# R1, MN ST, Open Source

# 1NC

### 1

#### Interpretation: restriction means a prohibition – this is distinct from reporting requirements

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

3. The ordinary definition of the term "restrictions" also does not include the reporting and monitoring or supervising terms and conditions that are included in the 2001 Stipulation. Black's Law Dictionary, 'fifth edition,(1979) defines "restriction" as; A limitation often imposed in a deed or lease respecting the use to which the property may be put. The term "restrict' is also cross referenced with the term "restrain." Restrain is defined as; To limit, confine, abridge, narrow down, restrict, obstruct, impede, hinder, stay, destroy. To prohibit from action; to put compulsion on; to restrict; to hold or press back. To keep in check; to hold back from acting, proceeding, or advancing, either by physical or moral force, or by interposing obstacle, to repress or suppress, to curb. In contrast, the terms "supervise" and "supervisor" are defined as; To have general oversight over, to superintend or to inspect. See Supervisor. A surveyor or overseer. . . In a broad sense, one having authority over others, to superintend and direct. The term "supervisor" means an individual having authority, in the interest of the employer, to hire, transfer, suspend, layoff, recall, promote, discharge, assign, reward, or discipline other employees, or responsibility to direct them, or to adjust their grievances, or effectively to recommend such action, if in connection with the foregoing the exercise of such authority is not of a merely routine or clerical nature, but required the use of independent judgment. Comparing the above definitions, it is clear that the definition of "restriction" is very different from the definition of "supervision"-very few of the same words are used to explain or define the different terms. In his 2001 stipulation, Mr. Kincheloe essentially agreed to some supervision conditions, but he did not agree to restrict his license.

#### “Statutory restrictions” means congress

**Mortenson 11** (Julian Davis Assistant Professor, University of Michigan Law School, “Review: Executive Power and the Discipline of History Crisis and Command: The History of Executive Power from George Washington to George W. Bush John Yoo. Kaplan, 2009. Pp vii, 524,” Winter 2011, University of Chicago Law Review 78 U. Chi. L. Rev. 377)

At least two of Yoo's main examples of presidential power are actually instances of presidential deference to statutory restrictions during times of great national peril. The earliest is Washington's military suppression of the Whiskey Rebellion (III, pp 66-72), a domestic disturbance that Americans viewed as implicating adventurism by European powers and threatening to dismember the new nation. n60 The Calling Forth Act of 1792 n61 allowed the President to mobilize state militias under federal control, but included a series of mandatory procedural checks--including judicial [\*399] approval--that restricted his ability to do so. n62 Far from defying these comprehensive restrictions at a moment of grave crisis, Washington satisfied their every requirement in scrupulous detail. He issued a proclamation ordering the Whiskey Rebels to disperse. n63 When they refused to do so, he submitted a statement to Justice James Wilson of the Supreme Court describing the situation in Pennsylvania and requesting statutory certification. n64 Only when Wilson issued a letter precisely reciting the requisite statutory language (after first requiring the President to come back with authentication of underlying reports and verification of their handwriting n65) did Washington muster the troops. n66 Washington's compliance with statutory restrictions on his use of force continued even after his forces were in the field. Because Congress was not in session when he issued the call-up order, Washington was authorized by statute to mobilize militias from other states besides Pennsylvania--but only "until the expiration of thirty days after the commencement of the ensuing [congressional] session." n67 When it became clear that the Pennsylvania campaign would take longer than that, Washington went back to Congress to petition for extension of the statutory time limit that would otherwise have required him to [\*400] disband his troops. n68 Far from serving as an archetypal example of presidential defiance, the Whiskey Rebellion demonstrates exactly the opposite. FDR's efforts to supply the United Kingdom's war effort before Pearl Harbor teach a similar lesson. During the run-up to America's entry into the war, Congress passed a series of Neutrality Acts that supplemented longstanding statutory restrictions on providing assistance to foreign belligerents. Despite these restrictions, FDR sent a range of military assistance to the future Allies. n69 Yoo makes two important claims about the administration's actions during this period. First, he claims the administration asserted that "[a]ny statutory effort by Congress to prevent the President from transferring military equipment to help American national security would be of 'questionable constitutionality'" (III, p 300). Second, he suggests that American military assistance in fact violated the neutrality statutes (III, pp 295-301, 310, 327-28).

#### Violation: the plan is an affirmative obligation, not a restriction.

David J. Barron & Martin S. Lederman, Harvard Law Review, February 2008. “THE COMMANDER IN CHIEF AT THE LOWEST EBB — A CONSTITUTIONAL HISTORY,” http://www.harvardlawreview.org/media/pdf/barron\_lederman2.pdf

This compromise did not address Browning’s separation of powers ¶ concern. But it did make the bill more palatable from the Administration’s perspective. In fact, to the chagrin of the Radical Republicans,290 the Act proved difficult to enforce, partly because the Attorney ¶ General pointedly refused to offer guidance on its meaning to district ¶ attorneys.291 Nevertheless, the bill was, as Browning knew, a remarkable example of a law regulating the discretion of the Commander in ¶ Chief. It dealt specifically with a tactic to be applied directly to the ¶ enemy. It imposed not a restriction, but an affirmative obligation on the President, because Congress perceived him as being insufficiently ¶ aggressive. And it was enacted not as a background, framework statute to govern all wars, but in the midst of a particular war, as a corrective to what Congress saw as an inadequate executive policy toward a ¶ particular foe. Nevertheless, as far as we have been able to discern, no ¶ executive branch official — including the President and his Attorney ¶ General — contended at any point in the extensive debate that the Act ¶ unconstitutionally interfered with the President’s constitutional war ¶ authority.292

#### Vote neg

#### 1. limits – they make the mechanism of the topic limitless - the Aff doesn’t have to actually decrease the presidents authority for war, they just add obligations to the authority, any form of notification becomes topical

#### 2. ground – they pike out of links to prez powers –

#### Limits are key tos clash and education – we can’t prepare without a predictable focus for the debate

### 2

#### Limit will be raised now—Boehner will hold a vote but political capital is key

USA Today, 10/4 (Aamer Madhani, “Obama hammers Boehner on shutdown, debt ceiling”, 10/4/2013http://www.usatoday.com/story/news/politics/2013/10/03/obama-boehner-shutdown-debt-limit/2918545/)

In perhaps a small sign of progress in the impasse, Boehner signaled on Thursday that he may be willing to hold a vote to raise the debt ceiling even if Obama refuses to agree to the Republican demand of delaying implementation of the president's signature health care law by a year. Jared Bernstein, who served as top economic adviser to Vice President Biden in the first term, said that by taking the debt ceiling debate off the table. Boehner could potentially gain some negotiating leverage in the budget fight, but he does it at the risk of the Republican base "throwing him under the bus." Bernstein said the best way forward for the White House is continuing to be "very explicit" with Boehner that it remains open on long term budget issues, while standing pat on the condition that a short-term budget and debt limit vote is passed without conditions. "You essentially tell him by putting clean votes on the floor right now buys a ticket to robust negotiations on the other side," Bernstein said. "At the point, it's perfectly legitimate for him to go into any negotiation with any asks that he wants." Even as Boehner showed signs of flexibility on a debt limit vote, House Republicans continued to pursue a piecemeal shutdown strategy to pass targeted funding bills for popular government services. House Majority Leader Eric Cantor, R-Va., wrote to rank-and-file Republicans in a memo Thursday that he was confident Obama and congressional Democrats would eventually bow to negotiations if Republicans hold the line.

#### Plan destroys Obama’s credibility – makes it impossible for him to get anything through Congress

Seeking Alpha 9-10, 9-10-2013, “Syria Could Upend Debt Ceiling Fight,” http://seekingalpha.com/article/1684082-syria-could-upend-debt-ceiling-fight

Unless President Obama can totally change a reluctant public's perception of another Middle-Eastern conflict, it seems unlikely that he can get 218 votes in the House, though he can probably still squeak out 60 votes in the Senate. This defeat would be totally unprecedented as a President has never lost a military authorization vote in American history. To forbid the Commander-in-Chief of his primary power renders him all but impotent. At this point, a rebuff from the House is a 67%-75% probability. I reach this probability by looking within the whip count. I assume the 164 declared "no" votes will stay in the "no" column. To get to 218, Obama needs to win over 193 of the 244 undecided, a gargantuan task. Within the "no" column, there are 137 Republicans. Under a best case scenario, Boehner could corral 50 "yes" votes, which would require Obama to pick up 168 of the 200 Democrats, 84%. Many of these Democrats rode to power because of their opposition to Iraq, which makes it difficult for them to support military conflict. The only way to generate near unanimity among the undecided Democrats is if they choose to support the President (recognizing the political ramifications of a defeat) despite personal misgivings. The idea that all undecided Democrats can be convinced of this argument is relatively slim, especially as there are few votes to lose. In the best case scenario, the House could reach 223-225 votes, barely enough to get it through. Under the worst case, there are only 150 votes. Given the lopsided nature of the breakdown, the chance of House passage is about one in four. **While a failure in the House would put action against Syria in limbo, I have felt that the market has overstated the impact of a strike there**, which would be limited in nature. Rather, **investors should focus on the profound ripple through the power structure in Washington, which would greatly impact impending battles over** spending and **the debt ceiling**. Currently, **the government** loses spending authority on September 30 while it **hits the debt ceiling by the middle of October. Markets have generally felt that Washington will once again strike a last-minute deal and avert total catastrophe**. Failure in the Syrian vote could change this**. For the Republicans to beat Obama on a President's strength (foreign military action), they will likely be emboldened that they can beat him on domestic spending issues.**  **Until now, consensus has been that the two sides would compromise** to fund the government at sequester levels while **passing a $1 trillion stand**

#### Political capital is finite and key --- the plan trades off

Moore, 9/10 --- Guardian's US finance and economics editor (Heidi, 9/10/2013, “Syria: the great distraction; Obama is focused on a conflict abroad, but the fight he should be gearing up for is with Congress on America's economic security,” <http://www.theguardian.com/commentisfree/2013/sep/10/obama-syria-what-about-sequester)>)

