Europe, East Asia, and the Middle East. Its military bases cover the map, its ships patrol transit routes across the globe, and tens of thousands of its troops stand guard in allied countries such as Germany, Japan, and South Korea.¶ The details of U.S. foreign policy have differed from administration to administration, including the emphasis placed on democracy promotion and humanitarian goals, but for over 60 years, every president has agreed on the fundamental decision to remain deeply engaged in the world, even as the rationale for that strategy has shifted. During the Cold War, the United States' security commitments to Europe, East Asia, and the Middle East served primarily to prevent Soviet encroachment into the world's wealthiest and most resource-rich regions. Since the fall of the Soviet Union, the aim has become to make these same regions more secure, and thus less threatening to the United States, and to use these security partnerships to foster the cooperation necessary for a stable and open international order.¶ Now, more than ever, Washington might be tempted to abandon this grand strategy and pull back from the world. The rise of China is chipping away at the United States' preponderance of power, a budget crisis has put defense spending on the chopping block, and two long wars have left the U.S. military and public exhausted. Indeed, even as most politicians continue to assert their commitment to global leadership, a very different view has taken hold among scholars of international relations over the past decade: that the United States should minimize its overseas military presence, shed its security ties, and give up its efforts to lead the liberal international order.¶ Proponents of retrenchment argue that a globally engaged grand strategy wastes money by subsidizing the defense of well-off allies and generates resentment among foreign populations and governments. A more modest posture, they contend, would put an end to allies' free-riding and defuse anti-American sentiment. Even if allies did not take over every mission the United States now performs, most of these roles have nothing to do with U.S. security and only risk entrapping the United States in unnecessary wars. In short, those in this camp maintain that pulling back would not only save blood and treasure but also make the United States more secure.¶ If Washington got out of East Asia, Japan and South Korea would likely expand their military capabilities and go nuclear.¶ They are wrong. In making their case, advocates of retrenchment overstate the costs of the current grand strategy and understate its benefits. In fact, the budgetary savings of lowering the United States' international profile are debatable, and there is little evidence to suggest that an internationally engaged America provokes other countries to balance against it, becomes overextended, or gets dragged into unnecessary wars.¶ The benefits of deep engagement, on the other hand, are legion. U.S. security commitments reduce competition in key regions and act as a check against potential rivals. They help maintain an open world economy and give Washington leverage in economic negotiations. And they make it easier for the United States to secure cooperation for combating a wide range of global threats. Were the United States to cede its global leadership role, it would forgo these proven upsides while exposing itself to the unprecedented downsides of a world in which the country was less secure, prosperous, and influential.¶ AN AFFORDABLE STRATEGY¶ Many advocates of retrenchment consider the United States' assertive global posture simply too expensive. The international relations scholar Christopher Layne, for example, has warned of the country's "ballooning budget deficits" and argued that "its strategic commitments exceed the resources available to support them." Calculating the savings of switching grand strategies, however, is not so simple, because it depends on the expenditures the current strategy demands and the amount required for its replacement -- numbers that are hard to pin down.¶ If the United States revoked all its security guarantees, brought home all its troops, shrank every branch of the military, and slashed its nuclear arsenal, it would save around $900 billion over ten years, according to Benjamin Friedman and Justin Logan of the Cato Institute. But few advocates of retrenchment endorse such a radical reduction; instead, most call for "restraint," an "offshore balancing" strategy, or an "over the horizon" military posture. The savings these approaches would yield are less clear, since they depend on which security commitments Washington would abandon outright and how much it would cost to keep the remaining ones. If retrenchment simply meant shipping foreign-based U.S. forces back to the United States, then the savings would be modest at best, since the countries hosting U.S. forces usually cover a large portion of the basing costs. And if it meant maintaining a major expeditionary capacity, then any savings would again be small, since the Pentagon would still have to pay for the expensive weaponry and equipment required for projecting power abroad.¶ The other side of the cost equation, the price of continued engagement, is also in flux. Although the fat defense budgets of the past decade make an easy target for advocates of retrenchment, such high levels of spending aren't needed to maintain an engaged global posture. Spending skyrocketed after 9/11, but it has already begun to fall back to earth as the United States winds down its two costly wars and trims its base level of nonwar spending. As of the fall of 2012, the Defense Department was planning for cuts of just under $500 billion over the next five years, which it maintains will not compromise national security. These reductions would lower military¶ spending to a little less than three percent of GDP by 2017, from its current level of 4.5 percent. The Pentagon could save even more with no ill effects by reforming its procurement practices and compensation policies.¶ Even without major budget cuts, however, the country can afford the costs of its ambitious grand strategy. The significant increases in military spending proposed by Mitt Romney, the Republican candidate, during the 2012 presidential campaign would still have kept military spending below its current share of GDP, since spending on the wars in Afghanistan and Iraq would still have gone down and Romney's proposed nonwar spending levels would not have kept pace with economic growth. Small wonder, then, that the case for pulling back rests more on the nonmonetary costs that the current strategy supposedly incurs.¶ UNBALANCED¶ One such alleged cost of the current grand strategy is that, in the words of the political scientist Barry Posen, it "prompts states to balance against U.S. power however they can." Yet there is no evidence that countries have banded together in anti-American alliances or tried to match the United States' military capacity on their own -- or that they will do so in the future.¶ Indeed, it's hard to see how the current grand strategy could generate true counterbalancing. Unlike past hegemons, the United States is geographically isolated, which means that it is far less threatening to other major states and that it faces no contiguous great-power rivals that could step up to the task of balancing against it. Moreover, any competitor would have a hard time matching the U.S. military. Not only is the United States so far ahead militarily in both quantitative and qualitative terms, but its security guarantees also give it the leverage to prevent allies from giving military technology to potential U.S. rivals. Because the United States dominates the high-end defense industry, it can trade access to its defense market for allies' agreement not to transfer key military technologies to its competitors. The embargo that the United States has convinced the EU to maintain on military sales to China since 1989 is a case in point.¶ The country's globe-spanning posture is the devil we know, and a world with a disengaged America is the devil we don't know.¶ If U.S. global leadership were prompting balancing, then one would expect actual examples of pushback -- especially during the administration of George W. Bush, who pursued a foreign policy that seemed particularly unilateral. Yet since the Soviet Union collapsed, no major powers have tried to balance against the United States by seeking to match its military might or by assembling a formidable alliance; the prospect is simply too daunting. Instead, they have resorted to what scholars call "soft balancing," using international institutions and norms to constrain Washington. Setting aside the fact that soft balancing is a slippery concept and difficult to distinguish from everyday diplomatic competition, it is wrong to say that the practice only harms the United States. Arguably, as the global leader, the United States benefits from employing soft- balancing-style leverage more than any other country. After all, today's rules and institutions came about under its auspices and largely reflect its interests, and so they are in fact tailor-made for soft balancing by the United States itself. In 2011, for example, Washington coordinated¶ action with several Southeast Asian states to oppose Beijing's claims in the South China Sea by pointing to established international law and norms.¶ Another argument for retrenchment holds that the United States will fall prey to the same fate as past hegemons and accelerate its own decline. In order to keep its ambitious strategy in place, the logic goes, the country will have to divert resources away from more productive purposes -- infrastructure, education, scientific research, and so on -- that are necessary to keep its economy competitive. Allies, meanwhile, can get away with lower military expenditures and grow faster than they otherwise would.¶ The historical evidence for this phenomenon is thin; for the most part, past superpowers lost their leadership not because they pursued hegemony but because other major powers balanced against them -- a prospect that is not in the cards today. (If anything, leading states can use their position to stave off their decline.) A bigger problem with the warnings against "imperial overstretch" is that there is no reason to believe that the pursuit of global leadership saps economic growth. Instead, most studies by economists find no clear relationship between military expenditures and economic decline.¶ To be sure, if the United States were a dramatic outlier and spent around a quarter of its GDP on defense, as the Soviet Union did in its last decades, its growth and competitiveness would suffer. But in 2012, even as it fought a war in Afghanistan and conducted counterterrorism operations around the globe, Washington spent just 4.5 percent of GDP on defense -- a relatively small fraction, historically speaking. (From 1950 to 1990, that figure averaged 7.6 percent.) Recent economic difficulties might prompt Washington to reevaluate its defense budgets and international commitments, but that does not mean that those policies caused the downturn. And any money freed up from dropping global commitments would not necessarily be spent in ways that would help the U.S. economy.¶ Likewise, U.S. allies' economic growth rates have nothing to do with any security subsidies they receive from Washington. The contention that lower military expenditures facilitated the rise of Japan, West Germany, and other countries dependent on U.S. defense guarantees may have seemed plausible during the last bout of declinist anxiety, in the 1980s. But these states eventually stopped climbing up the global economic ranks as their per capita wealth approached U.S. levels -- just as standard models of economic growth would predict. Over the past 20 years, the United States has maintained its lead in per capita GDP over its European allies and Japan, even as those countries' defense efforts have fallen further behind. Their failure to modernize their militaries has only served to entrench the United States' dominance.¶ LED NOT INTO TEMPTATION¶ The costs of U.S. foreign policy that matter most, of course, are human lives, and critics of an expansive grand strategy worry that the United States might get dragged into unnecessary wars. Securing smaller allies, they argue, emboldens those states to take risks they would not otherwise accept, pulling the superpower sponsor into costly conflicts -- a classic moral hazard problem. Concerned about the reputational costs of failing to honor the country's alliance commitments, U.S. leaders might go to war even when no national interests are at stake.¶ History shows, however, that great powers anticipate the danger of entrapment and structure their agreements to protect themselves from it. It is nearly impossible to find a clear case of a smaller power luring a reluctant great power into war. For decades, World War I served as the canonical example of entangling alliances supposedly drawing great powers into a fight, but an outpouring of new historical research has overturned the conventional wisdom, revealing that the war was more the result of a conscious decision on Germany's part to try to dominate Europe than a case of alliance entrapment.¶ If anything, alliances reduce the risk of getting pulled into a conflict. In East Asia, the regional security agreements that Washington struck after World War II were designed, in the words of the political scientist Victor Cha, to "constrain anticommunist allies in the region that might engage in aggressive behavior against adversaries that could entrap the United States in an unwanted larger war." The same logic is now at play in the U.S.-Taiwanese relationship. After cross-strait tensions flared in the 1990s and the first decade of this century, U.S. officials grew concerned that their ambiguous support for Taiwan might expose them to the risk of entrapment. So the Bush administration adjusted its policy, clarifying that its goal was to not only deter China from an unprovoked attack but also deter Taiwan from unilateral moves toward independence.¶ For many advocates of retrenchment, the problem is that the mere possession of globe-girdling military capabilities supposedly inflates policymakers' conception of the national interest, so much so that every foreign problem begins to look like America's to solve. Critics also argue that the country's military superiority causes it to seek total solutions to security problems, as in Afghanistan and Iraq, that could be dealt with in less costly ways. Only a country that possessed such awesome military power and faced no serious geopolitical rival would fail to be satisfied with partial fixes, such as containment, and instead embark on wild schemes of democracy building, the argument goes.¶ Furthermore, they contend, the United States' outsized military creates a sense of obligation to do something with it even when no U.S. interests are at stake. As Madeleine Albright, then the U.S. ambassador to the un, famously asked Colin Powell, then chairman of the Joint Chiefs of Staff, when debating intervention in Bosnia in 1993, "What's the point of having this superb military you're always talking about if we can't use it?"¶ If the U.S. military scrapped its forces and shuttered its bases, then the country would no doubt eliminate the risk of entering needless wars, having tied itself to the mast like Ulysses. But if it instead merely moved its forces over the horizon, as is more commonly proposed by advocates of retrenchment, whatever temptations there were to intervene would not disappear. The bigger problem with the idea that a forward posture distorts conceptions of the national interest, however, is that it rests on just one case: Iraq. That war is an outlier in terms of both its high costs (it accounts for some two-thirds of the casualties and budget costs of all U.S. wars since 1990) and the degree to which the United States shouldered them alone. In the Persian Gulf War and the interventions in Bosnia, Kosovo, Afghanistan, and Libya, U.S. allies bore more of the burden, controlling for the size of their economies and populations.¶ Besides, the Iraq war was not an inevitable consequence of pursuing the United States' existing grand strategy; many scholars and policymakers who prefer an engaged America strongly¶ opposed the war. Likewise, continuing the current grand strategy in no way condemns the United States to more wars like it. Consider how the country, after it lost in Vietnam, waged the rest of the Cold War with proxies and highly limited interventions. Iraq has generated a similar reluctance to undertake large expeditionary operations -- what the political scientist John Mueller has dubbed "the Iraq syndrome." Those contending that the United States' grand strategy ineluctably leads the country into temptation need to present much more evidence before their case can be convincing.¶ KEEPING THE PEACE¶ Of course, even if it is true that the costs of deep engagement fall far below what advocates of retrenchment claim, they would not be worth bearing unless they yielded greater benefits. In fact, they do. The most obvious benefit of the current strategy is that it reduces the risk of a dangerous conflict. The United States' security commitments deter states with aspirations to regional hegemony from contemplating expansion and dissuade U.S. partners from trying to solve security problems on their own in ways that would end up threatening other states.¶ Skeptics discount this benefit by arguing that U.S. security guarantees aren't necessary to prevent dangerous rivalries from erupting. They maintain that the high costs of territorial conquest and the many tools countries can use to signal their benign intentions are enough to prevent conflict. In other words, major powers could peacefully manage regional multipolarity without the American pacifier.¶ But that outlook is too sanguine. If Washington got out of East Asia, Japan and South Korea would likely expand their military capabilities and go nuclear, which could provoke a destabilizing reaction from China. It's worth noting that during the Cold War, both South Korea and Taiwan tried to obtain nuclear weapons; the only thing that stopped them was the United States, which used its security commitments to restrain their nuclear temptations. Similarly, were the United States to leave the Middle East, the countries currently backed by Washington -- notably, Israel, Egypt, and Saudi Arabia -- might act in ways that would intensify the region's security dilemmas.¶ There would even be reason to worry about Europe. Although it's hard to imagine the return of great-power military competition in a post-American Europe, it's not difficult to foresee governments there refusing to pay the budgetary costs of higher military outlays and the political costs of increasing EU defense cooperation. The result might be a continent incapable of securing itself from threats on its periphery, unable to join foreign interventions on which U.S. leaders might want European help, and vulnerable to the influence of outside rising powers.¶ Given how easily a U.S. withdrawal from key regions could lead to dangerous competition, advocates of retrenchment tend to put forth another argument: that such rivalries wouldn't actually hurt the United States. To be sure, few doubt that the United States could survive the return of conflict among powers in Asia or the Middle East -- but at what cost? Were states in one or both of these regions to start competing against one another, they would likely boost their military budgets, arm client states, and perhaps even start regional proxy wars, all of which should concern the United States, in part because its lead in military capabilities would narrow.¶ Greater regional insecurity could also produce cascades of nuclear proliferation as powers such as Egypt, Saudi Arabia, Japan, South Korea, and Taiwan built nuclear forces of their own. Those countries' regional competitors might then also seek nuclear arsenals. Although nuclear deterrence can promote stability between two states with the kinds of nuclear forces that the Soviet Union and the United States possessed, things get shakier when there are multiple nuclear rivals with less robust arsenals. As the number of nuclear powers increases, the probability of illicit transfers, irrational decisions, accidents, and unforeseen crises goes up.¶ The case for abandoning the United States' global role misses the underlying security logic of the current approach. By reassuring allies and actively managing regional relations, Washington dampens competition in the world's key areas, thereby preventing the emergence of a hothouse in which countries would grow new military capabilities. For proof that this strategy is working, one need look no further than the defense budgets of the current great powers: on average, since 1991 they have kept their military expenditures as a percentage of GDP to historic lows, and they have not attempted to match the United States' top-end military capabilities. Moreover, all of the world's most modern militaries are U.S. allies, and the United States' military lead over its potential rivals is by many measures growing.¶ On top of all this, the current grand strategy acts as a hedge against the emergence regional hegemons. Some supporters of retrenchment argue that the U.S. military should keep its forces over the horizon and pass the buck to local powers to do the dangerous work of counterbalancing rising regional powers. Washington, they contend, should deploy forces abroad only when a truly credible contender for regional hegemony arises, as in the cases of Germany and Japan during World War II and the Soviet Union during the Cold War. Yet there is already a potential contender for regional hegemony -- China -- and to balance it, the United States will need to maintain its key alliances in Asia and the military capacity to intervene there. The implication is that the United States should get out of Afghanistan and Iraq, reduce its military presence in Europe, and pivot to Asia. Yet that is exactly what the Obama administration is doing.¶ MILITARY DOMINANCE, ECONOMIC PREEMINENCE¶ Preoccupied with security issues, critics of the current grand strategy miss one of its most important benefits: sustaining an open global economy and a favorable place for the United States within it. To be sure, the sheer size of its output would guarantee the United States a major role in the global economy whatever grand strategy it adopted. Yet the country's military dominance undergirds its economic leadership. In addition to protecting the world economy from instability, its military commitments and naval superiority help secure the sea-lanes and other shipping corridors that allow trade to flow freely and cheaply. Were the United States to pull back from the world, the task of securing the global commons would get much harder. Washington would have less leverage with which it could convince countries to cooperate on economic matters and less access to the military bases throughout the world needed to keep the seas open.¶ A global role also lets the United States structure the world economy in ways that serve its particular economic interests. During the Cold War, Washington used its overseas security commitments to get allies to embrace the economic policies it preferred -- convincing West¶ Germany in the 1960s, for example, to take costly steps to support the U.S. dollar as a reserve currency. U.S. defense agreements work the same way today. For example, when negotiating the 2011 free-trade agreement with South Korea, U.S. officials took advantage of Seoul's desire to use the agreement as a means of tightening its security relations with Washington. As one diplomat explained to us privately, "We asked for changes in labor and environment clauses, in auto clauses, and the Koreans took it all." Why? Because they feared a failed agreement would be "a setback to the political and security relationship."¶ More broadly, the United States wields its security leverage to shape the overall structure of the global economy. Much of what the United States wants from the economic order is more of the same: for instance, it likes the current structure of the World Trade Organization and the International Monetary Fund and prefers that free trade continue. Washington wins when U.S. allies favor this status quo, and one reason they are inclined to support the existing system is because they value their military alliances. Japan, to name one example, has shown interest in the Trans-Pacific Partnership, the Obama administration's most important free-trade initiative in the region, less because its economic interests compel it to do so than because Prime Minister Yoshihiko Noda believes that his support will strengthen Japan's security ties with the United States.¶ The United States' geopolitical dominance also helps keep the U.S. dollar in place as the world's reserve currency, which confers enormous benefits on the country, such as a greater ability to borrow money. This is perhaps clearest with Europe: the EU's dependence on the United States for its security precludes the EU from having the kind of political leverage to support the euro that the United States has with the dollar. As with other aspects of the global economy, the United States does not provide its leadership for free: it extracts disproportionate gains. Shirking that responsibility would place those benefits at risk.¶ CREATING COOPERATION¶ What goes for the global economy goes for other forms of international cooperation. Here, too, American leadership benefits many countries but disproportionately helps the United States. In order to counter transnational threats, such as terrorism, piracy, organized crime, climate change, and pandemics, states have to work together and take collective action. But cooperation does not come about effortlessly, especially when national interests diverge. The United States' military efforts to promote stability and its broader leadership make it easier for Washington to launch joint initiatives and shape them in ways that reflect U.S. interests. After all, cooperation is hard to come by in regions where chaos reigns, and it flourishes where leaders can anticipate lasting stability.¶ U.S. alliances are about security first, but they also provide the political framework and channels of communication for cooperation on nonmilitary issues. NATO, for example, has spawned new institutions, such as the Atlantic Council, a think tank, that make it easier for Americans and Europeans to talk to one another and do business. Likewise, consultations with allies in East Asia spill over into other policy issues; for example, when American diplomats travel to Seoul to manage the military alliance, they also end up discussing the Trans-Pacific Partnership. Thanks¶ to conduits such as this, the United States can use bargaining chips in one issue area to make progress in others.¶ The benefits of these communication channels are especially pronounced when it comes to fighting the kinds of threats that require new forms of cooperation, such as terrorism and pandemics. With its alliance system in place, the United States is in a stronger position than it would otherwise be to advance cooperation and share burdens. For example, the intelligence- sharing network within NATO, which was originally designed to gather information on the Soviet Union, has been adapted to deal with terrorism. Similarly, after a tsunami in the Indian Ocean devastated surrounding countries in 2004, Washington had a much easier time orchestrating a fast humanitarian response with Australia, India, and Japan, since their militaries were already comfortable working with one another. The operation did wonders for the United States' image in the region.¶ The United States' global role also has the more direct effect of facilitating the bargains among governments that get cooperation going in the first place. As the scholar Joseph Nye has written, "The American military role in deterring threats to allies, or of assuring access to a crucial resource such as oil in the Persian Gulf, means that the provision of protective force can be used in bargaining situations. Sometimes the linkage may be direct; more often it is a factor not mentioned openly but present in the back of statesmen's minds."¶ THE DEVIL WE KNOW¶ Should America come home? For many prominent scholars of international relations, the answer is yes -- a view that seems even wiser in the wake of the disaster in Iraq and the Great Recession. Yet their arguments simply don't hold up. There is little evidence that the United States would save much money switching to a smaller global posture. Nor is the current strategy self- defeating: it has not provoked the formation of counterbalancing coalitions or caused the country to spend itself into economic decline. Nor will it condemn the United States to foolhardy wars in the future. What the strategy does do is help prevent the outbreak of conflict in the world's most important regions, keep the global economy humming, and make international cooperation easier. Charting a different course would threaten all these benefits.¶ This is not to say that the United States' current foreign policy can't be adapted to new circumstances and challenges. Washington does not need to retain every commitment at all costs, and there is nothing wrong with rejiggering its strategy in response to new opportunities or setbacks. That is what the Nixon administration did by winding down the Vietnam War and increasing the United States' reliance on regional partners to contain Soviet power, and it is what the Obama administration has been doing after the Iraq war by pivoting to Asia. These episodes of rebalancing belie the argument that a powerful and internationally engaged America cannot tailor its policies to a changing world.¶ A grand strategy of actively managing global security and promoting the liberal economic order has served the United States exceptionally well for the past six decades, and there is no reason to give it up now. The country's globe-spanning posture is the devil we know, and a world with a disengaged America is the devil we don't know. Were American leaders to choose retrenchment,¶ they would in essence be running a massive experiment to test how the world would work without an engaged and liberal leading power. The results could well be disastrous.