Before President Obama speaks to the nation about Syria tonight, take a look at what this fall will look like inside America. There are 49 million people in the country who suffered inadequate access to food in 2012, leaving the percentage of "food-insecure" Americans at about one-sixth of the US population. At the same time, Congress refused to pass food-stamp legislation this summer, pushing it off again and threatening draconian cuts. The country will crash into the debt ceiling in mid-October, which would be an economic disaster, especially with a government shutdown looming at the same time. These are deadlines that Congress already learned two years ago not to toy with, but memories appear to be preciously short. The Federal Reserve needs a new chief in three months, someone who will help the country confront its raging unemployment crisis that has left 12 million people without jobs. The president has promised to choose a warm body within the next three weeks, despite the fact that his top pick, Larry Summers, would likely spark an ugly confirmation battle – the "fight of the century," according to some – with a Congress already unwilling to do the President's bidding. Congress was supposed to pass a farm bill this summer, but declined to do so even though the task is already two years late. As a result, the country has no farm bill, leaving agricultural subsidies up in the air, farmers uncertain about what their financial picture looks like, and a potential food crisis on the horizon. The two main housing agencies, Fannie Mae and Freddie Mac, have been in limbo for four years and are desperately in need of reform that should start this fall, but there is scant attention to the problem. These are the problems going unattended by the Obama administration while his aides and cabinet members have been wasting the nation's time making the rounds on television and Capitol Hill stumping for a profoundly unpopular war. The fact that all this chest-beating was for naught, and an easy solution seems on the horizon, belies the single-minded intensity that the Obama White House brought to its insistence on bombing Syria. More than one wag has suggested, with the utmost reason, that if Obama had brought this kind of passion to domestic initiatives, the country would be in better condition right now. As it is, public policy is embarrassingly in shambles at home while the administration throws all of its resources and political capital behind a widely hated plan to get involved in a civil war overseas. The upshot for the president may be that it's easier to wage war with a foreign power than go head-to-head with the US Congress, even as America suffers from neglect. This is the paradox that President Obama is facing this fall, as he appears to turn his back on a number of crucial and urgent domestic initiatives in order to spend all of his meager political capital on striking Syria. Syria does present a significant humanitarian crisis, which has been true for the past two years that the Obama administration has completely ignored the atrocities of Bashar al-Assad. Two years is also roughly the same amount of time that key domestic initiatives have also gone ignored as Obama and Congress engage in petty battles for dominance and leave the country to run itself on a starvation diet imposed by sequestration cuts. Leon Panetta tells the story of how he tried to lobby against sequestration only to be told: Leon, you don't understand. The Congress is resigned to failure. Similarly, those on Wall Street, the Federal Reserve, those working at government agencies, and voters themselves have become all too practiced at ignoring the determined incompetence of those in Washington. Political capital – the ability to horse-trade and win political favors from a receptive audience – is a finite resource in Washington. Pursuing misguided policies takes up time, but it also eats up credibility in asking for the next favor. It's fair to say that congressional Republicans, particularly in the House, have no love for Obama and are likely to oppose anything he supports. That's exactly the reason the White House should stop proposing policies as if it is scattering buckshot and focus with intensity on the domestic tasks it wants to accomplish, one at a time. The president is scheduled to speak six times this week, mostly about Syria. That includes evening news interviews, an address to the nation, and numerous other speeches. Behind the scenes, he is calling members of Congress to get them to fall into line. Secretary of State John Kerry is omnipresent, so ubiquitous on TV that it may be easier just to get him his own talk show called Syria Today. It would be a treat to see White House aides lobbying as aggressively – and on as many talk shows – for a better food stamp bill, an end to the debt-ceiling drama, or a solution to the senseless sequestration cuts, as it is on what is clearly a useless boondoggle in Syria. There's no reason to believe that Congress can have an all-consuming debate about Syria and then, somehow refreshed, return to a domestic agenda that has been as chaotic and urgent as any in recent memory. The President should have judged his options better. As it is, he should now judge his actions better.

#### Failure to raise the debt ceiling causes global economic collapse

Popper 10/3 (Nathaniel, NYT, 10/3/13, “How a Debt Ceiling Crisis Could Do More Harm Than the Shutdown”, http://www.nytimes.com/2013/10/04/us/politics/how-debt-ceiling-could-do-more-harm-than-the-impasse-in-congress.html?\_r=0#h[], zzx)

The impasse in Congress this week has overshadowed the fact that the government is fast approaching its borrowing limit — or debt ceiling — later this month. Most economists and investors view the debt ceiling as a much more significant issue for the economy, with the potential to set off a global financial crisis. What is all the concern about? Here is an attempt to answer the basic questions. Q. What is the debt ceiling? A. Congress has long set an upper limit on the amount of money that the United States can borrow by selling Treasury bonds. That cap has been raised many times because the government regularly spends more than it brings in, forcing it to borrow more and more money to pay the bills. Most recently, in August 2011, Congress voted to raise the limit to $16.7 trillion. The government actually hit that threshold in May. But since then, the Treasury Department has used “extraordinary measures” to continue borrowing money while staying under the limit. Among other things, Treasury has not made new investments with money from the retirement funds it oversees for the Postal Service. Q. What happens on Oct. 17? A. Treasury Secretary Jacob J. Lew has said that on that day his department will run out of tricks to stay under the debt ceiling, making it impossible to borrow any more money. While new tax revenue will continue coming in, if the government cannot borrow, then it will not be able to pay all of the bills due that day. In a letter sent Tuesday to Representative John A. Boehner, the House speaker, Mr. Lew estimated that on Oct. 17 the government would have $30 billion on hand, indicating that its normal daily expenditures were about $60 billion. Q. Does the Treasury Department have any options to keep paying some or all of its bills at that point? A. The inspector general of the Treasury Department said in a 2012 report that when the department approached the debt ceiling in the past it considered multiple contingency plans, including selling the government’s gold or its portfolio of student loans and reducing payments across the board by a set amount. Both alternatives were deemed to be impossible. The report also said that Treasury officials determined that they could not choose to issue some checks while ignoring others. The only feasible option, according to the report, would be to delay payments until an entire day’s obligations could be paid at one time. Q. How quickly would big government bills come due? A. A payment for $12 billion in Social Security benefits is due on Oct. 23. On Oct. 31, the government is due to make $6 billion in interest payments on bonds it has already issued. If it missed any of its payments, the government would default on its obligations. If it missed an interest payment, it would default on its debt, which is considered particularly serious. Q. Why is there such concern about the interest payments on Treasury bonds? A. At the most basic level, if the government shows any hesitation in making scheduled interest payments on its outstanding bonds, investors will demand higher interest payments when the government borrows money in the future. That would add significantly to the federal budget. Treasury bonds are also used as a benchmark against which most other financial assets are priced. If the government was forced to pay higher interest rates, the borrowing costs for businesses and homeowners would rise as well. This would lead to less borrowing, which would put a brake on economic growth. Banks, meanwhile, already have large holdings of Treasury bonds. If the value of those bonds suddenly dropped, banks would have less money on hand and would be less likely to lend to one another, potentially causing a freeze in the credit markets like the one in 2008. More broadly, because investors have long believed that the United States government would always be able to pay its bills, Treasury bonds have become the bedrock of the global financial system and the dollar has become the most widely used currency in the world. If investors come to doubt the ability of the United States to pay its debt, the dollar could lose its special status and the basic plumbing of the financial system could become jammed. As the Treasury Department put it in a report released Thursday, “a default would be unprecedented and has the potential to be catastrophic.” Q. Is it possible the United States would truly default? A. Some investors and legal scholars believe that the president would be required to make interest payments on its bonds even if Congress failed to lift the debt ceiling because of the 14th Amendment, which says that “the validity of the public debt of the United States, authorized by law, including debts incurred for payment of pensions and bounties for services in suppressing insurrection or rebellion, shall not be questioned.” President Obama has said he does not think the Constitution grants him that authority. At the very least, many investors think that the Treasury Department would make debt payments the top priority, potentially buying time before the government actually defaulted on its debt. Q. Have we reached this point before? A. In the summer of 2011, Republicans hesitated to lift the debt ceiling until the last minute but ultimately relented. In 1979, there was a similar standoff, and it went so close to the wire that the Treasury Department accidentally failed to make one interest payment. But the government has never knowingly failed to fulfill its financial obligations. Q. Is Wall Street betting that the country will actually default? A. When investors believe a default is likely, the stock market will almost certainly plunge. So far, the markets have suggested that Congress will ultimately come to an agreement, but the mood is growing darker. On Thursday, the Standard & Poor’s 500-stock index had its worst day in more than a month.

**Nuclear war.**

Cesare Merlini 11, nonresident senior fellow at the Center on the United States and Europe and chairman of the Board of Trustees of the Italian Institute for International Affairs (IAI) in Rome. He served as IAI president from 1979 to 2001. Until 2009, he also occupied the position of executive vice chairman of the Council for the United States and Italy, which he co-founded in 1983. His areas of expertise include transatlantic relations, European integration and nuclear non-proliferation, with particular focus on nuclear science and technology. A Post-Secular World? Survival, 53:2, 117 – 130

Two neatly opposed scenarios for the future of the world order illustrate the range of possibilities, albeit at the risk of oversimplification. The first scenario entails the premature crumbling of the post-Westphalian system. One or more of the acute tensions apparent today evolves into an open and traditional conflict between states, perhaps even involving the use of nuclear weapons. The crisis might be triggered by a collapse of the global economic and financial system, the vulnerability of which we have just experienced, and the prospect of a second Great Depression, with consequences for peace and democracy similar to those of the first. Whatever the trigger, the unlimited exercise of national sovereignty, exclusive self-interest and rejection of outside interference would self-interest and rejection of outside interference would likely be amplified, emptying, perhaps entirely, the half-full glass of multilateralism, including the UN and the European Union. Many of the more likely conflicts, such as between Israel and Iran or India and Pakistan, have potential religious dimensions. Short of war, tensions such as those related to immigration might become unbearable. Familiar issues of creed and identity could be exacerbated. One way or another, the secular rational approach would be sidestepped by a return to theocratic absolutes, competing or converging with secular absolutes such as unbridled nationalism.

### 3

#### The AFF posits a world in which individuals have no responsibility – this fails to understand the way that the individual shapes war and everyday violence

**Kappeler 95**(Susanne, Associate Professor at Al-Akhawayn University, The Will to Violence: The politics of personal behavior, Pg.10-11)

Yet our insight that indeed we are not responsible for the decisions of a Serbian general or a Croatian president tends to mislead us into thinking that therefore we have no responsibility at all, not even for forming our own judgment, and thus into underrating the responsibility we do have within our own sphere of action. In particular, it seems to absolve us from having to try to see any relation between our own actions and those events, or to recognize the connections between those political decisions and our own personal decisions. It not only shows that we participate in what Beck calls ‘organized irresponsibility’, upholding the apparent lack of connection between bureaucratically, institutionally, nationally, and also individually organized separate competences. It also proves the phenomenal and unquestioned alliance of our personal thinking with the thinking of the major power mongers. For we tend to think that we cannot ‘do’ anything, say, about a war, because we deem ourselves to be in the wrong situation because we are not where the major decisions are made.Which is why many of those not yet entirely disillusioned with politics tend to engage in a form of mental deputy politics, in the style of ‘what would I do if I were the general, the prime minister, the president, the foreign minister or the minister of defense?’ Since we seem to regard their mega spheres of action as the only worthwhile and truly effective ones, and since our political analyses tend to dwell there first of all, any question of what I would do if I were indeed myself tends to peter out in the comparative insignificance of having what is perceived as ‘virtually no possibilities’: what I could do seems petty and futile. For my own action I obviously desire the range of action of a general, a prime minister, or a General Secretary of the UN – finding expression in ever more prevalent formulations like ‘I want to stop this war’, ‘I want military intervention’, ‘I want to stop this backlash’, or ‘I want a moral revolution. ‘We are this war’, however, even if we do not command the troops or participate in co-called peace talks, namely as Drakulic says, in our non-comprehension’: our willed refusal to feel responsible for our own thinking and for working out our own understanding, preferring innocently to drift along the ideological current of prefabricated arguments or less than innocently taking advantage of the advantages these offer. And we ‘are’ the war in our ‘unconscious cruelty towards you’, our tolerance of the ‘fact that you have a yellow form for refugees and I don’t’- our readiness, in other words, to build identities, one for ourselves and one for refugees, one of our own and one for the ‘others.’ We share in the responsibility for this war and its violence in the way we let them grow inside us, that is, in the way we shape ‘our feelings, our relationships, our values’ according to the structures and the values of war and violence.

#### We are the violence. Individuals are the impetus for exploitation and racism, and only this theory explains the truth behind violence

Kappeler 95 (Susanne, Associate Professor at Al-Akhawayn University, The Will to Violence: The politics of personal behavior, Pg.9)

war does not suddenly break out in a peaceful society; sexual violence is not the disturbance of otherwise equal gender relations. Racist attacks do not shoot like lightning out of a non-racist sky, and the sexual exploitation of children is no solitary problem in a world otherwise just to children. The violence of our most commonsense everyday thinking**,** and especially our personal will to violence, constitute the conceptual preparation**,** the ideological armament and the intellectual mobilizationwhich make the ;outbreak’ of war**,** of sexual violence, of racist attacks, of murder and destructionpossibleat all. ‘We are the war’, writes SlavenkaDrakulic at the end of her existential analysis at the end of her existential analysis of the question, ‘what is war?’: I do not know what war is, I want to tell [my friend], but I see it everywhere. It is in the blood-soaked street in Sarajevo, after 20 people have been killed while they queued for bread. But it is also in your non-comprehension, in my unconscious cruelty towards you, in the fact that you have a yellow form [for refugees] and I don’t, in the way in which it grows inside ourselves and changes our feelings, relationships, values – in short: us. We are the war…and I am afraid that we cannot hold anyone else responsible. We make this war possible, we permit it to happen. ‘We are the war’- and we also ‘are’ the sexual violence, the racist violence, the exploitation and the will to violence in all its manifestations in a society in co-called ‘peacetime’, for we make them possible and we permit them to happen.

#### The Alternative is to reject the affirmatives representations and reconcieve of violence as an issue of personal choice made by individuals.

Kappeler 95(Susanne, Associate Professor at Al-Akhawayn University, The Will to Violence: The politics of personal behavior, Pg.5-6)

**A politics aiming at a change in people’s behavior would require** political work that is very much more cumbersome and very much less promising of success than is the use of state power and social control. It would require political consciousness-raising- politicizing the way we think- which cannot be imposed on others by force or compulsory educational measures. It would require **a view of people which takes seriously and reckons with their will, both their will to violence or their will to change.** To take seriously the will of othershoweverwould mean recognizing one’s own, and putting people’s will, including our own, at the centre of political reflection. A political analysis of violence needs to recognize this will, the personal decision in favor of violence- not just to describe acts of violence, or the conditions which enable them to take place, but **also** to capture the moment of decision which is the real impetus for violent action. For without this decision there will be no violent act, not even in circumstances which potentially permit it.It is the decision to violate, not just the act itself, which make a person a perpetrator of violence-**just as it is the decision not to do so which makes people not act violently and not abuse their power in a situation which would nevertheless permit it.** This moment of decision, therefore, isalsothe locus of potential resistance to violence**. To understand the structures of thinking and the criteria by which such decisions are reached, but above all** to regard this decision as an act of choice, seems to mea necessary precondition for any political struggle against violenceand for a non-violent society. My focus then, is on the decision to violate- not just in circumstances where violence is conspicuous by its damage, but in every situation where the choice to violate presents itself. This means a change from the accustomed perspective on violence to the context where decisions for actions are being made, as it were “before” their consequence become apparent, and which we may not recognize as contexts of violence. Our political analysis of sexual or racist violence have necessarily concentrated on situations where the power disequilibrium between perpetrator and victim is extreme, where, in particular, it is supported by social power structures such as male and/or white supremacy, so that not only is the violence unlikely to receive sanctions, but on the contrary, the perpetrator will find support rather than the victim. Violence, however, is a possibility wherever there is freedom of action, however limited. Such violence may ‘look different’, not least because the possibilities or resistance may also be greater in situations where there is relative freedom of action also on the part of the other agent, that is, the violator’s envisaged victim.

### 4

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

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

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

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

#### Notification kills effective cyber responses

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

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

### Deterrence: 1NC

#### 1. Established cyber deterrent now

Eric Talbot Jensen, ‘12 (Associate Professor, Brigham Young University Law School. , “CYBER DETERRENCE”, Emory law Journal)

Among the most worrisome of hacking incidents are those focused on critical national infrastructure.14 This infrastructure is the backbone of United States’ transportation and economic systems.15 The cost of downtime alone from major attacks on critical national infrastructure “exceeds . . . $6 million per day.”16 The attacks have caused President Barack Obama to recently state, **From now on, our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage**.17 President **Obama’ s recognition of the role and importance of deterring malicious cyber operations,** including cyber attacks, **incorporates the traditional notions of deterrence to this modern risk to national security.** **Deterrence** has been a part of Western political security doctrine since ancient Greece18 and played a particularly key role in the post-World War II nuclear world.19 It is equally **important in today’s world of cyber operations** 20 **and will continue to play a key role in the U.S. national security strategy**.21 In fact, just as **cyber operations offer** unique capabilities as tools to accomplish national goals,22 they also present distinctive aspects of deterrence, both in line with traditional notions of deterrence and also some **innovative and progressive ways of viewing deterrence.**23

#### 2. Offensive capabilities are key to deterrence – without offensive policy flexibility the US will be vulnerable to attack

Jarno Limnéll October 9 2012 “Offensive Cyber Capabilities Need to be Built and Exposed Because of Deterrence”, <http://www.infosecisland.com/blogview/22534-Offensive-Cyber-Capabilities-Need-to-be-Built-and-Exposed-Because-of-Deterrence.html>

Within the next couple of years the world will experience more intentionally executed and demonstrated cyberattacks while the development of offensive cyberweapons will become fiercer and publicly more acceptable.¶ Today, cyber capabilities are essential for nation-states and armed forces that want to be treated as credible players**.** Cyberspace, the fifth dimension of warfare, has already become an important arena of world politics, especially since we are living in a time in which the lines between war and peace have blurred. The digital world has become a domain where strategic advantage can be either lost or won.¶ To succeed in the cyber domain is not merely a question of defense, even if we would like to think of it that way – at least not for the nation-states. Naturally, defense capabilities have to be as preventive as possible in order to reduce the effectiveness of the adversary´s – whoever it might be –cyber attack. However, despite the best defensive efforts, intrusions will occur. In the cyber domain, you must also be resilient, i.e. have the ability to withstand attacks and failures, to mitigate harm, more so than what is needed in other domains. Creating cyber defense capabilities and resilience are fairly easy for the public to accept. But they are not enough. Deterrence is also needed, that is, the capabilities and policies to convince others not to launch a cyber attack against you. Deterrence will only be effective if you can build and demonstrate offensive cyber capabilities. To put it clearly: cyber offensive capabilities are an essential element for nation-states to succeed in the current and future reality of both international and security policies. Defense, resilience, and offense contribute to a country’s overall ability to protect itself. You need them all.¶ From nuclear to cyber deterrence¶ Deterrence theory was developed in the 1950s, primarily to address the new strategic challenges posed by nuclear weapons. During the Cold War, nuclear deterrence was able to keep the United States and the Soviet Union in check. Nuclear deterrence was the art of convincing an enemy not to take a specific action by threatening it with intolerable punishment or unacceptable failure. The theory worked well**.**¶ Based on that logic, cyber deterrence should play a similar role in the digitalized world. However, the anonymity, the advantage of attacks, and the global reach and interconnectedness greatly reduce the efficiency of cyber deterrence. At the same time, there are suspicion and rumors surrounding the kind of capabilities others have and how they are already using those capabilities.¶ In the kinetic world, it is much simpler to evaluate an opponent’s capabilities. It is typically quite easy to accurately estimate how many tanks, interceptors, or submarines a given country possesses. Countries also openly expose their arsenal, in military parades for example, or their operational skills, by organizing large military exercises. In the logic of deterrence, even more important than having the actual capability is the perception of having that capability.

#### 3. Executive flexibility is key to deterrence

**Bradbury 11** (Steven – partner @ Dechert, LLP, “The Developing Legal Framework for Defensive and Offensive Cyber Operations” March 2011, Cybersecurity: Law, Privacy, and Warfare in a Digital World, Harvard National Security Journal, Vol. 2)

Conclusion. So here’s my thesis: To my view, **the lack of clarity on certain of these issues under international law means that with respect to those issues, the President is free to decide, as a policy matter, where and how the lines should be drawn on the limits of traditional military power** in the sphere of cyberspace. For example, that means that within certain parameters, **the President could decide when and to what extent military cyber operations may target computers located outside areas of hot fighting that the enemy is using for military advantage**. And when a cyber attack is directed at us, **the President can decide, as a matter of national policy, whether and when to treat it as an act of war**. The corollary to all this is that **in situations where the customs of war,** in fact, **are not crystallized**, **the lawyers at the State Department and the Justice Department shouldn’t make up new red lines** — **out of some aspirational sense of what they think international law ought to be** — **that end up putting dangerous limitations on the options available to the United States**. Certainly, the advice of lawyers is always important, especially so where the legal lines are established or firmly suggested. **No one would contend that the laws of war have no application to cyber operations or that cyberspace is a law free zone**. **But it’s not the role of the lawyers to make up new lines that don’t yet exist in a way that preempts the development of policy**. 14 In the face of this lack of clarity on key questions, some advocate for the negotiation of a new international convention on cyberwarfare — perhaps a kind of arms control agreement for cyber weapons. **I believe there is no foreseeable prospect that that will happen. Instead, the outlines of accepted norms and limitations in this area will develop through the practice of leading nations**. And **the policy decisions made by the United States in response to particular events will have great influence in shaping those international norms**. I think that’s the way we should want it to work.