## 1NC

#### A. Uniqueness – Obama is using political capital to prevent Iran sanctions now AND deal is close

Weisman and Gordon, New York Times Staff Writer, 11-15, 2013,

(Jonathan and Michael R., "Obama asks for room to reach Iran deal; New sanctions, he says, would derail effort to freeze nuclear program", New York Times, PAS) Accessed on LexisNexis 11-15-13

The Obama administration is pressing senators to give it breathing room to reach an accord with Iran to freeze its nuclear programs, warning that a new round of sanctions could mean war instead of diplomacy.¶ But it is facing extreme skepticism from lawmakers in both parties who worry the administration is prepared to give the Iranian government too much for too little.¶ On Thursday, President Obama offered a vigorous defense of the diplomatic approach to Iran, during a news conference called to discuss a change in his health-care law. He asked for forbearance, saying that there was little to lose in pursuing a short-term deal. ''Let's see if this short-term Phase 1 deal can be completed to our satisfaction,'' he said.¶ In the worst case, he said, the West will have bought time and delayed any Iranian progress toward a nuclear weapon. Administration officials said they were in striking distance of an agreement that would halt much of Iran's nuclear program for six months.¶ ''We will have lost nothing if, at the end of the day, it turns out that they are not prepared to provide the international community the hard proof and assurances necessary for us to know that they're not pursuing a nuclear weapon,'' the president said.¶ Secretary of State John Kerry, briefing the Senate Banking, Housing and Urban Affairs Committee on Wednesday, made his case against the committee's moving forward with a proposal for new sanctions even as Western diplomats were talking about easing existing sanctions in exchange for concessions on Iran's nuclear program.¶ Moving too soon on new sanctions amounted to ''getting in the way of diplomacy,'' he said, suggesting that Congress could always act later.¶ ''Let's give them a few weeks, see if it works and we have all our options at our disposal,'' he said as he ducked into the closed-door meeting.¶ The briefing was part of an all-out effort by the administration both to tamp down congressional saber-rattling and to move diplomacy forward to reach the agreement that proved elusive last weekend in Geneva. Mr. Obama has made a flurry of calls to the leaders of Britain and France before the resumption of negotiations in Geneva on Nov. 21 and 22. On Tuesday night, he called Senator Harry Reid of Nevada, the majority leader, to discuss Iran, among other issues.¶ Vice President Joseph R. Biden Jr. met with the Democratic Congressional leadership and administration officials were to hold briefings on Thursday for House leaders and members of the Senate.¶ The finger pointing over how the talks failed to come to an agreement is continuing, with Iran's foreign minister, Mohammad Javad Zarif, on Wednesday laying the blame on the Western powers, saying they were divided.¶ Mohammad Ali Shabani, a political analyst with close ties to Mr. Zarif, said, ''It's the United States which should get their partners on board, not Iran. From the information that is available, what was on the table was an American proposal. It was France that ripped into it, not Iran.''¶ Mr. Kerry said Mr. Zarif and his team balked after having been faced with a unified proposal that went further than the Iranian leadership was prepared to go. Mr. Zarif fired back on Twitter, hinting that the Americans had failed to get their ally France behind their own proposal, allowing France to sabotage the deal.¶ Following Mr. Zarif's lead, Iranian politicians, clerics, commanders and state news media outlets have been criticizing France. Students are threatening to occupy the French Embassy in Tehran and politicians are calling for a boycott of French products - of which there are very few because of the Western economic sanctions.¶ While Mr. Zarif aimed most of his criticism at Paris, he may have done so, analysts said, to placate or undercut various domestic audiences, beginning with the millions who voted for President Hassan Rouhani and his moderate government - one that has promised to end the cold war with the West and relieve the economy of the sanctions imposed over the nuclear program.¶ But he also has to worry about hard-liners, many of whom think the talks are a fool's errand and have warned that Iran's opponents will try to trick or coerce it into a bad deal.¶ A report issued Thursday by the United Nations nuclear agency said that Iran had virtually halted a previously rapid expansion of its uranium enrichment capacity in the past three months, Reuters reported.¶ The quarterly report by the International Atomic Energy Agency also said that Iran's stockpile of higher-grade enriched uranium - closely watched by the West and Israel - had risen by about 5 percent, to about 435 pounds, since August.

#### B. The plan cost capital- restrictions force Obama to defend his policies

Kriner, Boston University Assistant Political Science Professor, 2010,

(Douglas, “After the Rubicon: Congress, Presidents, and the Politics of Waging War”, 12-1, Pg. 68, PAS) Accessed on Google Books 8-12-13

While congressional support leaves the president’s reserve of political capital intact, congressional criticism saps energy from other initiatives on the home front by forcing the president to expand energy and effort defending his international agenda. ¶ Political capital spent shoring up support for a president’s foreign policies is capital that is unavailable for his future policy initiatives. ¶ Moreover, any weakening in the president’s political clout may have immediate ramifications for his reelection prospects, as well as indirect consequences for congressional races.59 indeed, Democratic efforts to tie congressional Republican incumbents to President George W. Bush and his war policies paid immediate political dividends in the 2006 midterms, particularly in states, districts, and counties that had suffered the highest casualty rates in the Iraq War.60 ¶ In addition to boding ill for the president’s perceived political capital and reputation, such partisan losses in Congress only further imperil his programmatic agenda, both international and domestic. Scholars have long noted that President Lyndon Johnson’s dream of a Great Society also perished in the rice paddies of Vietnam. Lacking both the requisite funds in a war-depleted treasury and the political capital needed to sustain his legislative vision, Johnson gradually let his domestic goals slip away as he hunkered down in an effort first to win and then to end the Vietnam War. In the same way, many of President Bush’s highest second-term domestic priorities, such as Social Security and immigration reform, failed perhaps in large part because the administration had to expand so much energy and effort waging a rear-guard action against congressional critics of the war in Iraq.61 ¶

#### C. Political capital is key to prevent sanctions – shift from domestic policies now

Andrew Hammond 11/13 was formerly a special adviser in the government of former UK Prime Minister Tony Blair, and also a geopolitical analyst at Oxford Analytica. “Iranian diplomacy underscores Obama's search for legacy,” 11-13-13, <http://www.cnn.com/2013/11/13/opinion/iran-obama-legacy-hammond/> DOA: 11-14-13, y2k

Significant progress was reportedly made last weekend in Geneva toward a landmark nuclear agreement with Iran. And, as talks concluded on November 10, U.S. Secretary of John Kerry announced that negotiations will start again on November 20. Despite the concerns of regional U.S. allies like Israel and Saudi Arabia, and also a significant number of legislators in the U.S. Congress, it is clear that the Obama administration is pushing strongly for deal as part of its wider Middle Eastern strategy. Indeed, Kerry has now spent more time negotiating with counterpart Iranian officials than any other U.S. high-level engagement for perhaps three decades. The seriousness of negotiations was emphasized by the fact that, as well as Kerry and his Iranian counterpart Mohammad Javad Zarif, foreign ministers from Russia, the United Kingdom, Germany and France, and the Chinese deputy foreign minister, came together. If agreement can be reached, an interim deal (potentially setting the ground for a later comprehensive agreement) would reportedly see Iran's nuclear capacity capped for six months and opened up to U.N. inspections. In exchange, Iran would be given limited, sequenced relief from sanctions. Remaining disagreements reportedly include the status of the Arak heavy-water reactor, and production of highly enriched uranium -- both processes, that can potentially be used to produce nuclear weapons. A second problem to resolve is how to handle the existing Iranian stockpile of uranium that Iran enriched to 20%. IAEA signs cooperation deal with Tehran President Obama's second term troubles Progress in nuclear diplomacy with Iran, combined with continued uncertainty in Syria and Egypt, has refocused Washington's attention towards the Middle East in a manner unanticipated by Obama only a few months ago. In addition to Syria and Egypt, the administration has spent significant political capital resuming Israeli-Palestinian peace talks. The urgency of U.S. focus there reflects growing international conviction that, 20 years after the Oslo Process began, the "window of opportunity" for securing a two-state solution may be receding. Intensified U.S. focus on the Middle East has accentuated a shift, common to many recent re-elected presidents, of increased focus on foreign policy in second terms of office. In part, this reflects the fact that presidents often see foreign policy as key to the legacy they wish to build. For instance, after the 2001 terrorist attacks, George W. Bush sought to spread his freedom agenda across the Middle East. Bill Clinton also devoted significant time to trying to secure a comprehensive Israeli-Palestinian peace deal. As important as an Iran nuclear agreement might prove to be, the Middle East is one of only two regions in which Obama is looking for legacy. Since he was elected in 2008, Asia in general, and China in particular, has assumed greater importance in U.S. policy. To this end, Obama is seeking to continue the so-called pivot towards Asia-Pacific through landmark initiatives like the Trans-Pacific Partnership. Key threats, however, remain on the horizon to securing this re-orientation. These include a dramatic, sustained escalation of tension in the Middle East (perhaps in Syria or Egypt); and/or the remaining possibility of further terrorist attacks on the U.S. homeland. As well as legacy-building, the likelihood of Obama concentrating more on foreign policy also reflects domestic U.S. politics. Particularly the intense polarization and gridlock of Washington. Since re-election, Obama has achieved little domestic policy success. His gun control bill was defeated, immigration reform faces significant opposition in the Republican-controlled House of Representatives, and the prospect of a long-term federal budgetary "grand bargain" with Congress looks unlikely. Moreover, implementation of his landmark healthcare initiative has been botched. Many re-elected presidents in the post-war era have, like Obama, found it difficult to acquire domestic policy momentum. In part, this is because the party of re-elected presidents, as with the Democrats now, often hold a weaker position in Congress. Thus Dwight Eisenhower in 1956, Richard Nixon in 1972, and Bill Clinton in 1996 were all re-elected alongside Congresses where both the House and Senate were controlled by their partisan opponents. Another factor encouraging foreign policy focus in second terms is the fact that re-elected presidents have often been impacted by domestic scandals in recent decades. Thus, Watergate ended the Nixon administration in 1974, Iran-Contra badly damaged the Reagan White House, and the Lewinsky scandal led to Clinton being impeached. Since Obama's re-election, a series of problems have hit the administration. These include revelations that the Internal Revenue Service targeted some conservative groups for special scrutiny; and the Department of Justice's secret subpoenaing of private phone records of several Associated Press reporters and editors in the wake of a terrorist plot leak. Even if Obama escapes further significant problems, he will not be able to avoid the "lame-duck" factor. That is, as a president cannot seek more than two terms, political focus will refocus elsewhere, particularly after the November 2014 congressional ballots when the 2016 presidential election campaign kicks into gear. Taken overall, Iranian diplomatic progress and wider recent events in the Middle East are therefore likely to accentuate the incentives for Obama to place increasing emphasis on foreign policy -- which Congress has less latitude over -- in his remaining period of office. And, this shift is only likely to be reinforced if, as anticipated, the U.S. economic recovery continues to build up steam in 2014.

#### D. Sanction increases causes Iranian proliferation

Reuters 11/14 Kerry: Failing to reach nuclear deal will push Iran to obtain nuclear weapons, JPOST.COM STAFF, 11/14/2013, http://www.jpost.com/Iranian-Threat/News/Kerry-Failing-to-reach-nuclear-deal-will-push-Iran-to-obtain-nuclear-weapons-331791

US secretary of state makes case against imposing additional sanctions on Tehran, saying such a move would signal to Iran the US isn't willing to negotiate in good faith; says no distance between US, Israel on issue. Imposing additional sanctions on Iran would signal to Tehran that the United States is not willing to negotiate a peaceful resolution to the nuclear dispute, and drive hardliners in the country to push for obtaining of nuclear weapons, US Secretary of State John Kerry said in an interview with MSNBC on Thursday. Kerry and Vice President Joe Biden met with senators on Capitol Hill on Wednesday in an attempt to convince them to hold off on increasing sanctions on the Islamic Republic, arguing that such a move would be viewed by Iran as a bad faith step from the US. "You have to do something in order to make it worthwhile for them to say, 'Yes, we’re going to lock our program where it is today and actually roll it back,'" he said. He stressed that 95 percent, the core of the sanctions regime, would remain in place, and only a "tiny portion" of sanctions would be eased. "Iran was bringing in a $110-120 billion a year in income from its oil revenues, banking and so forth. That has been knocked down to $40-45 billion and that money is frozen in banks around the world. All we're talking about doing is releasing a tiny portion of that," he said. He warned that failure to reach a deal would result in Tehran continuing its nuclear program, "and then we're locked in a standoff for the next how-many number of years that becomes more dangerous for Israel and our other allies in the region, and may even push other countries to nuclearize and could result in the requirement that we'd have to - rather than have to negotiate a peaceful resolution of this - take military action in order to secure our goals." Kerry said that he has had several phone conversations with Prime Minister Binyamin Netanyahu on the issue over the past week, including one of Thursday. "I respect completely [Netanyahu's] deep concerns, as a prime minister should have about the existential nature of this threat to Israel," he said, noting that the two countries agree about the goal of the talks - stopping Iran from obtaining nuclear weapons - but not on the way to achieve that goal. "We believe that you need to take the first step and that you will not get Iran to simply surrender and believe you're dealing in good faith if after two years of negotiating you don't follow through with what's on the table. But Mr. Netanyahu believes that you can increase the sanctions, put the pressure on even further, and that somehow this is going to force them to do what they haven't been willing to do any time previously," the secretary of state said. Despite that, he stressed that there is no distance between Israel and the United States. "I believe [this deal] is the best first step that will actually make Israel safer. It will extend the break out time. If we don't get that first step, not only will that break out time shrink, but Iran may interpret the congressional reaction to increase sanctions as bad faith on our part and unwillingness to negotiate and may drive the hardliners even more to a commitment that they have to have the weapons," he said.

#### Iranian prolif causes regional nuclear conflict

Edelman et al 11 The Dangers of a Nuclear Iran, The Limits of Containment, Eric S. Edelman, Andrew F. Krepinevich Jr, and Evan Braden Montgomery JANUARY/FEBRUARY 2011, ERIC S. EDELMAN is a Distinguished Fellow at the Center for Strategic and Budgetary Assessments; he was U.S. Undersecretary of Defense for Policy in 2005-9. ANDREW F. KREPINEVICH is President of the Center for Strategic and Budgetary Assessments. EVAN BRADEN MONTGOMERY is a Research Fellow at the Center for Strategic and Budgetary Assessments, http://www.foreignaffairs.com/articles/67162/eric-s-edelman-andrew-f-krepinevich-jr-and-evan-braden-montgomer/the-dangers-of-a-nuclear-iran

Yet this view is far too sanguine. Above all, it rests on the questionable assumptions that possessing nuclear weapons induces caution and restraint, that other nations in the Middle East would balance against Iran rather than bandwagon with it, that a nuclear-armed Iran would respect new redlines even though a conventionally armed Iran has failed to comply with similar warnings, and that further proliferation in the region could be avoided. It seems more likely that Iran would become increasingly aggressive once it acquired a nuclear capability, that the United States' allies in the Middle East would feel greatly threatened and so would increasingly accommodate Tehran, that the United States' ability to promote and defend its interests in the region would be diminished, and that further nuclear proliferation, with all the dangers that entails, would occur. The greatest concern in the near term would be that an unstable Iranian-Israeli nuclear contest could emerge, with a significant risk that either side would launch a first strike on the other despite the enormous risks and costs involved. Over the longer term, Saudi Arabia and other states in the Middle East might pursue their own nuclear capabilities, raising the possibility of a highly unstable regional nuclear arms race.

## China

#### Ip theft ruins relations

Lewis 7/9/2013 [James A. Director and Senior Fellow, Technology and Public Policy Program Center for Strategic and International Studies (CSIS) Statement before the House Energy and Commerce Committee, Subcommittee on Oversight and Investigations¶ “CYBER ESPIONAGE AND THE THEFT OF U.S. INTELLECTUAL PROPERTY AND¶ TECHNOLOGY”

Chinese leaders realize that they face conflicting domestic goals as well as a serious bilateral problem. Economic espionage provides a technology boost, but puts bilateral relations with the U.S. at risk and hampers China’s ability to create indigenous innovation. So far, China has been unwilling to give up its long-running national effort to illicitly acquire technology from Western companies, but action and engagement on this issue by the U.S. and other nations could change calculations of cost and benefit by Chinese leaders.¶ It is not useful to think of this issue in terms of confrontation, punishment, or conflict. We need a long-term diplomatic strategy linked to our larger goals for Asia and the world. Frustration with the lack of progress in stemming China’s activities has led to a variety of bellicose suggestions, few of which make any sense and some of which could actually harm the United States. It is not in our interest to start a military conflict with China, nor is it in our interest to crash the Chinese economy – something that would unleash another global recession. Similarly, a trade war could do more damage to the American economy than cyber-espionage. Hacking back has little real effect, holds real risk of unintended damage, and could start an inadvertent conflict with China, as the Chinese believe that the U.S. government endorses any private action by Americans. Hacking back runs contrary to U.S. international commitments and to the larger U.S. strategy for making cyberspace more secure.

#### Not sufficient---they still allow military targets which still pisses off China.

#### OCO Development Can Check China

Junio 13 Tim Junio, Cybersecurity Fellow At Stanford Center For International Security And Cooperation, More Shots Fired on the Cyber Front: Key Takeaways From Operation Troy, Huffinton Post, 7/11/13, http://www.huffingtonpost.com/tim-junio/operation-troy-cybersecurity\_b\_3582308.html

How can the U.S. and its allies cope with these threats? An answer is to incorporate law enforcement responses and the efforts of private companies into a whole-of-government approach that stresses reducing adversaries' incentives to conduct attacks. A diplomatic priority should be to link cyber conflict to other issues during negotiations. Getting North Korea (and China and Russia and Iran) to stop highly lucrative cyber operations just by asking nicely has no hope of success.¶ Military and intelligence agencies can help that bargaining process by aggressively developing new capabilities, and by pursuing new human intelligence leads to best exploit the bureaucratic errors detailed in the Mandiant and McAfee reports.

#### China’s cyber threat is exaggerated

Hjortdal 11 [Magnus is a researcher associated with CHINA-SEC, Centre for Military Studies at the University of Copenhagen. He holds an M.Sc. in Political Science from the University of Copenhagen and is owner of MH International Relations, which advises private and public institutions. Former Research Fellow at the Royal Danish Defense College, where he drew assessments and advised Danish authorities. Frequently featured in Danish television, radio, and print media. Expertise: China; East Asia; the U.S.; foreign, defense, and security policy; cyber warfare; intelligence; and espionage. China's Use of Cyber Warfare: Espionage¶ Meets Strategic Deterrence Journal of Strategic Security Volume 4 Number 2 Summer 2011: Strategic Security in Article 2 the Cyber Age Accessed 8/28/2013 DMW]

Who actually attacks whom? China's own network appears to be unprotected, and other countries can launch attacks through China, which makes it appear the primary suspect.84 IT expert Steve Arm- strong furthermore states that "[i]t's too easy to blame China [...] In fact, legitimate countries are bouncing their attacks through China. It's very easy to do, so why not? [...] My evil opinion is that some western governments are already doing this."85¶ 2. Actors in the United States have an interest in exaggerating China's capabilities. In order to justify their existence and obtain increased budgets, several actors in the United States may have an interest in presenting China as a threat to U.S. security. The Pentagon, specific politicians, and the intelligence services are often accused of acting as they did during the Cold War, thus contributing to conflict-like rela- tions between China and the United States.86¶ 3. China proposes global cooperation against hacking.87 This might sound like a sound proposal, but as described throughout this article, certain states have much to gain by carrying out cyber attacks, which makes cooperation difficult. Besides, it is extremely hard to see how such cooperation could be enforced and by whom.¶ 4. It is also possible to imagine that in China, CNO has an anarchic lead- ership structure, meaning that the central leadership cannot control who carries out attacks. Some American reports indicate this very fact.88 Critical voices say, however, that this is just due to the way the Chinese use hackers from outside the military and the government to carry out attacks.89¶ 5. China denies having any military hackers in the country.90 Other countries would most likely deny the same, but to what extent soldiers in the PLA with high-level IT knowledge are being used to carry out cyber attacks is another question. Based on the references cited in this article, it is likely that the PLA uses hackers for espionage.¶ 6. Some think that focusing on China's capabilities does not deal with the fact that Beijing itself is very dependent on cyberspace for military and civilian purposes. This means that at the same time as China is devel- oping cyber warfare techniques, its own vulnerability is often over- looked.91 I would argue that China can still deter the U.S., even though the U.S. is more powerful in all spheres. This is due to the dynamics of the asymmetrical techniques that China pursues, e.g., in cyberspace, which are changing the dynamics of the balance of power that we knew during the Cold War.

#### No U.S./China relations collapse

China Daily 3 2-13, Lexis

During President Jiang Zemin's visit to the United States last year, he and Bush stated that China and the United States had extensive and crucial common interests and should expand their exchanges and co-operation in various areas to develop a constructive and co-operative Sino-US relationship. Improving Sino-US relations thus became the inevitable option in Washington's China policy. Since the mid-1980s, economic and trade exchanges have been a vital factor in bilateral ties and remain the most resilient chain. Bearing in mind the huge economic interests arising from China's entry to the World Trade Organization (WTO), Bush emphasized the importance of Sino-US economic and trade relations, even when pursuing a hard-line China policy in the initial period of his tenure. History has proved that, despite some twists and turns, common interests have overweighed differences in Sino-US relations.

#### No motivation for China will first-strike the US

#### No U.S./China war

Global Times 11 11/15, “Sino-US war unlikely but not impossible,” http://www.globaltimes.cn/NEWS/tabid/99/ID/684012/Sino-US-war-unlikely-but-not-impossible.aspx

A recent report released by the RAND Corporation, a US think tank specializing in military studies, examined the prospect of China and the US going to war, but concluded it improbable. What is the ultimate red line for a major military conflict between the two powers? Will the US back other Asian countries in provoking China? Global Times (GT) reporter Wang Wenwen talked to Major General Luo Yuan (Luo), deputy secretary-general of the PLA Academy of Military Sciences, and Robert M. Farley (Farley), a professor at the Patterson School of Diplomacy and International Commerce in the University of Kentucky, on these issues. Luo: At the current stage, both countries don't have the desire to start a war, nor do they have the capability. However, if China's core interests such as its sovereignty, national security and unity are intruded on, a military conflict will be unavoidable. Farley: I think that war is unlikely, but not impossible. Both countries have a lot to lose, both from the conflict itself and the overall fallout. If war does occur, I suspect that the trigger will be a miscalculation over Taiwan, or possibly North Korea. Some in the US might feel compelled to defend Taiwan following a declaration of independence; a North Korean collapse will lead to competition over the new structure of politics on the Korean Peninsula. Luo: The US is a pragmatic country. It will try to trigger a war in other countries or regions to deplete their powers while maintaining its own safety. The US will not really get involved into a war if the harm is greater than the benefits. Even if it does get involved, it won't sacrifice itself for its allies. Farley: I doubt that the US will become engaged in the South China Sea in any but a supporting role. However, the Taiwan situation is ripe for miscalculation by all the parties involved. I'm a bit less worried about either India or North Korea. While the US and India have been building a good relationship, the focus of Indian foreign policy remains on Pakistan, and previous Indo-Pakistani wars haven't dragged either China or the US in. In North Korea, I'm optimistic that diplomats will be able to work out the major issues without war.

## Civilian

#### Extinction outweighs ontology and V2L.

Santoni 85 Maria Theresa Barney Chair Emeritus of Philosophy at Denison University, Ronald, “Nuclear War: Philosophical Perspectives” p 156-157

To be sure, Fox sees the need for our undergoing “certain fundamental changes” in our “thinking, beliefs, attitudes, values” and Zimmerman calls for a “paradigm shift” in our thinking about ourselves, other, and the Earth.  But it is not clear that what either offers as suggestions for what we can, must, or should do in the face of a runaway arms race are sufficient to “wind down” the arms race before it leads to omnicide.  In spite of the importance of Fox’s analysis and reminders it is not clear that “admitting our (nuclear) fear and anxiety” to ourselves and “identifying the mechanisms that dull or mask our emotional and other responses” represent much more than examples of basic, often. stated principles of psychotherapy. Being aware of the psychological maneuvers that keep us numb to nuclear reality may well be the road to transcending them but it must only be a “first step” (as Fox acknowledges), during which we Simultaneously act to eliminate nuclear threats, break our complicity with the ams race, get rid of arsenals of genocidal weaponry, and create conditions for international goodwill, mutual trust, and creative interdependence.  Similarly, in respect to Zimmerman: in spite of the challenging Heideggerian insights he brings out regarding what motivates the arms race, many questions may be raised about his prescribed “solutions.”  Given our need for a paradigm shift in our (distorted) understanding of ourselves and the rest of being, are we merely left “to prepare for a possible shift in our self-understanding? (italics mine)?  Is this all we can do?  Is it necessarily the case that such a shift “cannot come as a result of our own will?” – and work – but only from “a destiny outside our control?”  Does this mean we leave to God the matter of bringing about a paradigm shift?  Granted our fears and the importance of not being controlled by fears, as well as our “anthropocentric leanings,” should we be as cautious as Zimmerman suggests about out disposition “to want to do something” or “to act decisively in the face of the current threat?”  In spite of the importance of our taking on the anxiety of our finitude and our present limitation, does it follow that “we should be willing for the worst (i.e. an all-out nuclear war) to occur”?  Zimmerman wrongly, I contend, equates “resistance” with “denial” when he says that “as long as we resist and deny the possibility of nuclear war, that possibility will persist and grow stronger.”  He also wrongly perceives “resistance” as presupposing a clinging to the “order of things that now prevails.” Resistance connotes opposing, and striving to defeat a prevailing state of affairs that would allow or encourage the “worst to occur.”  I submit, against Zimmerman, that we should not, in any sense, be willing for nuclear war or omnicide to occur.  (This is not to suggest that we should be numb to the possibility of its occurrence.)  Despite Zimmerman’s elaborations and refinements his Heideggerian notion of “letting beings be” continues to be too permissive in this regard.  In my judgment, an individual’s decision not to act against and resist his or her government’s preparations for nuclear holocaust is, as I have argued elsewhere, to be an early accomplice to the most horrendous crime against life imaginable – its annihilation.  The Nuremburg tradition calls not only for a new way of thinking, a “new internationalism” in which we all become co-nurturers of the whole planet, but for resolute actions that will sever our complicity with nuclear criminality and the genocidal arms race, and work to achieve a future which we can no longer assume. We must not only “come face to face with the unthinkable in image and thought” (Fox) but must act now - with a “new consciousness” and conscience - to prevent the unthinkable, by cleansing the earth of nuclear weaponry. Only when that is achieved will ultimate violence be removed as the final arbiter of our planet’s fate.