#### 4. Independently undermines deterrence and turns the aff – ambiguity is the only way to maintain cyber dominance

Lieutenant Colonel **Mowchan** is a member of the staff and faculty at the Center for Strategic Leadership, U. S. Army War College, where he teaches cyber warfare and national intelligence. He is a career Army intelligence officer and holds a master’s degree in strategic intelligence from the National Intelligence University. He has served for 20 years in a variety of tactical, theater, and strategic intelligence positions and is a member of the U.S. Naval Institute’s Editorial Board, **11** [Don’t Draw the (Red) Line,” Proceedings Magazine - October 2011 Vol 137, no 10/1304, http://www.usni.org/magazines/proceedings/2011-10/dont-draw-red-line]

In a strategic environment that has become more volatile, complex, and uncertain, **the United States increasingly relies on cyberspace to advance its national interests.** Simultaneously, **our adversaries**, particularly nation states, **are afforded more opportunities to undermine our efforts through their own nefarious activities in the digital domain**. While not every act in coming years will pose an imminent threat to U.S. national security, economic well-being, or social stability, some will. Because of this, **strategists, government leaders, and scholars frequently disagree over whether the United States should establish thresholds (or “red lines”) for responding to such hostile acts.** Red-line proponents assert that thresholds can decrease the ambiguity of U.S. policies, bolster deterrence, and facilitate swift, decisive action.¶ **Establishing cyber red lines**, however, **is folly**. Given the evolving threat, **current strategies, and the challenges of attribution in this domain, the United States is better served by not delineating them. Maintaining ambiguity on when and how U.S. instruments of national power will be used after a cyber attack gives government leaders the flexibility to tailor responses** much as they would to threats in the other global domains.¶ Sources of Invisible Threats¶ To properly frame the issue**, it is necessary to understand the evolving digital threat environment and current U.S. strategies**. Hazards to national security and economic prosperity in cyberspace are multiplying. **As the world becomes more interconnected, diverse state and non-state actors will have greater access and operational maneuverability to conduct malicious activities**.¶ Sources of non-state cyber threats include, but are not limited to, hackers, “hacktivists,” terrorists, and organized crime groups. Hackers are generally thrill-seekers who regard accessing secure computer networks as a challenge. They usually don’t possess the technical skills to cause widespread, longstanding damage to computer networks; however, given the increasing availability of advanced tools, it is plausible that a skilled hacker could significantly disrupt critical U.S. information systems. Such a possibility becomes even more real if a nation state seeking to avoid attribution gives hackers the tools to disrupt or destroy critical networks.¶ For example, in early 2011, the computer security company McAfee, Inc., revealed that a Chinese hacker in Heze City, Shandong province, likely operating with external assistance, stole financial documents related to oil-and-gas-field exploration and operational details on data acquisition systems from five undisclosed Western multinational companies. The operation, known as Night Dragon, underscores how hackers can target not only the defense industrial base, government, and military computers, but global corporate and commercial targets. 1¶ By contrast, hacktivists use cyberspace to promote their political beliefs. While often focusing on propaganda, they can cause significant disruptions to computer networks, especially if technical or financial support is provided by external parties. For example, during the first 24 hours of the 2008 Russo-Georgian War, unidentified entities created a forum called StopGeorgia.ru, which contained target lists, links to advanced malware, and expert advice on attacking critical Georgian information systems. 2 No evidence linked the Russian government or military to this forum; however, its timing and Russia’s purported advanced digital capabilities suggest there could at least have been an indirect tie.¶ **With the proliferation of technologies, terrorist organizations such as al Qaeda also could cause catastrophic damage**. According to Deputy Secretary of Defense William J. Lynn, “**The greatest concern . . . is a terrorist group that gains the level of disruptive and destructive capability currently possessed by nation states.”** 3 For example, in 2010 a terrorism suspect with links to al Qaeda acknowledged that the latter had conducted offensive operations that included denial-of-service attacks against the Israeli prime minister’s computer server. 4¶ **Organized crime groups penetrate computer networks to steal money and trade secrets or financial information**. There is evidence that Central European crime groups have defrauded U.S. citizens and businesses of approximately $1 billion and as much as $1 trillion on a global scale in the past year. 5 More ominous, crime groups have also attempted to acquire sensitive U.S. defense-related information, which could then be sold on the black market to our adversaries.¶ Foreign Intelligence Networks¶ While nonstate actors may constitute the greatest threat, **nation states have the necessary resources to acquire the most advanced technologies**. Currently more than 100 foreign national intelligence organizations conduct operations, many of which target U.S. computer networks. 6 These organizations likely employ proxies to hide the identity of the responsible state. **The most sophisticated threats originate in Russia and China, which continue to make significant advancements in their capabilities.**¶ **In May, China’s defense minister announced the existence of an elite People’s Liberation Army cyber unit called the Blue Army**. 7 **While this unit’s mission is “cyber defense,” conducting offensive operations is but a keystroke away.** And last year, Russia’s director of the Institute of Information Security Issues at Moscow State University (also a member of Russia’s National Security Council) admitted the nation is developing offensive cyber capabilities. 8¶ **The extent of this activity leads to several key conclusions. First, nation states pose the greatest threat to U.S. computer networks. China and Russia, for instance, can conduct a full range of hostile actions, from web-page defacements and espionage to deploying malicious software that can disrupt or destroy computer networks operating critical U.S. information systems**. Second**, cyberspace affords anonymity, masking both perpetrator and motive**. Third, **relative ease of access and the proliferation of advanced information technologies allow almost anyone to cause significant damage to U.S. computer networks**. Finally, the lines differentiating the sources of these threats—nation state, criminal organization, or terrorists—are becoming increasingly blurred, rendering the appropriate response highly problematic.¶ Evolving U.S. Policies¶ The United States recently released two national strategies for operating in the digital domain: the International Strategy for Cyberspace (ISC) and the Department of Defense Strategy for Operating in Cyberspace (DSOC). **The ISC is a landmark policy document intended to “promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation.**” 9 While the document emphasizes diplomacy and development, defense plays a critical role, especially as it pertains to this domain. The ISC states:¶ When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. **All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners**. **We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation**, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible. 10¶ DOD followed with the DSOC, which acknowledges that such hostile operations will be prominent in any future conflict involving state or non-state actors. It outlines five strategic initiatives:¶ • Treat cyberspace as an operational domain to organize, train, and equip so that DOD can take full advantage of its potential.¶ • Employ new defense operating concepts to protect DOD networks and systems.¶ • Partner with other U.S. government departments, agencies, and the private sector.¶ • Build sound relationships with U.S. allies and international partners to strengthen collective security.¶ • Leverage the nation’s ingenuity through an exceptional workforce and rapid technological innovation. 11¶ **While DOD’s strategy is defensive in nature, it states that U.S. military power will be used if necessary:** “The Department will work with interagency and international partners to encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuade and deter malicious actors, and reserve the right to defend these vital national assets as necessary and appropriate.” 12¶ **Both plans lead to several key observations. First, the ISC and DSOC are intentionally ambiguous.** **Neither defines a hostile act in cyberspace, nor is there language explicitly stating when, how, and to what extent the United States will respond to such acts**. Second, **both strategies acknowledge that there are no simple solutions to the challenges of the day.** Finally, decisions will continue to be shaped by the dynamic interplay of a surfeit of political, economic, military, and social variables in the international environment, and **because the world is more “gray” than black-and-white, responses to hostile acts in the digital domain will be determined as strategic responses are in conventional warfare**.¶ The Case for Thresholds¶ **Red-line advocates believe that creating thresholds will decrease the ambiguity of our policies, bolster deterrence, and facilitate a more timely response**. Some pundits criticize the ISC and DSOC, arguing they take ambiguity too far. The DSOC in particular, they think, should outline response thresholds that if crossed, would result in diplomatic or military retaliation. Following the release of DOD’s strategy, Representative Jim Langevin (D-RI) acknowledged the DSOC represented a good start but said it was deficient in several key areas, including its fixation on defense and the identification of acceptable red lines. 13¶ **After the DSOC was published, now-retired Marine Corps General James Cartwright, the former vice chairman of the Joint Chiefs of Staff, remarked that the strategy was too defensive**, stating “**we are supposed to be offshore convincing people if they attack, it won’t be free** . . . [**and that] disabling computerized patient records at a hospital such that the patients cannot be treated would be a violation of the law of armed conflict** [which could] then [trigger a] proportional response.” 14 General **Cartwright went on to emphasize the nation will need stronger deterrents**. Although he did not say what the deterrents should be or what instruments of national power would be used, **his words lend support to red-line advocates who demand greater specificity in U.S. policies, greater clarity on what constitutes a hostile act,** and clear thresholds.¶ Why Ambiguity Is Good¶ **Those arguing for establishing red lines fail to comprehend the complexity of the digital domain, in which adaptation and anonymity are the norm.** **The United States is better served in the long run by not establishing such thresholds, for four reasons**. **First, not doing so allows government leaders the latitude to tailor response options based on a hostile act, its physical and digital effects, and how it relates to the current state of affairs in the international system**. As retired Air Force General Kevin Chilton remarked in 2009 as commander, U.S. Strategic Command, “**I don’t think you take anything off the table when you provide [response] options to the president to decide.** **Why would we constrain ourselves on how we would respond [to hostile acts in cyberspace**]?” 15¶ Such an approach does not differ from the way the United States addresses hostile acts in other domains. **If red lines are established, we will be compelled to respond to each threat that crosses the line, which is unrealistic, given that our computer networks are subjected to millions of probes, scans, and attacks on a daily basis**. **Even if red lines are narrowly focused (e.g., employing military force if a cyber attack results in the deaths of U.S. citizens**), **the first time the United States fails to respond accordingly, it will undermine the credibility and deterrence effect of our other capabilities**.¶ A second reason in favor of ambiguity is that **if our adversaries know our response to such acts, they will adjust accordingly**. Because neither the national nor the defense strategy explicitly defines a hostile act in cyberspace or exactly how the United States will respond, this leaves it open to interpretation. As one military official remarked, “**If you shut down our power grid, maybe we will put a missile down one of your smokestacks.”** 16 In addition, **hostile actors may perceive a green light for certain acts that do not cross a particular response threshold**. While one such act below this threshold may not be harmful to U.S. interests, what if 100 million are? Again, **maintaining ambiguity concerning when, how, and to what extent to respond gives the United States greater latitude.**¶ Third, **because cyberspace is a global domain that emphasizes open access, the free flow of information, and anonymity, it is extremely difficult to determine where the threat or attack originated**. For example, U.S. military networks are probed more than six million times a day by assailants operating in one corner of the world using computer networks or servers in another corner. Most perpetrators are never identified, except for a computer Internet protocol address or a one-time user alias. Army General Keith Alexander, commander of U.S. Cyber Command and Director, National Security Agency, emphasized this challenge, saying, “**Too often, the military discovers through forensics that network probes have been successful [and] as a consequence, response becomes policing up after the fact versus mitigating it real time**.” 17 **If red lines demand a timely response and there is no one to pin responsibility on, then how can a response be implemented?**¶ Finally, **even if the source of the attacks is determined** in a timely manner, **automatic triggers for a response, particularly those that employ military force, could create negative second- and third-order effects that make a bad situation even worse**. **Given that nation states pose the greatest threat to U.S. networks, red lines that automatically result in a response could escalate an already volatile situation.**¶ For example, in 2009 individuals in **China and Russia** penetrated computer networks operating parts of the U.S. electrical power grid. 18 They **reportedly inserted malware that could destroy infrastructure components.** Although their identities or associations with the Russian and Chinese governments were not disclosed, **it validates the point that response options must be tailored**. If Russia or China, two nuclear powers, were responsible, **a U.S. response would be markedly different than if they had they been conducted by a non-nuclear state**. Clearly the diplomatic, information, and economic instruments of national power versus military force would receive more emphasis with China or Russia for what could be considered a hostile act in cyberspace.¶ **Given the complex and indeterminate 21st century international system and the multitude of current threats, U.S. interests will be better served by not establishing clear thresholds**. **Ambiguity is a powerful tool to shape our adversaries’ actions in all domains and allows us the maneuverability to respond where, when, and how we choose**. **Red-line advocates must understand that thresholds only constrain our actions and could undermine credibility and the power to effectively deter our adversaries**.

#### 5. Your attribution argument takes out the adv—for others to perceive the US as a deterrent, they have to attribute the attack to the US

#### 6. Plan is unnecessary

**Brecher, 2012**. (Aaron, Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations, 111 Michigan Law Review, No 3, p 423, L/N)

Significantly more modest statutory interventions have also been proposed; however, statutory clarification may not be necessary to achieve their aims. Like Dycus, Robert Chesney is concerned about drawing lines between covert action and traditional military activity in the cyberattack context. He argues that it may be useful for Congress to clarify that the military may conduct those operations outside the title 50 framework when defending Pentagon assets or acting pursuant to a separate statute authorizing force. [n166](http://www.lexisnexis.com.ezp1.lib.umn.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1374611534093&returnToKey=20_T17845089181&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.59498.56057527503#n166) Moreover, he suggests notifying the congressional armed services committees when such operations are likely to have effects that spill over into areas outside a zone of conflict. [n167](http://www.lexisnexis.com.ezp1.lib.umn.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1374611534093&returnToKey=20_T17845089181&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.59498.56057527503#n167) But there need not be a legislative mandate for an executive practice of reporting cyberattacks to both intelligence and armed services committees. Moreover, as Chesney himself argues, under a proper understanding of the definitions in the covert action statute, where routine support for ongoing hostilities is exempt under the military activities exception, any cyberattack initiated in support of a conflict authorized by congressional statute would be exempt. [n168](http://www.lexisnexis.com.ezp1.lib.umn.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1374611534093&returnToKey=20_T17845089181&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.59498.56057527503#n168) This view accords well with that articulated in this Note, [n169](http://www.lexisnexis.com.ezp1.lib.umn.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1374611534093&returnToKey=20_T17845089181&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.59498.56057527503#n169) and an executive order setting covert action procedures as the default would hardly preclude forgoing that framework in appropriate circumstances; a presumption, after all, merely encourages findings and reporting when there is doubt about the appropriate framework.

#### 7. Nuclear war outweighs

Jason **Healey**, 3-30-**2013**, “No, Cyberwarfare Isn't as Dangerous as Nuclear War,” US News and World Report, http://www.usnews.com/opinion/blogs/world-report/2013/03/20/cyber-attacks-not-yet-an-existential-threat-to-the-us

**America does not face an existential cyberthreat today, despite recent warnings.** Our **cybervulnerabilities are** undoubtedly **grave and the threats** we face **are severe but far from comparable to nuclear war**. The most **recent** alarms come in a Defense Science Board **report** on how to make military cybersystems more resilient against advanced threats (in short, Russia or China). It **warned** that the "**cyber threat is serious, with potential consequences similar** in some ways **to the nuclear threat** of the Cold War." Such fears were also expressed by Adm. Mike Mullen, then chairman of the Joint Chiefs of Staff, in 2011. **He called cyber** "**The single biggest existential threat** that's out there" because "cyber actually more than theoretically, can attack our infrastructure, our financial systems." While it is true that cyber attacks might do these things, it is also **true they have not only never happened but are far more difficult to accomplish than mainstream thinking believes**. The **consequences from cyber threats may be similar in some ways to nuclear**, as the Science Board concluded**, but mostly, they are incredibly dissimilar**. [See a collection of political cartoons on defense spending.] Eighty years ago, the generals of the U.S. Army Air Corps were sure that their bombers would easily topple other countries and cause their populations to panic, claims which did not stand up to reality. **A study of the 25-year history of cyber conflict**, by the Atlantic Council and Cyber Conflict Studies Association**, has shown** a similar dynamic where **the impact of disruptive cyberattacks has been consistently overestimated**. Rather than theorizing about future cyberwars or extrapolating from today's concerns, **the history of cyberconflict that have actually been fought, shows that cyber incidents have so far tended to have effects that are either widespread but fleeting or persistent but narrowly focused.** **No attacks**, so far**, have been both widespread and persistent. There have been no authenticated cases of anyone dying from a cyber attack**. Any widespread disruptions, even the 2007 disruption against Estonia, have been short-lived causing no significant GDP loss. Moreover, as with conflict in other domains, cyberattacks can take down many targets but keeping them down over time in the face of determined defenses has so far been out of the range of all but the most dangerous adversaries such as Russia and China. Of course, if the United States is in a conflict with those nations, cyber will be the least important of the existential threats policymakers should be worrying about. **Plutonium trumps bytes in a shooting war.** [Read the U.S. News Debate: Should There Be an International Treaty on Cyberwarfare?] This is not all good news. Policymakers have recognized the problems since at least 1998 with little significant progress. Worse, the threats and vulnerabilities are getting steadily more worrying. Still, **experts have been warning of a cyber Pearl Harbor for 20** of the 70 **years** since the actual Pearl Harbor. The transfer of U.S. trade secrets through Chinese cyber espionage **could someday accumulate into an existential threat. But it doesn't seem so** seem just **yet,** with only handwaving estimates of **annual losses of 0.1 to 0.5 percent** to the total U.S. GDP of around $15 trillion. That's bad, but **it doesn't add up to an existential crisis or "economic cyberwar**." [See a collection of political cartoons on the economy.] Instead, the true existential cyberdanger is likely to come after America connects the electrical grid and other infrastructure to the Internet. An interconnected Smart Grid connects things made not just of bytes and silicon but of concrete and steel. It is all too likely that America will take its overstretched and insecure electrical system and connect it to the Internet. In this future our electric supply is no more or less reliable than the Internet and the years when no one died because of cyberattacks will seem like the quaint good ol' days. There are still **practical solutions** to avoid today's serious threats become tomorrow's existential ones but these **are often overshadowed by the rhetoric of cyberwar, the push for ever better U.S. cyberoffense**, and other distractions. Focusing on actual fixes, like securing the Smart Grid, will be the best ways to avoid future existential attacks.

#### 8. Cyber war infeasible

Clark, MA candidate – Intelligence Studies @ American Military University, senior analyst – Chenega Federal Systems, 4/28/’12 (Paul, “The Risk of Disruption or Destruction of Critical U.S. Infrastructure by an Offensive Cyber Attack,” American Military University)