#### Ethical policymaking must be grounded in consequences

Isaac 2 Jeffrey C. Isaac, James H. Rudy Professor of Political Science and director of the Center for the Study of Democracy and Public Life at Indiana University, Bloomington. He writes regularly for Dissent, and his most recent book is Democracy in Dark Times. “Ends, Means, and Politics” at <http://www.dissentmagazine.org/article/?article=601>

As a result, the most important political questions are simply not asked. It is assumed that U.S. military intervention is an act of “aggression,” but no consideration is given to the aggression to which intervention is a response. The status quo ante in Afghanistan is not, as peace activists would have it, peace, but rather terrorist violence abetted by a regime—the Taliban—that rose to power through brutality and repression. This requires us to ask a question that most “peace” activists would prefer not to ask: What should be done to respond to the violence of a Saddam Hussein, or a Milosevic, or a Taliban regime? What means are likely to stop violence and bring criminals to justice? Calls for diplomacy and international law are well intended and important; they implicate a decent and civilized ethic of global order. But they are also vague and empty, because they are not accompanied by any account of how diplomacy or international law can work effectively to address the problem at hand. The campus left offers no such account. To do so would require it to contemplate tragic choices in which moral goodness is of limited utility. Here what matters is not purity of intention but the intelligent exercise of power. Power is not a dirty word or an unfortunate feature of the world. It is the core of politics. Power is the ability to effect outcomes in the world. Politics, in large part, involves contests over the distribution and use of power. To accomplish anything in the political world, one must attend to the means that are necessary to bring it about. And to develop such means is to develop, and to exercise, power. To say this is not to say that power is beyond morality. It is to say that power is not reducible to morality. As writers such as Niccolo Machiavelli, Max Weber, Reinhold Niebuhr, and Hannah Arendt have taught, an unyielding concern with moral goodness undercuts political responsibility. The concern may be morally laudable, reflecting a kind of personal integrity, but it suffers from three fatal flaws: (1) It fails to see that the purity of one’s intention does not ensure the achievement of what one intends. Abjuring violence or refusing to make common cause with morally compromised parties may seem like the right thing; but , then it is hard to view them as serving any moral good beyond the clean conscience of their supporters; (2) it fails to see that in a world of real violence and injustice, moral purity is not simply a form of powerlessness; it is often a form of complicity in injustice. This is why, from the standpoint of politics—as opposed to religion—pacifism is always a potentially immoral stand. In categorically repudiating violence, it refuses in principle to oppose certain violent injustices with any effect; and (3) it fails to see that politics is as much about unintended consequences as it is about intentions; it is the effects of action, rather than the motives of action, that is most significant. Just as the alignment with “good” may engender impotence, it is often the pursuit of “good” that generates evil. This is the lesson of communism in the twentieth century: it is not enough that one’s goals be sincere or idealistic; it is equally important, always, to ask about the effects of pursuing these goals and to judge these effects in pragmatic and historically contextualized ways. Moral absolutism inhibits this judgment. It alienates those who are not true believers. It promotes arrogance. And it undermines political effectiveness.

#### Empirics disprove---we’ve never caused blackouts in other countries---proves no internal link.

#### No impact to cyber attack

Birch 12 (Douglas Birth is the former foreign correspondent for the Associated Press and the Baltimore Sun who has written extensively on technology and public policy, “Forget Revolution.” 10/1/12 <http://www.foreignpolicy.com/articles/2012/10/01/forget_revolution?page=full> DATE ACCESSED: 11/4/12) TM

"That's a good example of what some kind of attacks would be like," he said. "You don't want to overestimate the risks. You don't want somebody to be able to do this whenever they felt like it, which is the situation now. But this is not the end of the world." The question of how seriously to take the threat of a cyber attack on critical infrastructure surfaced recently, after Congress rejected a White House measure to require businesses to adopt stringent­ new regulations to protect their computer networks from intrusions. The bill would have required industries to report cyber security breaches, toughen criminal penalties against hacking and granted legal immunity to companies cooperating with government investigations. Critics worried about regulatory overreach. But the potential cost to industry also seems to be a major factor in the bill's rejection. A January study by Bloomberg reported that banks, utilities, and phone carriers would have to increase their spending on cyber security by a factor of nine, to $45.3 billion a year, in order to protect themselves against 95 percent of cyber intrusions. Likewise, some of the bill's advocates suspect that in the aftermath of a truly successful cyber attack, the government would have to bail the utilities out anyway. Joe Weiss, a cyber security professional and an authority on industrial control systems like those used in the electric grid, argued that a well-prepared, sophisticated cyber attack could have far more serious consequences than this summer's blackouts. "The reason we are so concerned is that cyber could take out the grid for nine to 18 months," he said. "This isn't a one to five day outage. We're prepared for that. We can handle that." But pulling off a cyber assault on that scale is no easy feat. Weiss agreed that hackers intent on inflicting this kind of long-term interruption of power would need to use a tool capable of inflicting physical damage. And so far, the world has seen only one such weapon: Stuxnet, which is believed to have been a joint military project of Israel and the United States. Ralph Langner, a German expert on industrial-control system security, was among the first to discover that Stuxnet was specifically designed to attack the Supervisory Control and Data Acquisition system (SCADA) at a single site: Iran's Natanz uranium-enrichment plant. The computer worm's sophisticated programs, which infected the plant in 2009, caused about 1,000 of Natanz's 5,000 uranium-enrichment centrifuges to self-destruct by accelerating their precision rotors beyond the speeds at which they were designed to operate. Professionals like Weiss and others warned that Stuxnet was opening a Pandora's Box: Once it was unleashed on the world, they feared, it would become available to hostile states, criminals, and terrorists who could adapt the code for their own nefarious purposes. But two years after the discovery of Stuxnet, there are no reports of similar attacks against the United States. What has prevented the emergence of such copycat viruses? A 2009 paper published by the University of California, Berkeley, may offer the answer. The report, which was released a year before Stuxnet surfaced, found that in order to create a cyber weapon capable of crippling a specific control system ­­-- like the ones operating the U.S. electric grid -- six coders might have to work for up to six months to reverse engineer the targeted center's SCADA system. Even then, the report says, hackers likely would need the help of someone with inside knowledge of how the network's machines were wired together to plan an effective attack. "Every SCADA control center is configured differently, with different devices, running different software/protocols," wrote Rose Tsang, the report's author. Professional hackers are in it for the money -- and it's a lot more cost-efficient to search out vulnerabilities in widely-used computer programs like the Windows operating system, used by banks and other affluent targets, than in one-of-a-kind SCADA systems linked to generators and switches. According to Pollard, only the world's industrial nations have the means to use the Internet to attack utilities and major industries. But given the integrated global economy, there is little incentive, short of armed conflict, for them to do so. "If you're a state that has a number of U.S. T-bills in your treasury, you have an economic interest in the United States," he said. "You're not going to have an interest in mucking about with our infrastructure." There is also the threat of retaliation. Last year, the U.S. government reportedly issued a classified report on cyber strategy that said it could respond to a devastating digital assault with traditional military force. The idea was that if a cyber attack caused death and destruction on the scale of a military assault, the United States would reserve the right to respond with what the Pentagon likes to call "kinetic" weapons: missiles, bombs, and bullets. An unnamed Pentagon official, speaking to the Wall Street Journal, summed up the policy in less diplomatic terms: "If you shut down our power grid, maybe we will put a missile down one of your smokestacks." Deterrence is sometimes dismissed as a toothless strategy against cyber attacks because hackers have such an easy time hiding in the anonymity of the Web. But investigators typically come up with key suspects, if not smoking guns, following cyber intrusions and assaults -- the way suspicions quickly focused on the United States and Israel after Stuxnet was discovered. And with the U.S. military's global reach, even terror groups have to factor in potential retaliation when planning their operations.

#### Won’t cause civilian impact.

Libicki 11 [Martin C PhD, is a senior management scientist at RAND Corporation, focusing on the impacts of information technology on domestic and national security. He has published Conquest in Cyberspace: National Security and Information Warfare and Information Technology Standards: Quest for the Common Byte, as well as numerous monographs. Prior employment includes the National Defense University, the Navy Staff, and the GAO’s Energy and Minerals Division. He holds a master’s degree and PhD from the University of California–Berkeley.. Cyberwar as a Confidence Game Strategic Studies Quar terly ♦ Spring 2011 Online, Accessed 8/29/2013 DMW]

There is a wide range of opinion on that score. People have worried about cyberwar for most of the last 20 years, and in all that time, not one person is known to have been killed by a cyber attack.5 As for damage, estimates vary widely from several hundred million dollars a year to several hundred billion dollars a year. The most costly single attack was probably the “I Love You” virus in 2000, whose costs have been estimated at as much as $15 billion but which may be more realistically estimated at several hundred million dollars, if that.6 Only one power plant is known to have been disabled by hackers—a system in southern Brazil in 2007—and even there, the power outage has been disputed by local authorities as soot buildup. The only two examples of a state’s using cyber attacks against another were Russia’s attacks against Estonia in 2007 and Georgia in 2008 (and Russia’s responsibility is questionable in the first case); both caused disruption that can be measured at no more than the low millions of dollars, and both pulled their victims closer to rather than pushing them farther from NATO. The Stuxnet worm, if it worked, did serious damage, but it was closer in form to a onetime act of sabotage.

#### Sq deterrence solves

Weiner 12 [Sarah is a research intern for the Project on Nuclear Issues Searching for Cyber-Deterrence http://csis.org/blog/searching-cyber-deterrence Accessed 9/1/2013 DMW]

If defense strategists develop an understanding of cyber-security that differentiates between cyber-nuisances and higher-level cyber-attacks, however, countries can begin to more credibly establish deterrence doctrines and red lines. Hacking into a commercial bank is one thing, but taking down the electric grid, causing the release of toxic chemicals, or damaging essential infrastructure is quite another. The US could credibly threaten to retaliate against such devastating cyber-attacks with conventional force. But to do so, it must clearly distinguish non-deterrable, low-impact cyber-nuisances from high-impact attacks so Washington can establish a credible pattern of response and non-response. The US has begun to develop such policies, but significantly more definitional and doctrinal clarity will be necessary before it has a cyber-doctrine capable of signaling clear red lines. ¶ ¶ The most devastating cyber-attacks – the kind that would accompany or precede offensive military operations – are almost certainly deterrable. If an adversary believes their actions are likely to begin a war with the US, then the heft of the US’s substantial conventional capabilities will weigh against their decision to strike. That said, the stability of cyber-deterrence is unlikely to ever reach the levels we currently experience in the nuclear domain, where the offensive use of such weapons is almost unthinkable. But that may not necessarily be a bad thing. Nuclear deterrence works so well because the costs are so high; mutually assured destruction really does mean total destruction if deterrence fails. Most cyber-attacks could never come close to such levels of damage. And although that means we may be unable to deter low-level cyber-nuisances, it also means that the threat posed by cyber-weapons is much lower than the risk created by other historical revolutions in military technology. On the whole, that seems like a bargain worth accepting.

#### Cyber-Deterrence fails- to difficult

Libicki 13 [Martin C. research described in this report was prepared for the Office of the Secretary of Defense (OSD). The research was conducted within the RAND National Defense Research Institute, a federally funded research and development center sponsored by OSD, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community under Contract W74V8H-06-C-0002. Brandishing Cyberattack Capabilities http://www.rand.org Accessed 8/29/2013 DMW

A bigger challenge is how to demonstrate cyberwar capabilities. The most obvious way to demonstrate the ability to hack into an enemy’s system is to actually do it, leave a calling card, and hope it is passed forward to national decisionmakers. If the attack can be repeated at will or if the penetration can be made persistent, the target will be forced to believe in the attacker’s ability to pop into his system at any time. This should force the target to recalculate its correla- tion of forces against the attacker.¶ But as with many things in cyberspace, it sounds simpler than it is. Hinting at outright success is difficult without conceding one’s participation in mischief in the first place and hence cyberwar’s legitimacy as a tool of statecraft, something countries only started acknowl- edging in mid-2012. Targets of little value tend to be easy, but penetrating them is unimpres- sive. Targets of some value are, for that reason, much harder, often because they are electroni- cally isolated. Finally, the ability to penetrate a system does not necessarily prove the ability to break a system. The latter requires not only breaking into sufficiently privileged levels but also figuring out how to induce a system to fail and keep on failing. But penetration may be suf- ficiently scary in itself if the target leadership cannot discern the difference between breaking into and breaking.¶ Breaking a system is more hostile and more difficult than breaking into one. It requires an understanding of what makes the system fail. Getting the desired results also requires shap- ing the attack so that those who administer the system cannot detect the attack and repair the damage quickly. Conveying to others the ability to bring their systems down and keep them down is not easy. Intended audiences of such demonstrations may subsequently identify the flaw that would allow such an attack and fix it. If so, for brandishing to work, cyberattack capabilities may require repeated demonstration. Alternatively, a less hostile demonstration could be to manipulate the system but not to the point of harming it, a fine line.

#### It’s not key- US tech and military is miles ahead of everyone else

Hjortdal 11 [Magnus is a researcher associated with CHINA-SEC, Centre for Military Studies at the University of Copenhagen. He holds an M.Sc. in Political Science from the University of Copenhagen and is owner of MH International Relations, which advises private and public institutions. Former Research Fellow at the Royal Danish Defense College, where he drew assessments and advised Danish authorities. Frequently featured in Danish television, radio, and print media. Expertise: China; East Asia; the U.S.; foreign, defense, and security policy; cyber warfare; intelligence; and espionage. China's Use of Cyber Warfare: Espionage¶ Meets Strategic Deterrence Journal of Strategic Security Volume 4 Number 2 Summer 2011: Strategic Security in Article 2 the Cyber Age Accessed 8/28/2013 DMW]

The West and the United States, for example, may also be expected to act similarly to what China is accused of doing.10 However, an analysis of American capabilities is not the topic here since the United States does not have as much to gain relative to China by developing an aggressive cyber capability. This can be seen in light of the three reasons previously cited for which states seek to maintain and utilize such a capability. First, the United States does not need to deter other states via cyberspace, since it manages just fine militarily. Secondly, the reality today is that since U.S. military technology is second to none, intensive espionage to gain knowl- edge about other states' military technology is not necessary. As for the third reason regarding economic advantage, industrial espionage has less significance for the United States since industrial-technological levels in the United States are among the most advanced in the world.

## Blowback

#### Blowback is inevitable---cyber prolif is already happening now

LEWIS 13 [JAMES ANDREW is a senior fellow and director of the Technology and Public Policy Program at CSIS. Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service officer and as a member of the Senior Executive Service. His current research examines the political effect of the Internet, strategic competition among nations, and technological innovation. Lewis received his Ph.D. from the University of Chicago. a report of the technology and public policy program

Conflict and Negotiation in Cyberspace, Accessed 9/2/2013 DMW

Nor is the idea of preventing the “proliferation” of cyber weapons a useful strategy to reduce risk. Widespread commercial availability undercuts any effort at control. Cyberattacks use widely available commercial products—roughly 400 million desktops and notebook computers were produced in 2001, for example, and estimates place the number of such machines produced since 2004 at over 2.3 billion.38 Software coding skills are ubiquitous and easily acquired, and many of the tools available for legitimate network analysis and administration can be used for attack pur- poses. While it might be possible to close down the flourishing back market in cyber exploits and criminal software, these are not the source of the most advanced techniques.¶ Cyber exploitation techniques are also widely and routinely used in criminal and espionage activities, and the line between a penetration for the purposes of exfiltrating information and a penetration for disruption network services and data is very thin. The notion of calling for an end to espionage is laughable, and since espionage will continue, nations will have access to the tools needed for certain kinds of cyberattack. The widespread availability of commercial products and software makes the idea of banning “cyber weapons” suspect and impossible to define in a mean- ingful way. Specific code like that used in Stuxnet could be called a weapon, but the components and “precursors” for the “weapon” are so widely available in legitimate markets around the globe that any ban could be easily circumvented.