The Department of Homeland Security worries that our critical infrastructure and key resources (CIKR) may be exposed, both directly and indirectly, to multiple threats because of CIKR reliance on the global cyber infrastructure, an infrastructure that is under routine cyberattack by a “spectrum of malicious actors” (National Infrastructure Protection Plan 2009). CIKR in the extremely large and complex U.S. economy spans multiple sectors including agricultural, finance and banking, dams and water resources, public health and emergency services, military and defense, transportation and shipping, and energy (National Infrastructure Protection Plan 2009). The disruption and destruction of public and private infrastructure is part of warfare, without this infrastructure conflict cannot be sustained (Geers 2011). Cyber-attacks are desirable because they are considered to be a relatively “low cost and long range” weapon (Lewis 2010), but prior to the creation of Stuxnet, the first cyber-weapon, the ability to disrupt and destroy critical infrastructure through cyber-attack was theoretical. The movement of an offensive cyber-weapon from conceptual to actual has forced the United States to question whether offensive cyber-attacks are a significant threat that are able to disrupt or destroy CIKR to the level that national security is seriously degraded. It is important to understand the risk posed to national security by cyber-attacks to ensure that government responses are appropriate to the threat and balance security with privacy and civil liberty concerns. The risk posed to CIKR from cyber-attack can be evaluated by measuring the threat from cyber-attack against the vulnerability of a CIKR target and the consequences of CIKR disruption. As the only known cyber-weapon, Stuxnet has been thoroughly analyzed and used as a model for predicting future cyber-weapons. The U.S. electrical grid, a key component in the CIKR energy sector, is a target that has been analyzed for vulnerabilities and the consequences of disruption predicted – the electrical grid has been used in multiple attack scenarios including a classified scenario provided to the U.S. Congress in 2012 (Rohde 2012). Stuxnet will serve as the weapon and the U.S. electrical grid will serve as the target in this risk analysis that concludes that there is a low risk of disruption or destruction of critical infrastructure from a an offensive cyber-weapon because of the complexity of the attack path, the limited capability of non-state adversaries to develop cyber-weapons, and the existence of multiple methods of mitigating the cyber-attacks. To evaluate the threat posed by a Stuxnet-like cyber-weapon, the complexity of the weapon, the available attack vectors for the weapon, and the resilience of the weapon must be understood. The complexity – how difficult and expensive it was to create the weapon – identifies the relative cost and availability of the weapon; inexpensive and simple to build will be more prevalent than expensive and difficult to build. Attack vectors are the available methods of attack; the larger the number, the more severe the threat. For example, attack vectors for a cyberweapon may be email attachments, peer-to-peer applications, websites, and infected USB devices or compact discs. Finally, the resilience of the weapon determines its availability and affects its usefulness. A useful weapon is one that is resistant to disruption (resilient) and is therefore available and reliable. These concepts are seen in the AK-47 assault rifle – a simple, inexpensive, reliable and effective weapon – and carry over to information technology structures (Weitz 2012). The evaluation of Stuxnet identified malware that is “unusually complex and large” and required code written in multiple languages (Chen 2010) in order to complete a variety of specific functions contained in a “vast array” of components – it is one of the most complex threats ever analyzed by Symantec (Falliere, Murchu and Chien 2011). To be successful, Stuxnet required a high level of technical knowledge across multiple disciplines, a laboratory with the target equipment configured for testing, and a foreign intelligence capability to collect information on the target network and attack vectors (Kerr, Rollins and Theohary 2010). The malware also needed careful monitoring and maintenance because it could be easily disrupted; as a result Stuxnet was developed with a high degree of configurability and was upgraded multiple times in less than one year (Falliere, Murchu and Chien 2011). Once introduced into the network, the cyber-weapon then had to utilize four known vulnerabilities and four unknown vulnerabilities, known as zero-day exploits, in order to install itself and propagate across the target network (Falliere, Murchu and Chien 2011). Zero-day exploits are incredibly difficult to find and fewer than twelve out of the 12,000,000 pieces of malware discovered each year utilize zero-day exploits and this rarity makes them valuable, zero-days can fetch $50,000 to $500,000 each on the black market (Zetter 2011). The use of four rare exploits in a single piece of malware is “unprecedented” (Chen 2010). Along with the use of four unpublished exploits, Stuxnet also used the “first ever” programmable logic controller rootkit, a Windows rootkit, antivirus evasion techniques, intricate process injection routines, and other complex interfaces (Falliere, Murchu and Chien 2011) all wrapped up in “layers of encryption like Russian nesting dolls” (Zetter 2011) – including custom encryption algorithms (Karnouskos 2011). As the malware spread across the now-infected network it had to utilize additional vulnerabilities in proprietary Siemens industrial control software (ICS) and hardware used to control the equipment it was designed to sabotage. Some of these ICS vulnerabilities were published but some were unknown and required such a high degree of inside knowledge that there was speculation that a Siemens employee had been involved in the malware design (Kerr, Rollins and Theohary 2010). The unprecedented technical complexity of the Stuxnet cyber-weapon, along with the extensive technical and financial resources and foreign intelligence capabilities required for its development and deployment, indicates that the malware was likely developed by a nation-state (Kerr, Rollins and Theohary 2010). Stuxnet had very limited attack vectors. When a computer system is connected to the public Internet a host of attack vectors are available to the cyber-attacker (Institute for Security Technology Studies 2002). Web browser and browser plug-in vulnerabilities, cross-site scripting attacks, compromised email attachments, peer-to-peer applications, operating system and other application vulnerabilities are all vectors for the introduction of malware into an Internetconnected computer system. Networks that are not connected to the public internet are “air gapped,” a technical colloquialism to identify a physical separation between networks. Physical separation from the public Internet is a common safeguard for sensitive networks including classified U.S. government networks. If the target network is air gapped, infection can only occur through physical means – an infected disk or USB device that must be physically introduced into a possibly access controlled environment and connected to the air gapped network. The first step of the Stuxnet cyber-attack was to initially infect the target networks, a difficult task given the probable disconnected and well secured nature of the Iranian nuclear facilities. Stuxnet was introduced via a USB device to the target network, a method that suggests that the attackers were familiar with the configuration of the network and knew it was not connected to the public Internet (Chen 2010). This assessment is supported by two rare features in Stuxnet – having all necessary functionality for industrial sabotage fully embedded in the malware executable along with the ability to self-propagate and upgrade through a peer-to-peer method (Falliere, Murchu and Chien 2011). Developing an understanding of the target network configuration was a significant and daunting task based on Symantec’s assessment that Stuxnet repeatedly targeted a total of five different organizations over nearly one year (Falliere, Murchu and Chien 2011) with physical introduction via USB drive being the only available attack vector. The final factor in assessing the threat of a cyber-weapon is the resilience of the weapon. There are two primary factors that make Stuxnet non-resilient: the complexity of the weapon and the complexity of the target. Stuxnet was highly customized for sabotaging specific industrial systems (Karnouskos 2011) and needed a large number of very complex components and routines in order to increase its chance of success (Falliere, Murchu and Chien 2011). The malware required eight vulnerabilities in the Windows operating system to succeed and therefore would have failed if those vulnerabilities had been properly patched; four of the eight vulnerabilities were known to Microsoft and subject to elimination (Falliere, Murchu and Chien 2011). Stuxnet also required that two drivers be installed and required two stolen security certificates for installation (Falliere, Murchu and Chien 2011); driver installation would have failed if the stolen certificates had been revoked and marked as invalid. Finally, the configuration of systems is ever-changing as components are upgraded or replaced. There is no guarantee that the network that was mapped for vulnerabilities had not changed in the months, or years, it took to craft Stuxnet and successfully infect the target network. Had specific components of the target hardware changed – the targeted Siemens software or programmable logic controller – the attack would have failed. Threats are less of a threat when identified; this is why zero-day exploits are so valuable. Stuxnet went to great lengths to hide its existence from the target and utilized multiple rootkits, data manipulation routines, and virus avoidance techniques to stay undetected. The malware’s actions occurred only in memory to avoid leaving traces on disk, it masked its activities by running under legal programs, employed layers of encryption and code obfuscation, and uninstalled itself after a set period of time, all efforts to avoid detection because its authors knew that detection meant failure. As a result of the complexity of the malware, the changeable nature of the target network, and the chance of discovery, Stuxnet is not a resilient system. It is a fragile weapon that required an investment of time and money to constantly monitor, reconfigure, test and deploy over the course of a year. There is concern, with Stuxnet developed and available publicly, that the world is on the brink of a storm of highly sophisticated Stuxnet-derived cyber-weapons which can be used by hackers, organized criminals and terrorists (Chen 2010). As former counterterrorism advisor Richard Clarke describes it, there is concern that the technical brilliance of the United States “has created millions of potential monsters all over the world” (Rosenbaum 2012). Hyperbole aside, technical knowledge spreads. The techniques behind cyber-attacks are “constantly evolving and making use of lessons learned over time” (Institute for Security Technology Studies 2002) and the publication of the Stuxnet code may make it easier to copy the weapon (Kerr, Rollins and Theohary 2010). However, this is something of a zero-sum game because knowledge works both ways and cyber-security techniques are also evolving, and “understanding attack techniques more clearly is the first step toward increasing security” (Institute for Security Technology Studies 2002). Vulnerabilities are discovered and patched, intrusion detection and malware signatures are expanded and updated, and monitoring and analysis processes and methodologies are expanded and honed. Once the element of surprise is lost, weapons and tactics are less useful, this is the core of the argument that “uniquely surprising” stratagems like Stuxnet are single-use, like Pearl Harbor and the Trojan Horse, the “very success [of these attacks] precludes their repetition” (Mueller 2012). This paradigm has already been seen in the “son of Stuxnet” malware – named Duqu by its discoverers – that is based on the same modular code platform that created Stuxnet (Ragan 2011). With the techniques used by Stuxnet now known, other variants such as Duqu are being discovered and countered by security researchers (Laboratory of Cryptography and System Security 2011). It is obvious that the effort required to create, deploy, and maintain Stuxnet and its variants is massive and it is not clear that the rewards are worth the risk and effort. Given the location of initial infection and the number of infected systems in Iran (Falliere, Murchu and Chien 2011) it is believed that Iranian nuclear facilities were the target of the Stuxnet weapon. A significant amount of money and effort was invested in creating Stuxnet but yet the expected result – assuming that this was an attack that expected to damage production – was minimal at best. Iran claimed that Stuxnet caused only minor damage, probably at the Natanz enrichment facility, the Russian contractor Atomstroyeksport reported that no damage had occurred at the Bushehr facility, and an unidentified “senior diplomat” suggested that Iran was forced to shut down its centrifuge facility “for a few days” (Kerr, Rollins and Theohary 2010). Even the most optimistic estimates believe that Iran’s nuclear enrichment program was only delayed by months, or perhaps years (Rosenbaum 2012). The actual damage done by Stuxnet is not clear (Kerr, Rollins and Theohary 2010) and the primary damage appears to be to a higher number than average replacement of centrifuges at the Iran enrichment facility (Zetter 2011). Different targets may produce different results. The Iranian nuclear facility was a difficult target with limited attack vectors because of its isolation from the public Internet and restricted access to its facilities. What is the probability of a successful attack against the U.S. electrical grid and what are the potential consequences should this critical infrastructure be disrupted or destroyed? An attack against the electrical grid is a reasonable threat scenario since power systems are “a high priority target for military and insurgents” and there has been a trend towards utilizing commercial software and integrating utilities into the public Internet that has “increased vulnerability across the board” (Lewis 2010). Yet the increased vulnerabilities are mitigated by an increased detection and deterrent capability that has been “honed over many years of practical application” now that power systems are using standard, rather than proprietary and specialized, applications and components (Leita and Dacier 2012). The security of the electrical grid is also enhanced by increased awareness after a smart-grid hacking demonstration in 2009 and the identification of the Stuxnet malware in 2010; as a result the public and private sector are working together in an “unprecedented effort” to establish robust security guidelines and cyber security measures (Gohn and Wheelock 2010).

#### 9. Cyberattacks impossible – empirics and defenses solve

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

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

#### 11. Status quo redundancy checks space impacts

**Forden, 8** - Massachusetts Institute of Technology (Geoffrey, Astropolitics, 6:138–153, “VIEWPOINT: CHINA AND SPACE WAR,” Ebsco Political Science)

Four days prior to the attack, China would launch the first of its Long March rockets carrying deep-space attack ASATs; the same launch pad would have to be used for the second rocket stacked inside the vertical assembly building. As the technicians renovated that pad, the first rocket’s payload would circle the Earth in a parking orbit at about 300km altitude waiting to be joined by the other deep-space ASATs. This would appear to be a tell-tale sign of an impending strike. China, of course, could explain the delay to the international community by claiming that the third stage, intended to take the payload it its final altitude, had failed to fire and that they were working on it. Roughly six hours before the first the attack on U.S. LEO military satellites, the other three Long March rockets would have to be fired since it takes roughly that long to get their payloads up to their target’s orbits. Delays or failures to launch any of these rockets would strand their interceptors on the launch pad and subject them to possible retaliatory bombing by the U.S.

If all goes as planned, China would have launched between 12 and 16 ASATs, each capable of destroying a strategically important deep-space satellite. However, the U.S. military has many more deep space satellites. Presently, there are 32 functioning GPS navigation satellites even though the original design called for 24.5 In addition, the U.S. has 23 military communications satellites, six early warning satellites that observe missile launches, and six surveillance satellites—most of which detect and monitor electronic transmissions of potential adversaries but one, apparently capable of photoreconnaissance—in GEO orbit.6 These satellites are reinforced by a private network of 90 commercial communications satellites—owned and operated by U.S. corporations—which could be used to replace destroyed military communications satellites, presumably.7 In addition, there are 75 civilian and the 64 military/civilian communications satellites in LEO—although they do not have the same transmission capacity as the GEO satellites.8 The U.S. may be the country most dependent on space for its military activities, but it is also the least vulnerable, because of the tremendous redundancy of its space assets.

### LOAC: 1NC

#### 1. No modeling - strategic incentive to maintain legal ambiguity

**Waxman 11**

Matthew C. Waxman, Associate Professor, Columbia Law School; Adjunct Senior Fellow, Council on Foreign Relations; Member of the Hoover Institution Task Force on National Security and Law, Yale Journal of International Law, March 16, 2011, “Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," vol 36, http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1674565