#### US can’t solve modeling- no norms are followed---can’t solve blowback

Libicki 9 (Martin, Senior Management Scientist at the RAND Corporation, "Cyberdeterrence and Cyberwar", http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND\_MG877.pdf)

Historically, arms control has always gone hand in hand with deter- rence and crisis stability, but it would be difficult to be optimistic about its prospects in cyberspace. A good deal depends on what one means by arms control. If the model were to be something like the treaties signed between the United States–NATO and the Soviet Union– Warsaw Pact, which limited certain classes of weapons and banned others, there is little basis for hope. 1 If, instead, the goal were a framework of international agreements and norms that could raise the diffi- culty of certain types of cyberattacks, some progress can be made. Why is it nearly impossible to limit or ban cyberweapons? First, although the purpose of “limiting” arms is to put an inventory-based lid on how much damage they can do in a crisis, such a consideration is irrelevant in a medium in which duplication is instantaneous. 2 Second, banning attack methods is akin to banishing “how-to” information, which is inherently impossible (like making advanced mathematics illegal). The same holds for banning knowledge about vulnerabilities. Third, banning attack code is next to impossible. Such code has many legitimate purposes, not least of which is in building defenses against attack from others. These others include individuals and nonstate actors, so the argument that one does not need defenses because offenses have been outlawed is unconvincing. In many, per- haps most cases, such attack code is useful for espionage, an activity that has yet to be banned by treaty. Furthermore, finding such code is a hopeless quest. The world’s information storage capacity is immense; much of it is legitimately encrypted; and besides, bad code does not emit telltale odors. If an enforcement entity could search out, read, and decrypt the entire database of the world, it would doubtless find far more interesting material than malware. Exhuming digital informa- tion from everyone else’s systems is hard enough when the authorities with arrest powers try it; it may be virtually impossible when outsiders try. The only barely feasible approach is to ban the activity of writing attack code, then hope that the fear of being betrayed by an insider who goes running to international authorities prevents governments from organizing small groups of elite hackers from engaging in such nefarious activities. If the international community had the manpower and access to enforce such norms, it could probably enforce a great many other, and more immediately practical, norms (e.g., against cor- ruption). Such a world does not exist.

## Solvency

#### Congress doesn’t have capabilities to ensure compliance or success

Dycus 10 [Stephen, Professor, Vermont Law School. Congress’s Role in Cyber Warfare JOURNAL OF NATIONAL SECURITY LAW & POLICY [Vol. 4:155 2010] http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDUQFjAB&url=http%3A%2F%2Fjnslp.com%2Fwp-content%2Fuploads%2F2010%2F08%2F11\_Dycus.pdf&ei=-r8fUouoM-izsQTGvIGoCw&usg=AFQjCNFeTSdaF\_RrGhCVMDeCrO02XeCzGw&sig2=aXj04Yn\_CPE493NHErRmOw&bvm=bv.51495398,d.cWc&cad=rja Accessed 8/29/2013 DMW

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

#### **DOD Incapable of maintaining cyber ops**

GAO 11

(United States Government Accountability Office, July 2011, "DEFENSE DEPARTMENT CYBER EFFORTS DOD Faces Challenges In Its Cyber Activities", www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-049.pdf, Date Accessed: 8/28/13, MSN)

According to the 2006 National Military Strategy for Cyberspace ¶ Operations, military departments and certain agencies and commands ¶ should develop the capabilities necessary to conduct cyberspace ¶ operations, including consistently trained personnel, infrastructure, and ¶ organization structures. U.S. Strategic Command’s Operational Concept ¶ for Cyberspace reported in 2008 that national security vulnerabilities ¶ inherent in cyberspace make it imperative that the United States develop ¶ the requisite capabilities, policy, and tactics, techniques, and procedures ¶ for employing offensive, defensive, and supporting operations to ensure ¶ freedom of action in cyberspace. In addition, a study commissioned by ¶ the Joint Staff and conducted by the Institute for Defense Analyses states ¶ that the key underlying drivers of effectiveness in cyberspace are ¶ developing and deploying the right tools and building and sustaining an ¶ adequate cyber force of trained and certified people.55 Institute for Defense Analyses officials stated that unless DOD has adequate ¶ resources for cyber ¶ operations, organizational changes within the cyber domain will not be ¶ effective. ¶ DOD commands have identified capability gaps that hinder their ability to ¶ marshal resources to operate in the cyberspace domain. U.S. Strategic ¶ Command and other combatant commands highlighted their cyber ¶ capability gaps in their Integrated Priority Lists for fiscal years 2011-¶ 2015.56 U.S. Strategic Command, which is tasked with being the global ¶ synchronizer for cyber operations within DOD, identified in its Integrated ¶ Priority List for fiscal years 2011-2015 gaps and associated priorities in ¶ such areas as the need to be able to defend against known threats, ¶ detect or characterize evolving threats, and conduct exploitation and ¶ counter operations, as desired. U.S. Strategic Command listed cyberrelated gaps as its highest priority, emphasizing the need for and ¶ importance of resources to increase cyber capabilities. U.S. Pacific ¶ Command, U.S. Special Operations Command, and U.S. Joint Forces ¶ Command have also reported cyber capability gaps involving lack of ¶ sufficient numbers of trained personnel to support their cyber operations ¶ and a need for additional cyber intelligence capabilities. ¶ U.S. Strategic Command has reported that the lack of cyber resources it ¶ identified has affected the command’s ability to respond to requests for ¶ cyber capabilities from other combatant commands, particularly for fullspectrum cyberspace operations. It remains to be seen what effect the ¶ newly proposed U.S. Cyber Command will have on this process, ¶ particularly with Joint Functional Component Command for Network ¶ Warfare and Joint Task Force–Global Network Operations being merged ¶ into one organization within the new U.S. Cyber Command. ¶ A need for more cyber planners and cyber-focused intelligence analysts ¶ was a common theme during our meetings with officials at the combatant ¶ commands. Officials at several of the geographic combatant commands ¶ stated that without the proper planners and cyber-focused intelligence ¶ analysts, they lacked situational awareness of their networks and the ability to both plan cyber operations for their respective commands and ¶ request applicable support from U.S. Strategic Command. For example, ¶ cyber planners play a key part in the developmental process of a ¶ computer network attack operation. U.S. Central Command officials ¶ stated that although most computer network attack operations are being ¶ conducted in its area of responsibility, it does not have a single full-time ¶ dedicated cyber planner to assist in the development of such operations. ¶ Because it lacks the appropriate trained personnel and dedicated career ¶ path, U.S. Central Command has redirected personnel with cyber ¶ expertise to act as temporary planners. This greatly affected the ¶ command’s ability to match resources to, and plan for, all cyber-related ¶ functions. For example, a cyber planner within U.S. Central Command ¶ was borrowed from another career field, worked as a planner for a time, ¶ and then was reassigned to help resolve information technology issues at ¶ a help desk. ¶ Without a sufficient number of cyber planners in-theater, combatant ¶ commands will continue to struggle with being able to plan cyber activities ¶ to assist in accomplishing the commander’s mission objectives, and ¶ communicating their need for assistance to U.S. Strategic Command. The ¶ lack of skilled and highly trained cyber personnel presents challenges for ¶ many DOD components, and the lack of sufficient personnel prevents ¶ DOD components from fulfilling essential computer network operation ¶ activities

# 2NC

## CP

#### Classified QDR solves implementation problems

Whiting, Fierce Government Reporter, 2013,

(Geoff, "QDR doesn't set useable defense strategy, say panelists,", Fierce Government, 2-4, PAS) <http://www.fiercegovernment.com/story/qdr-doesnt-set-useable-defense-strategy-say-panelists/2013-02-04> 9-1-13

The 2014 QDR process needs to have fewer players and focus on new ways to approach goals, he said, such as recent efforts to combat terrorist networks by directing federal efforts at reducing global, catastrophic capabilities while relying on friendly regional partners to address local events.¶ Shawn Brimley, a senior fellow at the Center for a New American Security who played a part in crafting the 2010 QDR, said that the process would set better targets and goals if it were classified, either in part or in whole.¶ Brimley said the process now is essentially "coming up with a bumper sticker that would describe an incredibly complicated set of force planning scenarios and methodology." Since the QDR relies heavily on classified documents and reports, said Brimley, the QDR would be best served by having their findings represented as accurately as possible by not removing important classified findings.¶ The declassified document also cannot be explicit enough on some goals so it can leave some issues open to interpretation and that "extends the difficulties of trying to implement some of the decisions in the QDR," he said.

#### Classification solves bureaucracy problems and delay

Brimley, (CNAS) Center for a New American Security Senior Fellow, 2013,

(Shawn, “Preparing for the 2014 Quadrennial Defense Review”, CSIS, March, Pg. 29, PAS) <http://csis.org/files/publication/130319_Murdock_Preparing2014QDR_Web.pdf> 8-28-13

Moreover, a classified component of the QDR could be disseminated within DOD, and could ¶ provide better and more specific guidance to the Services and the COCOMs, who will typically ¶ interpret the unclassified QDR in “creative ways” during the next budget cycle, or when ¶ developing other guidance (e.g. GEF, GDF etc.). A formal classified component of the QDR could ¶ prevent months of debating “first principles” based on what an unclassified QDR really “meant ¶ to say.”¶ Key Point: The 2014 QDR should include a classified component that is formally ¶ integrated into the QDR report to Congress, and can be leveraged inside DOD to ¶ disseminate key implementation guidance.

#### Experience of Hagel’s office and sequestration allows opportunity to overcome barriers

Hoffman, Institute for National Strategic Studies Senior Research Fellow, 2013,

(Frank, "MAKING THE QDR A SUCCESS", War on the Rocks, 7-28, PAS) warontherocks.com/2013/07/making-the-qdr-a-success/ 9-1-13

Does the Quadrennial Defense Review (QDR) matter?¶ Former Pentagon strategist and current CNAS Vice President Shawn Brimley recently commented, “With wars ending, budgets declining, technology proliferating, and other powers rising, a real window of opportunity to reshape U.S. defense strategy has opened for the first time since the end of the Cold War.” The Atlantic Council’s Dr. James Joyner, disagrees and bemoans the “hype” behind the QDR. He has a valid point about the long odds against the QDR given their track record, but he underestimates its strategic importance this time around.\*¶ The upcoming QDR is the most important one in two decades. It’s not only a window of opportunity, but a desperate door to solvency. We need to close the gap between our missions and forces, and our expansive aspirations and a shrinking budget. Until that occurs the insolvency gap between our strategy and defense spending will only widen. The consequences are high and many allies and adversaries are watching.¶ As disappointed as I’ve been with our strategic thinking (or lack thereof) in the post-Cold War era, the stars are aligned for this QDR to deliver what we really need from it. Secretary of Defense Chuck Hagel has the remaining tenure to take on and implement bold changes. Moreover, his office’s policy team is well-established, having produced a solid strategic defense guidance in early 2012. Add sequestration – which is forcing everyone to make hard choices, albeit clumsily – and you finally have the right pressure for innovation. A lot of interwar innovation in the 1920s and 1930s at the Naval War College and in annual Fleet Exercises came during periods of even greater austerity.

## DA

#### DA comes faster than the aff solves- the plan collapses perceptions of deterrence

Zeisberg 4 Mariah Zeisberg, PhD in Politics from Princeton, Postdoc Research Associate at the Political Theory Project of Brown University; “INTERBRANCH CONFLICT AND CONSTITUTIONAL MAINTENANCE: THE CASE OF WAR POWERS”; June 2004; found in Word document, can be downloaded from [www.brown.edu/Research/ppw/files/Zeisberg%20Ch5.doc](http://www.brown.edu/Research/ppw/files/Zeisberg%20Ch5.doc)

The first significant argument of pro-Presidency insularists is that flexibility is a prime value in the conduct of foreign affairs, and especially war. Implicit in this argument is the recognition that the executive is functionally superior to Congress in achieving flexibility and swiftness in war operations, a recognition I share. The Constitution cannot be meant to curtail the very flexibility that may be necessary to preserve the nation; and yet, according to the insularists, any general norm which would include Congress in decision-making about going to war could only undermine that flexibility. Writing on the War Powers Act, Eugene Rostow predicts that it would, “**put the Presidency in a straightjacket of a rigid code**, and prevent new categories of action from emerging, **in response** to the necessities of a tense and unstable world.” In fact, Rostow believes, “[t]he centralization of authority in the president is particularly crucial in matters of national defense, war, and foreign policy, where a unitary executive can evaluate threats, consider policy choices, and mobilize national resources **with a speed and energy** that is **far superior to any other branch.”** Pro-presidency insularists are fond of quoting Hamilton, who argued that “[o]f all the cares or concerns of government, the direction of war most peculiarly demands those qualities which distinguish the exercise of power by a single hand.” This need for flexibility, some insularists argue, is especially acute given modern conditions, where devastating wars can develop quickly. Today, “many foreign states have the power to attack U.S. forces - and some even the U.S. mainland - almostinstantly**,”** and in such a world it is impracticable to require the President to seek advance authorization for hostilities. Such a requirement would simply be too risky to U.S. security. We furthermore face a nuclear age, and the system of deterrence that operates to contain that threat requires that a **single person** be capable of responding to nuclear attack with nuclear weapons immediately. Rostow writes, “the requirement for advance authorization would collapse the system of deterrence**, making preemptive strikes by our enemies** more **likely**.” Hence, “modern conditions” require the President to “act quickly, and often alone.” While this does not mean that Congress has no role to play in moments of crisis, it does mean that Congress should understand its role largely in terms of cooperating with the President to support his negotiations and decisions regarding relationships with foreign powers. Rostow writes, “Congress should be able to act effectively both before and after moments of crisis or potential crisis. It may join the President in seeking to deter crisis by publicly defining national policy in advance, through the sanctioning of treaties or other legislative declarations. Equally, Congress may participate formally in policymaking after the event through legislative authorization of sustained combat, either by means of a declaration of war, or through legislative action having more limited legal and political consequences. Either of these devices, or both in combination, should be available in situations where cooperation between the two branches is indicated at many points along an arc ranging from pure diplomacy at one end to a declaration of war at the other.” In other words, for Congress to understand itself as having any justifiable role in challenging executive security determinations, especially at moments of crisis, would be to undermine the strength that the executive requires in order to protect the nation. Conflict in this domain represents political degradation.

## Solv

### Ext- Rollback

#### Oversight fails- congress provide guidance in urgent circumstances- also the person in charge with implementation might make mistakes such as misinterpreting attacs- statutory policy cant get compliance from the executive- that’s Dycus

#### President can circumvent reforms- empirics

Lorber 13 [Eric, Upenn Law School; Duke University - Department of Political Science Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power? http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2017036&download=yes Accessed 8/29/2013 DMW]

Pg.1001

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.234 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).235 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.