B. Technology, Power Shifts, and the Strategic Logic of Legal Interpretation With these relationships between law and power in mind, the United States has an interest in regulating cyber-attacks, but it will be difficult to achieve such regulation through international use-of-force law or through new international agreements to outlaw types of cyber-attacks.143 That is **because the distribution of emerging cyber-capabilities** and vulnerabilities— vulnerabilities defined not only by the defensive capacity to block actions but also by the ability to tolerate and withstand attacks—**is unlikely to correspond to** the **status quo distribution of power built on traditional** measures like **military and economic might**. It is not surprising that the United States seems inclined toward an interpretation of Articles 2(4) and 51 that allows it to classify some offensive cyber-attacks as prohibited “force” or an “armed attack” but does not otherwise move previously drawn lines to encompass economic coercion or other means of subversion in that classification. Nor is it surprising to see the United States out in front of other states on this issue. The power and vulnerability distribution that accompanies reliance on networked information technology is not the same as past distributions of military and economic power, **and perhaps not to the U**nited **S**tates**’s advantage relative to rivals**. Moreover, some U.S. strengths are heavily built on digital interconnectedness and infrastructure that is global, mostly private, and rapidly changing; these strengths are therefore inextricably linked to new and emerging vulnerabilities.144 Although some experts assess that the United States is currently strong relative to others in terms of offensive capabilities,145 several factors make the **U**nited **S**tates especially vulnerable to cyber-attack, including the informational and electronic interconnectedness of its military and public and private sectors, and political obstacles to curing some of these vulnerabilities through regulation.146 As the Obama administration’s 2010 National Security Strategy acknowledged: The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority . . . . Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale.147 In other words, U.S. technological strengths create corresponding exposures to threats. The U.S. government is especially constrained politically and legally in securing its information infrastructure—which is largely privately held or privately supplied—against cyber-threats, and these constraints shape its international strategy. Proposals to improve cyber-security through regulation include promulgating industry standards to enhance the security of information technology products and protect networks and computers from intrusion, and, more invasively, expanding the government’s authority to monitor information systems and communications.148 Such proposals invariably face powerful antiregulatory industry pressures and heightened civil liberties sensitivities.149 Information technology industry groups and privacy organizations have together pushed back against moves to impose government security mandates and against more intrusive government cyber-security activities, arguing that they would stifle innovation, erode civil liberties, and fail to keep up with rapidly evolving threats amid a globalized economy.150 A reluctance to secure information systems domestically through government regulation then elevates U.S. government reliance on other elements of a defensive strategy. In that light, **U.S. legal interpretations** **and declaratory postures** that define prohibited force in ways that extend narrow Charter interpretations to take account of cyber-warfare **may be seen as part of an effort to sustain** a legal order in which anticipated U.S. military and economic moves and countermoves against potential adversaries fit quite comfortably—that is, **a legal order that preserves U.S. comparative advantages.** In extending the foundational U.N. Charter prohibition on force to cyber-attacks by emphasizing their comparable effects to conventional military attacks, such interpretations help deny that arsenal to others by raising the costs of its use. At the same time, by casting that prohibition and complementary self-defense authority in terms that help justify military force in response, this interpretation reduces the costs to the United States of using or threatening to use its vast military edge (and it helps signal a willingness to do so). Put another way, the United States appears to be placing hedged bets about what the future strategic environment will look like and how best to position itself to operate and compete in it. On balance, for example, the **U**nited **S**tates may prefer relatively clear standards with respect to cyber-actions that have immediate destructive effects—at least clear enough to justify armed response or deterrence to activities or scenarios deemed threatening—while at the same time preferring some permissive haziness with respect to intelligence collection and its own countermeasures in cyberspace. Such a posture allows the United States to protect itself from hostile penetrations while also preserving some latitude for those activities in which it may be relatively strong.151 Internally, that clarity facilitates planning for contingencies and deliberation about options;152 externally, it may help articulate and deter the crossing of red lines.153 In trying to explain what may be driving the U.S. interpretation, this Article is neither affirming nor denying this strategic logic, which is contingent on future capabilities and vulnerabilities that are both highly uncertain and shrouded in secrecy. Rather, it is trying to uncover and scrutinize some of the underlying assumptions. There are several strategic reasons for the United States to be cautious in considering interpretations that expand narrow definitions of “force” and “attack” so that they include potentially broad categories of cyber-attacks— risks that are often not acknowledged or addressed in discussions of the U.S. interpretive trajectory. For one thing, the United States has generally defeated efforts by other states to interpret Articles 2(4) and 51 expansively to include economic coercion and other forms of political subversion.154 In thinking about the Charter regime as a whole, therefore, the United States may not want to reopen those debates. Cyber-attacks can allow state and nonstate actors to inflict massive harm without resort to arms, but that has long been true of many other instruments, including economic and financial means, covert subterfuge, and other widely used instruments. In that regard, one advantage of promoting legal regulation of cyber-attacks through a new treaty or international agreement instead of through Charter interpretation is that such efforts would have little if any effect on broader Charter law. An advantage, however, to working through Charter interpretation rather than new agreements is that Charter law can evolve incrementally and begin shaping international actors’ expectations through unilaterally initiated state practice without having to reach consensus (the difficulties of which are discussed in the next Section). Depending on the relative risk of different types of future cyber-attack scenarios, it might also be in the United States’s strategic interest to legally delink cyber-activities from armed force instead of defining force by reference to effects, or at least to impose extremely high legal thresholds for treating cyberattacks equivalent to force or armed attack, in order to reduce the chances of military escalation from cyber-activities.155 As capabilities proliferate among state and nonstate actors to conduct various sorts of malicious, hostile, or intelligence-gathering activities in cyberspace, any normative constraints that come from treating some cyber-attacks as force prohibited by Article 2(4) and any deterrence value of treating them as armed attacks triggering self-defense rights under Article 51 might be outweighed by the dangers of lowering legal barriers to military force in a wider range of circumstances.156 That is, the value of promoting a right of armed self-defense against cyber-attacks may turn out to be quite low—since, among other things, it may be difficult to sufficiently prove one’s case publicly in justifying military responses—while doing so may introduce greater security instability to the international system by eroding normative constraints on military responses to nonmilitary harms.157 As the following Section explores, it is very difficult to assess these risk balances because the global security environment is shifting dramatically and unpredictably. Moreover, even if the **U**nited **S**tates could assess the risks accurately, **other states may be operating under different sets of strategic assumptions about that future**. C. Divergent Interests and Implications for Charter Interpretation Assuming the United States decides firmly on a legal interpretation going forward, the redrawing of legal lines on a map of inequitably distributed power and vulnerabilities **would create winners and losers** and would make it difficult to reach agreement on new legal boundaries, whether through interpretive evolution of the U.N. Charter or new conventions.158 In thinking about legal interpretations of Articles 2(4) and 51, success therefore depends on the ability of proponents to articulate and defend their legal lines using combinations of traditional and new forms of power for deterrence, self-defense, enforcement, and influence. Again, one should not divorce analysis of any proposed content of Articles 2(4) and 51 from the processes by which it is interpreted, reinterpreted, enforced, and reinforced.159 The likely factual ambiguity surrounding cyberattacks and the pressures to take aggressive responsive or escalatory measures more quickly than those facts can be resolved may sometimes require strategic and military decisionmaking **amid legal gray zones**. Moreover, as involved states marshal their arguments amid these moves and countermoves, and as they consider their long-term interests, they may also calculate differently what Stone calls “the expected value . . . **of built-in** [**legal**] **ambiguities as future political weapons**.”160 That is, **even if** states widely share a common, minimum interest in restricting some cyber-attacks, **states may have divergent interests regarding specific substantive content** as well as the **desired degree of clarity in the law**. Salient differences will likely stem from asymmetries of geostrategic ambitions, internal and external commitment to legal norms generally, and the nature and extent of public-private institutional relationships.161 In contrast to the **U**nited **S**tates, some states that are developing offensive cyber-warfare capabilities (**such as North Korea**, according to many experts) **are non-status-quo powers** or aspiring regional powers,162 and they **may prefer legal ambiguity** **as to cyber-attacks** or narrow interpretations of Article 51 that would allow them—if they resort to cyber-attacks—to portray themselves as victims of any responsive military strikes.163 Offensive cyber-capabilities have the potential to shift or upset international balances of power, because some states are more vulnerable than others to cyber-attack (in terms of capacity to block actions as well as to tolerate or withstand them), and attacks could have a disproportionately large impact on countries or militaries that have a higher reliance on networked information systems.164 Developing an offensive cyberwarfare capability is likely to be **less expensive** in resources and diplomatic costs **than competing economically or militarily with much stronger states**, though legal flexibility or constraints could alter that calculus.165 On the other hand, some small states that are unlikely to develop sophisticated offensive or defensive systems may advocate international legal interpretations or new agreements that are very restrictive of cyber-attacks and define attacks broadly, seeing themselves as highly reliant on protective norms.166 Individually, though, they will have little power to promote those principles. Like the United States, other major actors may have much to lose from cyber-attacks. However, they may calculate their short- and long-term strategic interests with respect to cyber-warfare and its regulation differently than the United States, in light of their own matrix of offensive and defensive capabilities, public-private institutional relationships, and asymmetries in the ways international law constrains different actors.167 Russia, for example, has proposed to the **U**nited **N**ations a draft statement of principles that would prohibit the development, creation, and use of cyber-attack tools. **Meanwhile, though**, Russia is engaged in developing cyber-attack capabilities,168 and some **analysts are skeptical of Russia’s sincerity in proposing cyber-arms control agreements, especially given the difficulties of verifying them**.169 **China** likely **sees cyber**-warfare capabilities **as a way of equalizing the conventional military superiority of the U**nited **S**tates,170 so it may be reluctant to concede legally “disarming” interpretations, at least without some reciprocal benefit or legal concession. Russia and China, which, as mentioned earlier, both reportedly exploit informal relationships with private actors (i.e., “citizen hackers”) to conduct attacks and collect intelligence in cyberspace, may also incline toward legal doctrine that makes it difficult to impute private cyber-actions to governments.171 Meanwhile, some European states have approached the legal relationship between cyber-attacks and force cautiously, perhaps because of general concerns about military escalation of crises and divergent strategic assessments among themselves.172 Differences in internal politics, ideology, and government control over information will also shape state interests in competing interpretations of Charter norms. With echoes of debates from prior eras,173 various types of states are likely to view cyber-threats differently and to distinguish offensive attacks from defensive measures differently. For instance, some states that tightly control information, including major powers like China, are especially concerned about internal political dissent and might therefore define what the United States sees as “Internet freedom” as a threat to vital security interests. Efforts to crack down on what they (or other states that exercise strong state control over Internet content) may view as defensive measures against hostile subversion may be viewed by the United States (or other states that value and promote free speech) as hostile, offensive measures.174 It is hard to envision a state in China’s position strongly endorsing or standing behind U.S. visions for international legal regulation of cyber-attacks **without** some **unlikely concessions by the U**nited **S**tates.175 From a policy standpoint, this should sound another cautionary note about efforts to build international legal consensus about cyber-attacks and the use of force, whether through Charter interpretation or new agreements. Emergent U.S. government inclinations toward effects-based interpretations of the Charter may be legally reasonable and protective of some core U.S. interests, as well as widely shared foreign interests. But even if they help in the short term to manage competing risks of too much or too little authority to employ cyberattacks, or too much or too little leeway to resort to armed self-defense in response, a coherent legal strategy can only be forged and advanced in the long term if it is integrated effectively with broader diplomacy and security strategy, including efforts to build and sustain offensive, defensive, deterrent, and intelligence capabilities—while others do the same based on a different set of objectives, capabilities, vulnerabilities, and constraints.

#### 2. International law doesn’t change state action

**Posner 12** (Eric, law prof, Slate, “Obama’s Drone Dilemma”, Oct. 8, 2012, http://www.slate.com/articles/news\_and\_politics/view\_from\_chicago/2012/10/obama\_s\_drone\_war\_is\_probably\_illegal\_will\_it\_stop\_.single.html)