#### Low threshold for circumvention

Lorber 13 [Eric, Upenn Law School; Duke University - Department of Political Science Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power? http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2017036&download=yes Accessed 8/29/2013 DMW]

999-1000

Despite falling into this category, however, such an offensive operation, for the reasons discussed above, likely satisfies the congressional test for a traditional military activity. First, because General Alexander is the commander of both CYBERCOM and the head of the National Security Agency and because many of the personnel are dual-hatted at the respective organizations, any offensive cyber operation conducted independently of a kinetic assault will be commanded and executed by military personnel.230 Second, because the President can launch offensive cyber operations without congressional notification if they are in anticipation of hostilities,231 he also has great flexibility in deciding whether to report his activities. For example, if the President were to order the launch of a Stuxnet-style attack against Iran to degrade its nuclear enrichment capability, such an activity would—assuming it was done with the Secretary of Defense’s consent— necessarily constitute approval by the National Command Authority. In addition, because the definition of operational planning—another element required in fulfilling the TMA exception to the definition of covert action— is so broad, such an attack would likely fall within its purview. The President would simply argue that approval has been given for operational planning of future combat operations with Iran (which it almost certainly has in the U.S. military)232 and therefore the activity was taking place in the context where overt hostilities are anticipated. Indeed, only in a situation where no contingency planning has occurred—such as with an ally or a country that the United States takes little interest—would this exception not apply.¶ As a result, it becomes evident that even a Stuxnet-type of attack likely will not trigger the requirements set forth in the Intelligence Authorization Act. Given the dual-hatted nature of many NSA and CYBERCOM personnel, as well as the fact that action approved by the President and the Secretary of Defense necessarily constitutes approval by the National Command Authority, all the executive branch must realistically show is that it undertook the operation in a context where operational planning had occurred for potential hostilities at some undefined point in the future. This hurdle is very low and the executive should have little problem clearing it.¶ These limited requirements suggest that the executive can easily argue that offensive cyber operations conducted both as independent actions and in conjunction with kinetic operations likely fall under the Traditional Military Activity exception to the definition of covert action as provided by the Intelligence Authorization Act. As a result, the President is likely not statutorily required to report any offensive cyberattacks under the Act.

### Ext- No impact

#### No impact to cyber attacks- they overestimate the risks- years after Stutnex we have seen no similar attacks- also the only countries that can have no incentive to attack due to interdependence and well as the threat of retaliation- that’s Birch

#### Impact would be small and temporary

Gartzke 12 (Erik, Associate Professor in Political Science at UC-San Diego. “The Myth of Cyberwar” Page 15-16 12-7-12 http://dss.ucsd.edu/~egartzke/papers/cyberwar\_12062012.pdf

Beyond questions of means and motive, two basic features make cyber warfare di erent from other¶ types of con¶ ict. First, the bulk of damage contemplated by cyberwar is in all likelihood temporary.¶ The assumption among many cyber-pessimists that the potential for creating harm is sufficient to¶ make cyber space a suitable substitute for, or at least an alternative to, terrestrial conflict is simply¶ incorrect. Shutting down the power grid, or preventing communication could be tremendously¶ costly, but most such damage can be corrected quickly and with comparatively modest investment¶ of tangible resources. Regardless, damage of this type is sunk. Losses experienced over a given time¶ interval cannot be recovered whatever one's reactions and so should not have much direct impact on subsequent policy behavior. Harm inflicted over the internet or through any other medium¶ will matter politically when it involves changes to the subsequent balance of power, or when it¶ indicates enemy capabilities that must be taken into account in future plans. Precisely because¶ cyberwar does not involve bombing cities or devastating armored columns, the damage inflicted¶ will have a short-term impact on targets.10 To accomplish meaningful objectives, cyber attacks¶ must contribute to other aspects of a more conventional war e ort. In order to a ect the long-term¶ balance-of-power, for instance, cyberwar must be joined to other, more traditional, forms of war.

#### 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.

#### No motive

Gartzke 12 (Erik, Associate Professor in Political Science at UC-San Diego. “The Myth of Cyberwar” Page 1 12-7-12 http://dss.ucsd.edu/~egartzke/papers/cyberwar\_12062012.pdf

A blitz of media, punditry and public pronouncements inform interested observers and policy¶ makers that the next war is likely to be won or lost on the internet. Indeed, events such as the¶ coordinated cyber attacks on Estonia and the Stuxnet worm seem to indicate that cyberwar has¶ already begun. The sense of urgency surrounding cyberwar appears to be tied to perceptions that¶ internet con¶ ict is the newest phase in the ongoing revolution in military a airs, only this time the¶ threat is directed at the sophisticated technological civilizations of the West, rather than at poor¶ developing states or the recipients of inferior second-world military hardware.1 To believe a growing¶ number of pundits and practitioners, cyberwar threatens to render existing military advantages¶ impotent, exposing those nations most dependent on comprehensive information infrastructures to¶ devastating and unpredictable attacks. If powerful states largely immune to terrestrial invasion¶ can have their military might blunted and their factories and cities idled by foreign hackers, then¶ perhaps this latest technological revolution really does presage a \Pearl Harbor" in which the¶ United States and other great powers will be targets, rather than perpetrators, of shock and awe.¶ There is a problem with the growing consensus of impending cyber apocalypse, however: it is¶ far from clear that con¶ ict over the internet can actually function as war. Discussions of cyberwar¶ commit a common fallacy of arguing from opportunity to outcome, rather than considering whether¶ something that could happen is at all likely, given the motives of those who are able to act.¶ Cyber pessimism rests heavily on capabilities (means), with little thought to a companion logic of¶ consequences (ends). Much that could happen in the world fails to occur, largely because those¶ capable of initiating action discern no benefit from doing so. Put another way, advocates have yet¶ to work out how cyberwar actually accomplishes the objectives that typically sponsor terrestrial¶ military violence. Absent a logic of consequences, it is di cult to believe that cyberwar will proveas devastating for world a airs and for developed nations in particular as many seem to believe.

### Ext- OCO Solves

#### OCO contains China- asking nicely wont solve- that’s Junio

#### Weak Obama on cybersecurity emboldens Chinese attacks

Davis 13 Matthew Davis, March 08, 2013, Matthew Davis: Obama's weak response to Chinese cyber attacks puts America at risk, <http://www.mlive.com/politics/index.ssf/2013/03/matthew_davis_obamas_weak_resp.html>

American foreign policy is usually the sole province of the executive branch - treaty ratification and Congressional resolutions authorizing the use of force notwithstanding. In a world that is still decades -- and in some cases centuries -- behind Western civilization with respect to openness, tolerance, and human rights, American foreign policy works best when we have a president who grasps Theodore Roosevelt's "big stick" doctrine. Moreover, the president must, in the words of John F. Kennedy, "Let every nation know, whether it wishes us well or ill, that we shall pay any price, bear any burden, meet any hardship, support any friend, oppose any foe to assure the survival and the success of liberty." President Barack Obama is failing miserably on both accounts when it comes to Chinese cyber security. Last month, the security firm Mandiant released a report that concluded the Chinese military "has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously." Moreover, the report notes that the observed thefts are but a fraction of what has likely been stolen since at least 2006. In other words, Obama is fiddling while our technology is being pilfered. Michigan's own U.S. Rep. Mike Rogers, R-Brighton, said in a statement the same day the report was released: "The Chinese government's direct role in cyber theft is rampant and the problems have grown exponentially. The Mandiant report provides vital insights into the Chinese government’s economic cyber espionage campaign against American companies. It is crucial that the Administration begin bilateral discussions to ensure that Beijing understands that there are consequences for state sponsored economic espionage." Rogers is a tough, no-nonsense former FBI agent. He's an expert on international security. He and C.A. "Dutch" Ruppersberger, D-Maryland, have introduced legislation to help, but that doesn't make China -- or its ambitions with respect to American technology -- disappear. Rather, the main person who needs to act -- and with a clear demonstration that Chinese predation of American technology will be punished severely -- is the president. It is his reaction to this crisis (another one that has been all but ignored by the mainstream media, for the sake of the usual twaddle) that will either thwart or encourage the Chinese.

#### Maintaining OCO is key to prevent conflicts

McAllister 13 [Neil, The Register, Leaked Obama brief reveals US cyber defense, offense policy http://www.theregister.co.uk/2013/06/07/presidential\_policy\_directive\_20/ Accessed 8/27/2013 DMW]

The United States has an abiding interest in developing and maintaining use of cyberspace as an integral part of U.S. national capabilities to collect intelligence and to deter, deny, or defeat any adversary that seeks to harm U.S. national interests in peace, crisis, or war.¶ In the case of OCEO, the directive advises a proactive stance, lest the US be caught with its pants down. When the time comes for an offensive strike, government agencies are advised to know in advance where there adversaries' weak spots are:¶ OCEO can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging. The development and sustainment of OCEO capabilities, however, may require considerable time and effort if access and tools for a specific target do not already exist.¶ The United States Government shall identify potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power, establish and maintain OCEO capabilities integrated as appropriate with other U.S. offensive capabilities, and execute those capabilities in a manner consistent with the provisions of this directive.

#### OCOs give the US coercive leverage to deescalate rogue state 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.

## No spillover

#### Issues don’t spillover

IPS 3 Inter-Press Service, 11-4, Lexis

Indeed, it now appears that, despite rising tensions over the bilateral trade balance and the value of the yuan, the realists centered in the State Department have decisively taken control over U.S. China policy, thanks largely to Beijing's own behavior and rapidly growing influence. "The administration has come to the conclusion that strategic engagement is the only viable option on relations with China," says Garrett. That Washington's major problem today is over currency, he adds, illustrates the degree to which Sino-U.S. relations have stabilized. "This is the kind of problem we have with Japan," Garrett said. "We're at the point where we can have differences in one area without it threatening other aspects of the relationship."

## Empirics

#### Collapse empirically denied

Shambaugh 5 David, Professor of Political Science and International Affairs – George Washington University and Fellow – Brookings Institute, “The New Strategic Triangle: U.S. and European Reactions to China's Rise”, Washington Quarterly, Summer, Lexis

Third, significant divergences exist along all the legs of the new strategic triangle as well. The United States and Europe have certainly had their fair share of recent disagreements about Iraq, a series of international treaties and regimes, the role of the United States in the world, and the China arms embargo. China and Europe have had a series of disputes over trade and MES classification as well as disagreements over human rights. Europe has concerns about China’s proliferation practices, as well as the arms embargo. More recently, China’s Europe specialists have begun to criticize the motives underlying EU programs to promote civil society in China as an ideological ruse to “Westernize and divide China” (Xi-hua, fen-Hua).12 The United States and China have also disputed human rights, trade, and proliferation, as well as Taiwan, missile defense, and regional security in East Asia. All these features add up to a very fluid and shifting set of relationships in which mutual positions sometimes converge and sometimes diverge. The EU and the United States sometimes side with each other, China and the EU sometimes find themselves in agreement, the United States and China sometimes work well together, and sometimes the interests and policies of all three intersect, all while each side simultaneously has disputes with the other two parties. What has not occurred, to date, is a situation where U.S. and Chinese perspectives converge against European interests.

#### No U.S./China war- ties check

Sargent 8 Sara, Business Reporter – Medill News Service, “China Space Launch Raises Fears”, UPI, 10-3, Lexis

In January 2007 China conducted its first successful anti-satellite weapons test by destroying one of its own space weather satellites. The move angered the U.S. government, which accused the Chinese of making a move toward militarizing outer space. Despite the U.S. government's concerns, the only circumstance under which the United States and China would engage in space warfare is in the face of another conflict, suggests Dean Cheng, senior Asia analyst for Virginia-based think tank CNA. And given the **current** stability of U.S.-Chinese relations and the **economic interdependence** of the two nations, Cheng and other experts agree that war is an exceptionally unlikely scenario.

#### Nuclear primacy checks

Lieber and Press 6 Keir A., Assistant Professor of Political Science – Notre Dame and Daryl G., Associate Professor of Political Science – University of Pennsylvania, Foreign Affairs, March / April, Lexis

For almost half a century, the world's most powerful nuclear states have been locked in a military stalemate known as mutual assured destruction (MAD). By the early 1960s, the nuclear arsenals of the United States and the Soviet Union had grown so large and sophisticated that neither country could entirely destroy the other's retaliatory force by launching first, even with a surprise attack. Starting a nuclear war was therefore tantamount to committing suicide. During the Cold War, many scholars and policy analysts believed that MAD made the world relatively stable and peaceful because it induced great caution in international politics, discouraged the use of nuclear threats to resolve disputes, and generally restrained the superpowers' behavior. (Revealingly, the last intense nuclear standoff, the 1962 Cuban missile crisis, occurred at the dawn of the era of MAD.) Because of the nuclear stalemate, the optimists argued, the era of intentional great-power wars had ended. Critics of MAD, however, argued that it prevented not great-power war but the rolling back of the power and influence of a dangerously expansionist and totalitarian Soviet Union. From that perspective, MAD prolonged the life of an evil empire. This debate may now seem like ancient history, but it is actually more relevant than ever -- because the age of MAD is nearing an end. Today, for the first time in almost 50 years, the United States stands on the verge of attaining nuclear primacy. It will probably soon be possible for the United States to destroy the long-range nuclear arsenals of Russia or China with a first strike. This dramatic shift in the nuclear balance of power stems from a series of improvements in the United States' nuclear systems, the precipitous decline of Russia's arsenal, and the glacial pace of modernization of China's nuclear forces. Unless Washington's policies change or Moscow and Beijing take steps to increase the size and readiness of their forces, Russia and China -- and the rest of the world -- will live in the shadow of U.S. nuclear primacy for many years to come. One's views on the implications of this change will depend on one's theoretical perspective. Hawks, who believe that the United States is a benevolent force in the world, will welcome the new nuclear era because they trust that U.S. dominance in both conventional and nuclear weapons will help deter aggression by other countries. For example, as U.S. nuclear primacy grows, China's leaders may act more cautiously on issues such as Taiwan, realizing that their vulnerable nuclear forces will not deter U.S. intervention -- and that Chinese nuclear threats could invite a U.S. strike on Beijing's arsenal. But doves, who oppose using nuclear threats to coerce other states and fear an emboldened and unconstrained United States, will worry.

#### Chinese leadership will pull back

Ross 1 Robert S., Professor of Political Science – Boston College, The National Interest, Fall, Lexis

The strategic costs to China of a war with the United States are only part of the deterrence equation. China also possesses vital economic interests in stable relations with the United States. War would end China's quest for modernization by severely constraining its access to U.S. markets, capital and technology, and by requiring China to place its economy on permanent war-time footing. The resultant economic reversal would derail China's quest for "comprehensive national power" and great power status. Serious economic instability would also destabilize China's political system on account of the resulting unemployment in key sectors of the economy and the breakdown of social order. Both would probably impose insurmountable challenges to party leadership. Moreover, defeat in a war with the United States over Taiwan would impose devastating nationalist humiliation on the Chinese Communist Party. In all, the survival of the party depends onpreventing a Sino-American war**.**

**No US-China conflict**

Allison & Blackwill 3/5 -- \*director of the Belfer Center for Science and International Affairs and Douglas Dillon Professor at Harvard's John F. Kennedy School of Government AND \*\*Henry A. Kissinger Senior Fellow for U.S. foreign policy at the Council on Foreign Relations (Graham and Robert D., 2013, "Interview: Lee Kuan Yew on the Future of U.S.- China Relations," http://www.theatlantic.com/china/archive/2013/03/interview-lee-kuan-yew-on-the-future-of-us-china-relations/273657/)

Interview with Lee Kuan Yew, the founding prime minister of Singapore, one of Asia's most prominent public intellectuals, a member of the Fondation Chirac's honour committee

Competition between the United States and China is inevitable, but conflict is not. This is not the Cold War. The Soviet Union was contesting with the United States for global supremacy. China is acting purely in its own national interests. It is not interested in changing the world. There will be a struggle for influence. I think it will be subdued because the Chinese need the United States, need U.S. markets, U.S. technology, need to have students going to the United States to study the ways and means of doing business so they can improve their lot. It will take them 10, 20, 30 years. If you quarrel with the United States and become bitter enemies, all that information and those technological capabilities will be cut off. The struggle between the two countries will be maintained at the level that allows them to still tap the United States. Unlike U.S.-Soviet relations during the Cold War, there is no irreconcilable ideological conflict between the United States and a China that has enthusiastically embraced the market. Sino-American relations are both cooperative and competitive. Competition between them is inevitable, but conflict is not. After the collapse of the Soviet Union, the United States and China are more likely to view each other as competitors if not adversaries. But the die has not been cast. The best possible outcome is a new understanding that when they cannot cooperate, they will coexist and allow all countries in the Pacific to grow and thrive. A stabilizing factor in their relationship is that each nation requires cooperation from and healthy competition with the other. The danger of a military conflict between China and the United States is low. Chinese leaders know that U.S. military superiority is overwhelming and will remain so for the next few decades. They will modernize their forces not to challenge America but to be able, if necessary, to pressure Taiwan by a blockade or otherwise to destabilize the economy. China's military buildup delivers a strong message to the United States that China is serious about Taiwan. However, the Chinese do not want to clash with anyone -- at least not for the next 15 to 20 years. The Chinese are confident that in 30 years their military will essentially match in sophistication the U.S. military. In the long term, they do not see themselves as disadvantaged in this fight.

# 1NR

#### Iranian proliferation causes wide-spread counter-proliferation within the Middle East that causes massive miscalculation to nuclear conflicts---independently Israel will first-strike Iran in preemptive strikes that causes quick escalation to global conflict---causes extinction.

#### Err neg on timeframe – deal successful now but war will escalate quickly if talks fail

Dahl, Reuters Nuclear Reporter, 11-14, 2013,

(Fredrik, "Iran Halts Nuclear Facilities' Expansion: IAEA", Huffington Post, PAS) [www.huffingtonpost.com/2013/11/14/iran-halts-nuclear-facilities-expansion\_n\_4274888.html?utm\_hp\_ref=politics&ir=Politics](http://www.huffingtonpost.com/2013/11/14/iran-halts-nuclear-facilities-expansion_n_4274888.html?utm_hp_ref=politics&ir=Politics) 11-14-13

VIENNA, Nov 14 (Reuters) - Since Hassan Rouhani became president, Iran has halted a rapid expansion of its uranium enrichment capacity, a U.N. inspection report showed on Thursday, in a potential boost for diplomacy to end Tehran's nuclear dispute with the West.¶ The quarterly report by the International Atomic Energy Agency (IAEA) also said no further major components had been added to a potential plutonium-producing reactor since August.¶ The marked slowdown in the growth of activities of possible use in developing nuclear bombs may be intended to back up Rouhani's warmer tone towards the West after years of worsening confrontation, and strengthen Tehran's hand in negotiations with world powers due to resume on Nov. 20.¶ Iran stopped increasing its capacity to refine uranium - which can fuel nuclear power plants but also bombs if processed much more - "when their team changed" in August, a senior diplomat said, referring to Rouhani and his administration.¶ But Israeli Prime Minister Benjamin Netanyahu - who strongly opposes any deal with Iran short of dismantling its enrichment programme - said he was "not impressed".¶ Israel, believed to be the Middle East's sole nuclear-armed power, has long warned it could use force to prevent Iran from gaining an atomic bomb.¶ "I am not impressed with reports that we hear that Iran has not expanded its nuclear facilities and the reason for that is they don't need to. They've got enough facilities, enough centrifuges to develop and to complete the fissile material which is at the core of an atomic bomb," Netanyahu said.¶ The Arak reactor, which Iran previously said it would start up in the first quarter of 2014 but later postponed, is of great concern for Western powers as it could yield weapons-grade plutonium once it is operating. It was a major sticking point in talks between Iran and the powers in Geneva last week.¶ Iran has "more or less frozen" construction of the heavy water reactor, the diplomat, familiar with the report, said.¶ The quarterly IAEA document was the first that included developments only since Rouhani took office on Aug. 3, prompting a diplomatic opening during which Iran and six major powers have made progress towards a possible nuclear deal.¶ STILL BELOW ISRAELI "RED LINE"¶ It also showed that Iran's stockpile of higher-grade enriched uranium had risen by about 5 percent to 196 kg (431 pounds) since August, largely due to a temporary halt in converting the material into reactor fuel.¶ But the amount of uranium gas enriched to a fissile concentration of 20 percent still remained below the roughly 250 kg (550 pounds) needed for a bomb if processed further - an amount that Israel has indicated is a "red line" that could trigger military action.¶ Iran's higher-grade enrichment is controversial as it is a relatively short technical step to ramp it up to the 90 percent required for making a nuclear warhead. Iran says it needs the material to fuel a medical research reactor.¶ Tehran denies Western and Israeli accusations that it is seeking nuclear weapons capability, saying it is enriching uranium only for peaceful energy. But its refusal so far to curb its nuclear programme, or open it up to unfettered IAEA inspections, has drawn tough sanctions that have severely damaged the OPEC giant's oil-dependent economy.¶ The IAEA said Iran had installed only four first-generation centrifuges - machines used to refine uranium - at its Natanz plant since August, making a total of 15,240. In the previous three-month period, May-August, it put in place an additional 1,800. Not all of the installed centrifuges are operating.¶ "Adding four means adding basically nothing. There is absolutely no technical reason. Clearly it is a choice not to increase the number of centrifuges," the senior diplomat said.¶ The report also said Iran had not installed any more advanced centrifuges, which can refine uranium must faster than the breakdown-prone IR-1 model and have also fanned concern in the West.¶ Rouhani succeeded hardliner Mahmoud Ahmadinejad in August, promising to try to settle the nuclear row and ease sanctions.¶ Negotiations between Iran and six powers - the United States, Britain, France, Germany, Russia and China - are scheduled to resume next week.¶ The powers want Iran to halt its most sensitive nuclear work and take other measures in exchange for limited sanctions relief as part of a confidence-building deal that would buy time for talks on a more far-reaching settlement. (Editing by Mark Heinrich and Robin Pomeroy)

#### B. Probability--- Their impacts are china-US tensions and civilian deaths which have been ongoing for decades---Middle East prolif is more probable because it’s one place cascading and rapid proliferation will occur and it’s a new geopolitical tension---they also don’t have A SCENARIO for global cyber-war means prefer our specific scenario.

#### AND---High risk of conflict now

Lamont, Central Connecticut State University Political Science Professor, 11-14, 2013,

(Ned, "Give Peace a Chance", Huffington Post, PAS) [www.huffingtonpost.com/ned-lamont/give-peace-a-chance\_1\_b\_4276402.html?utm\_hp\_ref=politics&ir=Politics](http://www.huffingtonpost.com/ned-lamont/give-peace-a-chance_1_b_4276402.html?utm_hp_ref=politics&ir=Politics) 11-14-13

Israeli PM Benjamin Netanyahu told his parliament yesterday that war is getting close. Former VP Dick Cheney predicted military action while appearing on ABC News last week, Romney bundler Sheldon Adelson recently threatened a nuclear strike on Iran. America has a fractured Congress that can not even agree that the sun rises in the east, but the Senate last spring gave Israel a green light to take military action against Iran by a vote of 99-0. Rather than negotiate with his Iranian counterpart this week, Secretary Kerry is negotiating with the Senate banking committee to hold off on slapping any more sanctions on Iran and instead letting the negotiations play out. A lot less chest thumping and a bit more thought about a broader relationship with a new Iranian regime is overdue.

## Impact-Turn Debate

#### They haven’t answered independent US-strike impact---our internal link evidence says that absence of negotiation, the US will first-strike Iranian facilities to prevent acquisition---causes escalation that their proliferation evidence doesn’t assume---FRAMING issue---collapse of negotiation causes hardliners to take-over which causes emboldening and aggressive military posture---their prolif evidence only assumes that Israel won’t strike, but Iranian aggression independently invites attacks.

#### Their evidence only assumes limited proliferation and attack between Iran and Israel---Iran prolif allow for wide—spread regional prolif which escalates.

#### Middle-East is uniquely different---multiple factors make conflicts likely---causes great-power intervention which exacerbates tensions---turns China and US.

Edelman et al 11 The Dangers of a Nuclear Iran, The Limits of Containment, Eric S. Edelman, Andrew F. Krepinevich Jr, and Evan Braden Montgomery JANUARY/FEBRUARY 2011, ERIC S. EDELMAN is a Distinguished Fellow at the Center for Strategic and Budgetary Assessments; he was U.S. Undersecretary of Defense for Policy in 2005-9. ANDREW F. KREPINEVICH is President of the Center for Strategic and Budgetary Assessments. EVAN BRADEN MONTGOMERY is a Research Fellow at the Center for Strategic and Budgetary Assessments, http://www.foreignaffairs.com/articles/67162/eric-s-edelman-andrew-f-krepinevich-jr-and-evan-braden-montgomer/the-dangers-of-a-nuclear-iran

The reports of the Congressional Commission on the Strategic Posture of the United States and the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, as well as other analyses, have highlighted the risk that a nuclear-armed Iran could trigger additional nuclear proliferation in the Middle East, even if Israel does not declare its own nuclear arsenal. Notably, Algeria, Bahrain, Egypt, Jordan, Saudi Arabia, Turkey, and the United Arab Emirates -- all signatories to the Nuclear Nonproliferation Treaty (NPT) -- have recently announced or initiated nuclear energy programs. Although some of these states have legitimate economic rationales for pursuing nuclear power and although the low-enriched fuel used for power reactors cannot be used in nuclear weapons, these moves have been widely interpreted as hedges against a nuclear-armed Iran. The NPT does not bar states from developing the sensitive technology required to produce nuclear fuel on their own, that is, the capability to enrich natural uranium and separate plutonium from spent nuclear fuel. Yet enrichment and reprocessing can also be used to accumulate weapons-grade enriched uranium and plutonium -- the very loophole that Iran has apparently exploited in pursuing a nuclear weapons capability. Developing nuclear weapons remains a slow, expensive, and difficult process, even for states with considerable economic resources, and especially if other nations try to constrain aspiring nuclear states' access to critical materials and technology. Without external support, it is unlikely that any of these aspirants could develop a nuclear weapons capability within a decade. There is, however, at least one state that could receive significant outside support: Saudi Arabia. And if it did, proliferation could accelerate throughout the region. Iran and Saudi Arabia have long been geopolitical and ideological rivals. Riyadh would face tremendous pressure to respond in some form to a nuclear-armed Iran, not only to deter Iranian coercion and subversion but also to preserve its sense that Saudi Arabia is the leading nation in the Muslim world. The Saudi government is already pursuing a nuclear power capability, which could be the first step along a slow road to nuclear weapons development. And concerns persist that it might be able to accelerate its progress by exploiting its close ties to Pakistan. During the 1980s, in response to the use of missiles during the Iran-Iraq War and their growing proliferation throughout the region, Saudi Arabia acquired several dozen CSS-2 intermediate-range ballistic missiles from China. The Pakistani government reportedly brokered the deal, and it may have also offered to sell Saudi Arabia nuclear warheads for the CSS-2s, which are not accurate enough to deliver conventional warheads effectively. There are still rumors that Riyadh and Islamabad have had discussions involving nuclear weapons, nuclear technology, or security guarantees. This "Islamabad option" could develop in one of several different ways. Pakistan could sell operational nuclear weapons and delivery systems to Saudi Arabia, or it could provide the Saudis with the infrastructure, material, and technical support they need to produce nuclear weapons themselves within a matter of years, as opposed to a decade or longer. Not only has Pakistan provided such support in the past, but it is currently building two more heavy-water reactors for plutonium production and a second chemical reprocessing facility to extract plutonium from spent nuclear fuel. In other words, it might accumulate more fissile material than it needs to maintain even a substantially expanded arsenal of its own. Alternatively, Pakistan might offer an extended deterrent guarantee to Saudi Arabia and deploy nuclear weapons, delivery systems, and troops on Saudi territory, a practice that the United States has employed for decades with its allies. This arrangement could be particularly appealing to both Saudi Arabia and Pakistan. It would allow the Saudis to argue that they are not violating the NPT since they would not be acquiring their own nuclear weapons. And an extended deterrent from Pakistan might be preferable to one from the United States because stationing foreign Muslim forces on Saudi territory would not trigger the kind of popular opposition that would accompany the deployment of U.S. troops. Pakistan, for its part, would gain financial benefits and international clout by deploying nuclear weapons in Saudi Arabia, as well as strategic depth against its chief rival, India. The Islamabad option raises a host of difficult issues, perhaps the most worrisome being how India would respond. Would it target Pakistan's weapons in Saudi Arabia with its own conventional or nuclear weapons? How would this expanded nuclear competition influence stability during a crisis in either the Middle East or South Asia? Regardless of India's reaction, any decision by the Saudi government to seek out nuclear weapons, by whatever means, would be highly destabilizing. It would increase the incentives of other nations in the Middle East to pursue nuclear weapons of their own. And it could increase their ability to do so by eroding the remaining barriers to nuclear proliferation: each additional state that acquires nuclear weapons weakens the nonproliferation regime, even if its particular method of acquisition only circumvents, rather than violates, the NPT. Were Saudi Arabia to acquire nuclear weapons, the Middle East would count three nuclear-armed states, and perhaps more before long. It is unclear how such an n-player competition would unfold because most analyses of nuclear deterrence are based on the U.S.-Soviet rivalry during the Cold War. It seems likely, however, that the interaction among three or more nuclear-armed powers would be more prone to miscalculation and escalation than a bipolar competition. During the Cold War, the United States and the Soviet Union only needed to concern themselves with an attack from the other. Multipolar systems are generally considered to be less stable than bipolar systems because coalitions can shift quickly, upsetting the balance of power and creating incentives for an attack. More important, emerging nuclear powers in the Middle East might not take the costly steps necessary to preserve regional stability and avoid a nuclear exchange. For nuclear-armed states, the bedrock of deterrence is the knowledge that each side has a secure second-strike capability, so that no state can launch an attack with the expectation that it can wipe out its opponents' forces and avoid a devastating retaliation. However, emerging nuclear powers might not invest in expensive but survivable capabilities such as hardened missile silos or submarine-based nuclear forces. Given this likely vulnerability, the close proximity of states in the Middle East, and the very short flight times of ballistic missiles in the region, any new nuclear powers might be compelled to "launch on warning" of an attack or even, during a crisis, to use their nuclear forces preemptively. Their governments might also delegate launch authority to lower-level commanders, heightening the possibility of miscalculation and escalation. Moreover, if early warning systems were not integrated into robust command-and-control systems, the risk of an unauthorized or accidental launch would increase further still. And without sophisticated early warning systems, a nuclear attack might be unattributable or attributed incorrectly. That is, assuming that the leadership of a targeted state survived a first strike, it might not be able to accurately determine which nation was responsible. And this uncertainty, when combined with the pressure to respond quickly, would create a significant risk that it would retaliate against the wrong party, potentially triggering a regional nuclear war. Most existing nuclear powers have taken steps to protect their nuclear weapons from unauthorized use: from closely screening key personnel to developing technical safety measures, such as permissive action links, which require special codes before the weapons can be armed. Yet there is no guarantee that emerging nuclear powers would be willing or able to implement these measures, creating a significant risk that their governments might lose control over the weapons or nuclear material and that nonstate actors could gain access to these items. Some states might seek to mitigate threats to their nuclear arsenals; for instance, they might hide their weapons. In that case, however, a single intelligence compromise could leave their weapons vulnerable to attack or theft. Meanwhile, states outside the Middle East could also be a source of instability. Throughout the Cold War, the United States and the Soviet Union were engaged in a nuclear arms race that other nations were essentially powerless to influence. In a multipolar nuclear Middle East, other nuclear powers and states with advanced military technology could influence -- for good or ill -- the military competition within the region by selling or transferring technologies that most local actors lack today: solid-fuel rocket motors, enhanced missile-guidance systems, warhead miniaturization technology, early warning systems, air and missile defenses. Such transfers could stabilize a fragile nuclear balance if the emerging nuclear powers acquired more survivable arsenals as a result. But they could also be highly destabilizing. If, for example, an outside power sought to curry favor with a potential client state or gain influence with a prospective ally, it might share with that state the technology it needed to enhance the accuracy of its missiles and thereby increase its ability to launch a disarming first strike against any adversary. The ability of existing nuclear powers and other technically advanced military states to shape the emerging nuclear competition in the Middle East could lead to a new Great Game, with unpredictable consequences.

#### Prolif causes mid-east war---multiple reasons.

Collins 13 Iran is Not the Problem, Wider Proliferation Is, Brian C. Collins, Lieutenant Colonel Brian C. Collins is a USMC Infantry and Middle East/North Africa Regional Affairs Officer currently assigned to Headquarters, Marine Corps, October 31, 2013, http://smallwarsjournal.com/jrnl/art/iran-is-not-the-problem-wider-proliferation-is

One danger of increased proliferation could well be the commencement of an accelerated race to go nuclear across the Middle East. Iran is already perceived to be a threat to many other regional actors and it would be reasonable to assume that, should Tehran gain a nuclear capability, neighbors will want one as well. The Saudis, Emiratis, and Jordanians will undoubtedly be first in line. Diplomatically it would be prudent to begin honest discussions of security guarantees (or lack thereof). Even with steadfast guarantees, the threatening image projected by Iran could also result in the hardening of alliances. These alliances would likely become more openly hostile and confrontational. Such shifts would only be compounded by the tremendous social and political upheavals the region is currently experiencing. The states of the so-called Shia crescent could bandwagon with an ascendant Iran, forcing a stand-off between Iran, Iraq, and what's left of Syria on the one side, and the Gulf States, Saudi Arabia, and Jordan on the other. With each bloc in greater competition with one another and willing to take increasingly provocative actions in defense of their interests, open conflict may ensue. An aspect of positive engagement includes the provision of a meaningful presence, both physical and virtual, to moderate potential behavior and prepare for contingency. Another aspect to maintaining regional stability remains the effective management of the competition between Israel and those states seeking to constrain its aspirations of survival and growth. Here, Israel’s maintenance of a qualitative military edge has been vital to preserving even the slightest modicum of peace. Israelis increasingly view themselves as being held hostage by the specter of annihilation, and a strong physical deterrent has done much practically and psychologically to ameliorate attendant fears. A third consequence of proliferation, therefore, is that the Israeli advantage would, if not in real terms but in perceived terms, be threatened should nuclear weapons technologies and capabilities spread throughout the greater Middle East. Again, the building of assurances and trust to allay Israeli fears of abandonment should begin. Perhaps the greatest fear, however, is a fourth potential consequence of an Iranian capability; the increased chance for proxy conflict. The Iranian regime already possesses a capable network of surrogates ranging from those available through their own government resources within the Ministry of Intelligence and Security (MOIS), Iranian Revolutionary Guards Corps (IRGC), and Quds force, to vassals such as Hezbollah and Hamas. Balanced against the Iranians would be the instruments of opposing states. Proxies unleashed upon one another, even if limited, could be incredibly de-stabilizing. Add to the mix the potential nightmare of uncontrolled transfer of advanced technology to other revisionist third parties--state, non-state, and quasi-state--and a potentially lethal mix of conditions results. Under these circumstances, a regional issue could quickly escalate to one of global proportion. Capabilities must be developed to detect, deter, disrupt, and defeat any organization seeking to engage in incredibly dangerous acts of nuclear terror.

#### YES Israel will retaliate

Sagan 07

(Scott Sagan is a professor of political science at Stanford University ”A Nuclear Iran”, Journal of international affairs, Spring/summer 2007, Vol. 60 Issue 2, Accessed via GMU Libraries, Last Accessed 6/25/13) ELJ

**Richard Betts:** Now we'll open the forum to audience questions. **Question:** Two names that weren't mentioned with regard to Iran developing nuclear weapons were Israel and Saudi Arabia. Could you both comment on possible reactions of those two actors? **Scott Sagan:** Well, **both the Israelis and the Saudis have spoken about the danger of Iran acquiring nuclear weapons, but they have also spoken by their actions**. The **Israelis have commented both in saying that** they will not accept a nuclear Iran and in starting to build submarine forces that could house nuclear weapons at sea, so they are able to retaliate even if Israel itself was destroyed first. That is, **they are working to reduce the vulnerability of their nuclear arsenal**. **These actions** **suggest** that the **Israelis** themselves ha**ve not yet decided whether they are going to use military force to reduce the threat,** or accept Ken Waltz's arguments and live with a nuclear Iran. Either option is hard for them.

## T

#### No reasonability standards mean you evaluate T in competing interpretation because it’s the most objective standards---that means debate’s over because they’ve conceded our impacts and they don’t have counter-standards.

#### Our interpretation is the affirmation should restrict an existing war powers authority of the president by amending the legislation from which the authority originates. Our interpretation allows oversight, transparency, limiting the types of targeted killing that can occur, restrictions on offensive cyber operations, and review courts---this was CONCEDED---means no new answer---they might have defined increase, but it doesn’t make sense---increase statutory restrictions as WHOLE means you have to establish already-existing mechanisms---prefer neg because we defined phrases, not words which is more resolutional and holistic.

#### The affs we limit out are affs that restrict presidential authority that is NOT granted by a congressional statute, such as Liberty’s aff that gives Pakistan a veto over drone strikes in their country, an aff that just says ban signature strikes, an aff that bans forced feeding in indefinite detention, and any aff based on a presidential assertion of power that doesn’t originate from a statute because neg can’t predictably research those affs.

#### Topical version of the aff---Cyber is the WPR and the NDAA

Jay P. Kesan, Professor, H. Ross & Helen Workman Research Scholar, and Director of the Program ¶ in Intellectual Property & Technology Law, University of Illinois College of Law. and Carol M. Hayes, Research Fellow, University of Illinois College of Law. After receiving her J.D. from ¶ the University of Illinois, Carol Hayes served as a Christine Mirzayan Science and Technology Policy Graduate Fellow at the National Academy of Sciences in Fall 2010.¶ “MITIGATIVE COUNTERSTRIKING:SELF-DEFENSE ¶ AND DETERRENCE IN CYBERSPACE,” Harvard Journal of Law & Technology¶ Volume 25, Number 2 Spring 2012. http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech415.pdf

Additionally, Congress used § 954 to clear up several questions about the President’s authority, rules governing cyberattacks, and the ¶ role of the DOD. In a very short section, Congress stated that the President has the authority to direct the DOD to “conduct offensive operations in cyberspace to defend our Nation, Allies and interests,” while applying the same rules that govern kinetic capabilities, and subject to ¶ the limitations placed on the President by the War Powers Resolution.517 In § 954, Congress recognized the importance of cyberspace ¶ to future international conflicts and the need to codify rules in advance. The question of Congress’s position on the President’s authority to direct formal cyberwarfare activities is thus partly answered by § 954 of the NDAA. Given § 954’s reference to offensive cyber operations undertaken in defense, it is likely that Congress would approve military use of active defense as described in this Article. However, ¶ these provisions address only the President’s authority to order the ¶ DOD to use cyber capabilities in a formal military context, leaving ¶ unanswered the issue of possible federal involvement in protecting ¶ privately held CNI. ¶ Congress has now explicitly spoken on the President’s authority ¶ to direct military cyber activities, but has not yet addressed the President’s authority to exercise control over cybersecurity matters in the ¶ private sector outside of the context of national emergencies and wartime. Therefore, under Justice Jackson’s test in Youngstown, the President may have intermediate authority on matters involving ¶ cybersecurity and the private sector, though we argue that setting out ¶ guidelines in advance of a crisis would be preferable to ad hoc presidential management of individual issues as they arise.

#### They’ve conceded the bidirectionality that’s our Horowitz evidence---not using clear original congressional statue allows for commander and chief powers that functionally increases presidential authority---that makes stable offense impossible.

#### Plan vagueness begets authorization – related legislation sparks confusion and provides territory for executive expansion, crushing limits – THE CLOSER, THE FARTHER \*\*\*

Graham Cronogue, Duke University School of Law, J.D. expected 2013; A NEW AUMF: DEFINING COMBATANTS IN THE ¶ WAR ON TERROR, DUKE JOURNAL OF COMPARATIVE & INTERNATIONAL LAW [Vol. 22:377 2012] http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1294&context=djcil

Second, the AUMF’s language illustrates congressional acquiescence or approval of broad presidential authority to use force. “[T]he enactment of legislation closely related to the question of the President’s authority in a particular case which evinces legislative intent to accord the President broad discretion may be considered to ‘invite’ ‘measures on independent presidential responsibility.’”45 The language in the AUMF is very similar to ¶ declarations of war and authorizations, in which presidents have exercised ¶ plenary power in determining the means and type of force.46 In these ¶ “perfect” wars, “all the members act[ed] under a general authority, and all ¶ the rights and consequences of war attach to their condition.”47 For ¶ instance, the Gulf of Tonkin Resolution allowed the President to “take all ¶ necessary measures” and was used as broad authority to wage combat and ¶ detain enemies.48 Similarly, the AUMF allows for the use of “all necessary ¶ and appropriate force.” Presidents have commonly exercised broad authority under similar grants of power, and Congress’s failure to act in limiting these powers here suggests acquiescence to this interpretation.49¶ More convincingly than in Dames & Moore, where Congress failed to ¶ object to executive action, there are numerous comments from the ¶ legislature that the President should have broad authority under the ¶ AUMF.50 Given these statements and Congress’s ample opportunity to limit the scope or type of force, Congress must have acquiesced to past executive practice and interpretation.

#### Specific language should hold priority – Constitution’s ONLY use of “war” supports our distinction between Commander-in-Chief and war powers authority\*\*\*

R. Andrew Smith, Breaking the Stalemate: The Judiciary's Constitutional Role in Disputes over the War Powers, 41 Val. U. L. Rev. 1517¶ (2007). http://scholar.valpo.edu/cgi/viewcontent.cgi?article=1194&context=vulr

The text of Article II states that the president acts as the Commander in Chief of the Army, Navy, and the Militia of the several states.45 However, the only provision in the Constitution using the word “war” is in the definition of legislative war power.46 A reading of the ¶ Constitution may generally indicate that the president’s war power only activates when Congress issues a declaration of war; however, the ¶ president has used military force under both declarations of war and ¶ congressional resolutions authorizing military action.47

#### It’s not the same thing – totally separate realms

ConLawProf July 29, 2010. “Groups Sue to Represent Government-Designated Terrorist,” http://lawprofessors.typepad.com/conlaw/separation\_of\_powers/page/9/

But the report's conclusion that the administration "will enshrine permanently within the law" certain policies and practices is perhaps overly dire. For example, some of President Obama's positions have received push-back from Congress; and President Obama has repeatedly signaled that Congress matters--that he will respect Congress in acting under the national security constitution. Unlike President Bush, President Obama has relied only sparsely on inherent executive authority under Article II, instead looking first to congressional authorization for his actions. His consistent reliance on the AUMF before any inherent Article II authority is a good example. Moreover, some of the Obama administration's positions have received push-back from the courts. Most recently, federal courts have rejected the administration's more outlandish positions in Guantanamo habeas cases. (The administration itself scaled back its prior expansive definition of a detainable person.) The full Ninth Circuit now has a chance to reject the administration's extreme position on the state secrets privilege in the Jeppesen case. Finally, the administration's actions alone simply cannot "enshrine permanently in the law" those extreme policies and positions that never reach Congress or the courts, especially for a president who claims to rely sparsely on inherent Article II authority. In these areas the President at most establishes an executive precedent. The practice and precedent of President Obama will be important, to be sure, in interpreting future executive authority, but this is not "enshrin[ing] permanently in the law." (This kind of past practice doesn't bind a future executive to also adopt it. Instead, at most, it sets an outer limit to presidential authority with reference to what President Obama did.)

## OCO violation

#### Now the OCO violation---extend our Belk evidence---PLAN IS NOT offensive cyber oeprations because it doesn’t affect US ability to target MILITARY capabilities---this is a clear delination.

#### Your interpretation goes OUR way---says that there’s a specific difference between cyber exploitation and offensive operations---literally says that only MILITARY operations are topical---they would allow ANYTHING that the DOD does AND allow for informational or scanning operations that explodes the mechanism limits.

#### You also don’t meet your interpretation---says that exploitation is scanning ADVERSARY information targets---they only do civilians which doesn’t affect opponent’s military capabilities.

#### But we’ve limit out exploitation anyways because Cyber-exploitation is not T

Tsagourias 2012

[Nicolas Tsagourias is a professor of International Law at the University of Sheffield, joining the University in 2012 from the University of Glasgow where he was Professor of International Law and Security. He completed his law studies at the University of Thessaloniki in Greece, obtaining an LL.M. from the University of Bristol and his Ph.D from the University of Nottingham. “Cyber attacks, self-defence and the problem of attribution,” Journal of Conﬂict & Security Law (2012), Vol. 17 No. 2, 229–244, Ebsco ]jap

What distinguishes a cyber attack as defined above from other cyber provocations¶ such as cyber exploitations is its harmful effect, in that a cyber attack¶ makes the targeted system unavailable or compromises its integrity and authenticity.¶ 6 The immediate question is whether such effects are in themselves sufficient¶ to trigger self-defence in the absence of other material and/or human harm.

#### Prefer narrow definitions – scanning isn’t offensive

Belk and Noyes 12

[Robert and Matthew, Robert is, studying international and global affairs at the Harvard Kennedy School.. Following graduation, he is scheduled to report to the Naval Operations staff in the Pentagon to develop and execute Navy network and cybersecurity policy, Matthew studies international security policy and is a senior associate with the cybersecurity practice at Good Harbor Consulting.. He has a degree in Computer Science and Applied Computational Mathematics from the University of Washington. “On the Use of Offensive Cyber Capabilities A Policy Analysis on Offensive US Cyber Policy”, <http://belfercenter.ksg.harvard.edu/files/cybersecurity-pae-belk-noyes.pdf>, Accessed 9-1-13]jap-lkm

Scanning poses few significant ethical concerns. It causes no harm to the “victim,” and scanning can be conducted for very benevolent purposes (e.g. to inform a victim that he/she is vulnerable to cyber attacks ) . Only under the broadest notions of privacy could one view scanning as offensive, because the act of connecting a computer system to a publically accessible network certainly suggests an acceptance for communication based upon basic protocols. Individuals acts of scanning conducted as part of an operation can result in a denial of service type attack. However, such an action would be amount to a cyber attack in that it causes disruption.

#### Intrusions aren’t offensive cyber operations – no harm is caused

Belk and Noyes 12

[Robert and Matthew, Robert is, studying international and global affairs at the Harvard Kennedy School.. Following graduation, he is scheduled to report to the Naval Operations staff in the Pentagon to develop and execute Navy network and cybersecurity policy, Matthew studies international security policy and is a senior associate with the cybersecurity practice at Good Harbor Consulting.. He has a degree in Computer Science and Applied Computational Mathematics from the University of Washington. “On the Use of Offensive Cyber Capabilities A Policy Analysis on Offensive US Cyber Policy”, <http://belfercenter.ksg.harvard.edu/files/cybersecurity-pae-belk-noyes.pdf>, Accessed 9-1-13]jap-lkm

A cyber intrusion is the unauthorized access of a computer system. Many computer systems are ineffectively protected . Gaining unauthorized access may be a trivial task that does not require any sophisticated capabilities, but yet may have potentially severe implications. We have isolated this category of external actions from attacks or those with information effects (such as information collection), because, even without any exploitation or harm being caused, the intrusion in of itself poses ethical and legal complications. **It is important to recognize that while many external cyber actions require an intrusion (particularly cyber attacks and cyber force), not all do**. For example DDoS does not require an intrusion.

#### The biggest policy challenges in the literature stem from cyber attacks – not the rest. We give them more than enough ground

Belk and Noyes 12

[Robert and Matthew, Robert is, studying international and global affairs at the Harvard Kennedy School.. Following graduation, he is scheduled to report to the Naval Operations staff in the Pentagon to develop and execute Navy network and cybersecurity policy, Matthew studies international security policy and is a senior associate with the cybersecurity practice at Good Harbor Consulting.. He has a degree in Computer Science and Applied Computational Mathematics from the University of Washington. “On the Use of Offensive Cyber Capabilities A Policy Analysis on Offensive US Cyber Policy”, <http://belfercenter.ksg.harvard.edu/files/cybersecurity-pae-belk-noyes.pdf>, Accessed 9-1-13]jap-lkm

Cybersecurity expert Herb Lin has described this category as the most challenging for policy makers saying, “Most cyber actions are in this domain and responding to these actions is by far the most substantial policy challenges in cybersecurity.” This category is the most challenging because external cyber actions rising to the level of a use of force are clearly governed by existing standards regarding the use of force; external cyber actions with consequences less severe than attack are largely permissible under international law, and even protected in some cases. Given the complexity of this category, a full analysis requires consideration of intent and deeper situational aspects than the other categories of external cyber we have defined. A full analysis is beyond the scope of this project. Instead, we limit the analysis at present to a general overview of cyber attack, and specific analysis of perhaps the most permissible form of cyber attack—defensive cyber counter-attacks against computer systems presently engaged in conducting a cyber attack.