The Wall Street Journal recently reported on debates within the Obama administration about the legality of the drone war in Pakistan. State Department legal adviser Harold Koh, the former dean of Yale Law School and even more former darling of the left for his criticisms of the Bush administration’s aggressive theories of executive power, plays a prominent role in them. Koh apparently concluded that the drone war “veers near the edge” of illegality but does not quite tumble over it. That is a questionable judgment. The U.N. Charter permits countries to use military force abroad only with the approval of the U.N. Security Council, in self-defense, or with the permission of the country in which military force is to be used. The U.N. Security Council never authorized the drone war in Pakistan. Self-defense, traditionally defined to mean the use of force against an “imminent” armed attack by a nation-state, does not apply either, because no one thinks that Pakistan plans to invade the United States. That leaves consent as the only possible legal theory. But Pakistan has never consented to the drone war. Publicly and officially the country has opposed it. Before the raid that killed Osama bin Laden in May 2011, the CIA sent a fax every month to Pakistan’s Inter-Services Intelligence agency that would identify the airspace in which drones would be sent. The ISI would send back an acknowledgment that it had received the fax, and the U.S. government inferred consent on the basis of the acknowledgments. But after the raid, the ISI stopped sending back the acknowledgments. Now what to do? The administration argues that consent can still be inferred despite the unanswered faxes. The reason is that “the Pakistani military continues to clear airspace for drones and doesn’t interfere physically with the unpiloted aircraft in flight”—meaning that Pakistan does not shoot down the drones or permit private aircraft to collide with them. We might call this “coerced consent.” Consider it this way: You walk into a jewelry store and the proprietor announces that he will deem you to have consented to the purchase of a diamond tiara for $10,000, despite all your protests to the contrary, unless you use physical force to stop him as he removes your wallet from your pocket. Imagine further that he’s 7 feet tall and weighs 400 pounds. This is what a Pakistani official meant when he told the Wall Street Journal that shooting down a drone would be “needlessly provocative.” He meant that such an action would risk provoking retaliation from the United States, a risk that Pakistan cannot afford to take. Because Pakistan lies prostrate and endures the pummeling rather than makes a futile effort to stop it, it is deemed to consent to the bombing of its own territory. But don’t blame government lawyers like Koh for devising this theory. **International law lacks the resources for constraining the U.S. government**. Koh knows this now if he did not before. Since he built his academic career on the claim that international law can and should be used to control nation-states and harshly criticized the Bush administration for violating international law, this must have been a bitter pill to swallow. (Though he has swallowed so many bitter pills that perhaps he has lost his sense of taste: The man who told the Senate at the end of the Bush administration that the United States must “unambiguously reassert our historic commitments to human rights and the rule of law as a major source of our moral authority” has backed away from his earlier opposition to expansive war powers, targeted killing, military commissions, and military detention.) The weakness of international law governing the use of military force goes back to the signing of the U.N. Charter in 1945. The founders understood that a simple rule prohibiting the use of military force except in self-defense, or with the consent of another state, would not be adequate for regulating war. But they could not draft a code complex enough to anticipate all the contingencies that might justify war. Instead they set up the Security Council and reasoned that this body could determine when war might be justified for purposes other than self-defense. But the Security Council was frozen first by the Cold War rivalry between the United States and the Soviet Union, and then the cold peace rivalries between the United States, Russia, and China. It has authorized only two wars since its inception (the Korean War and the first Iraq War; it also retroactively approved the U.S. invasion of Afghanistan in 2001). **Needless to say, there have been dozens of wars since 1945.** Participants have included countries as diverse as China, the Soviet Union, India, Pakistan, the United Kingdom, Vietnam, Iran, Iraq, Egypt, Israel, and Argentina. Even the supposedly pacific European countries participated via NATO in several of these wars. The United States has on several occasions justified wars (for example, in Kosovo in 1999, Libya in 2011) as humanitarian interventions—a principle that can be found nowhere in the U.N. Charter but enjoys some international support. In other cases, including current drone operations in Pakistan, the United States has invoked a new idea of the “unable or unwilling” country, one that outside powers can invade because that country cannot prevent terrorists located on its territory from launching attacks across its borders. But most U.S. wars can be fit into these two categories only with difficulty. Those wars are undertaken to shut down a destabilizing or dangerous regime, one that typically has used violence to keep itself in power. One can put the second Iraq War in this category, as well as the Panama intervention in 1990, the interventions in Yugoslavia in the 1990s, and the intervention in Granada in 1983. During the Cold War, the United States also often evaded the U.N. prohibition on interstate war by funding and training a domestic insurgency. The U.N. Charter does not permit states to use military force to unilaterally address long-term threats in this way. It is too easy for states to characterize other states as long-term threats regardless of whether they are. And yet this omission rendered the charter unworkable, because all states must take long-term threats seriously, whether or not the members of the Security Council can be persuaded or bribed to agree with them. Government lawyers like Koh must **scramble to revise their interpretation of international law** so as to keep up with the new events that justify, in the eyes of the president, a military intervention. The “coerced consent” doctrine, the “unable and unwilling” doctrine, and the exception for humanitarian intervention all **whittle away at whatever part of the law on United Nations use of force blocks U.S. goals**. If the United States ever decides to invade Iran in order to prevent it from acquiring nuclear weapons, **expect a new doctrine to take shape**, perhaps one that emphasizes the unique dangers of nuclear weapons and Iran’s declared hostility toward a nearby country. It is curious that **there is not a global outcry about the illegality of the wars in Pakistan or Libya**, as there was about the illegality of the recent war in Iraq, which the Bush administration dubiously justified on the basis of Iraq’s violations of earlier U.N. resolutions that had suspended hostilities after the first Iraq War. Maybe the world doesn’t care as much about Pakistan, which has no oil. Or maybe people have finally realized that the United States, which has been almost continuously at war since the collapse of the Soviet Union, **will not be swayed by legal arguments. A powerful army is too useful not to use**, whether you are a Republican president or a Democratic one.

#### 3. Legal limitations on war powers not key and a laundry list of military invasions thump their internal link.

**Posner 13** (Eric, law prof, “The U.S. Has No Legal Basis to Intervene in Syria”, Aug. 28, 2013, http://www.slate.com/articles/news\_and\_politics/view\_from\_chicago/2013/08/the\_u\_s\_has\_no\_legal\_basis\_for\_its\_action\_in\_syria\_but\_that\_won\_t\_stop\_us.html)

Inter arma enim silent leges, said the Romans—in times of war, the law falls silent. But ours is a chattier society. Rather than keep silent, **our laws speak loudly about war. We just don’t follow them**—as the U.S. military intervention in Syria is about to show. Press reports say that President Obama has ordered his lawyers to supply him with a legal justification for a military assault on Syria, and unnamed officials have cited the Geneva Protocol, the Chemical Weapons Convention, the Kosovo precedent, and the so-called Responsibility to Protect doctrine. They have not cited the United Nations Charter, which flatly bans military interventions without Security Council approval, which the United States cannot obtain because of Russian and Chinese opposition. The Geneva Protocol of 1925 (which Syria ratified) and the Chemical Weapons Convention of 1993 (which Syria has not ratified) ban the use of chemical weapons, but do not authorize countries to attack other countries that violate these treaties. The United States has no more authority to attack Syria for violating these treaties than it does to bomb Europe for giving import preferences to Caribbean banana producers in violation of international trade law. At one time, countries could use military force as “countermeasures” against treaty violators, but only against violators that harmed the country in question—and Syria has not used chemical weapons against the United States—but in any event, that rule has been superseded by the U.N. Charter. The Kosovo precedent refers to the 1999 military intervention in Serbia, launched to stop a campaign of ethnic cleansing against people living in that region of Serbia. Then, too, the United States failed to obtain approval from the Security Council but attacked anyway. It’s odd to claim the Kosovo attack as a precedent, as it was widely regarded as illegal at the time and afterward. But most people, or at least Westerners, believed that the Kosovo intervention was morally justified because it stopped a massacre, and efforts were made to carve out an exception to the U.N. rules, so that a “humanitarian intervention” would be lawful even without Security Council approval. That effort failed because people believed it would be too easy for countries to use humanitarian intervention as a pretext for attacking countries for other reasons. After all, humanitarian conditions are bad in nearly all countries that someone might like to invade. Instead, an international conference hammered together a compromise that all countries have a “Responsibility to Protect” their own citizens and citizens of other countries. But this idea was never sanctified in a treaty and is not law. The most honest thing to do would be to admit that the **international law on the use of force is defunct**, as professor Michael Glennon has argued. **Virtually all major countries have broken the rules** from time to time, even the saintly European countries that joined in the Kosovo intervention. The U.S. has **ignored the U.N. rules on numerous occasions**—Vietnam, Grenada, Panama, Kosovo, the second Iraq War, and the 2011 war in Libya, where it secured an authorization to stop massacres of civilians but violated its terms by seeking regime change. But the U.S. government does not repudiate the U.N. rules because it wants other countries to comply with them. On the domestic front, things are hardly better. The Constitution gives Congress, not the executive, the power to declare war, and at present writing, the administration seems unlikely to ask Congress for authorization lest it say no. This too would be a repeat of the Libya intervention, which lacked congressional authorization. To avoid the impression that the president can go to war whenever he wants, pretty much in clear violation of the founders’ intentions, the executive branch has invented a number of largely phony limits on executive military action. At one point the theory was that the executive may send military forces anywhere in the world in order to discharge its responsibility to protect Americans or American property, a theory that was used to justify the use of military force without congressional authorization in Somalia in 1992–1993. One might wonder whether such a theory imposes any limits; one might ask, “In what country are there no Americans or American property that could be protected?” Syria, it turns out. No one alleges that the Syrian government poses a threat to Americans or American property, so the Obama administration can’t fall back on that theory, and doesn’t seem inclined to. But the executive branch claims the authority to use military intervention to protect the “national interest,” and it is not hard to find a national interest at stake. Ironically, the Justice Department’s Libya opinion identified “maintaining the credibility of the United Nations Security Council and the effectiveness of its actions to promote international peace and security” as one of the national interests justifying military intervention without congressional approval. Don’t expect a repeat of that argument in the Syria opinion. The other national interest was that of promoting regional stability—also not a good one here either, since no one seems to think that lobbing some cruise missiles onto Syrian soil will promote regional stability. Most likely the government will argue that there is a (heretofore ignored) national interest in deterring the use of chemical weapons as well as in protecting foreign civilians from massacres. With “national interest” so capaciously understood, it is clear that the president will always be able to find a national interest justifying a military intervention, so there are no constitutional constraints on his power to initiate military intervention. Congress tried to bring the executive under control back in 1973 by enacting the War Powers Resolution, which can be read to implicitly authorize the use of military force as long as the president reports back to Congress and withdraws forces after 60 days unless Congress gives authorization in the interim. In 2011 President Obama ignored a Justice Department opinion that he must end the use of force in Libya, instead obtaining a compliant legal opinion from White House Counsel Robert Bauer and State Department Legal Adviser Harold Koh, who argued that the bombings and killings in Libya did not amount to “hostilities” and so did not trigger the withdrawal provision in the War Powers Resolution. In another indication of the administration’s respect for Congress, earlier this month the administration refused to call the coup in Egypt a coup so as to evade a statute that requires a cutoff of foreign aid to countries in which a military coup overthrows a democratically elected leader. One can be cynical or realistic. I prefer the latter. The Romans had it right: **It is not realistic to put legal constraints on war powers.** Law works through general prospective rules that apply to a range of factual situations. International relations and national security are too fluid and unpredictable to be governed by a set of legal propositions that command general assent secured in advance. Laws governing war make us feel more secure but they **don’t actually make us more secure.** So while it is satisfying to fling the charge of hypocrisy at the president and his lawyers, and we might disagree about the wisdom of an attack on Syria, let’s just hope that when they invoke the law, they don’t actually believe what they are saying.

#### 5. Consultation won’t be genuine – the president will just lie to get what he wants

Grimmett 8 [Grimmett; 24 April 2008; “WAR POWERS FOR THE 21ST CENTURY: THE EXECUTIVE BRANCH PERSPECTIVE HEARING BEFORE THE SUBCOMMITTEE ON INTERNATIONAL ORGANIZATIONS, HUMAN RIGHTS, AND OVERSIGHT OF THE COMMITTEE ON FOREIGN AFFAIRS”; House of Representatives (110th Congress), Second Session; Serial No. 110-168; Printed for the use of the Committee on Foreign Affairs; <http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg41989/pdf/CHRG-110hhrg41989.pdf>]

Mr. GRIMMETT. I would just add one thing. We are talking about consultation, so we are talking about two branches of government. And even if you organized the committee structure or the new entity, however you want to characterize it, at this end, you are still going to confront the reality of the executive branch that has been very chary about giving information out, especially on something as sensitive as possible war activity or military operations, because of concerns about operational security and about people having the proper clearances and all that sort of thing. And even though most of the major committees that deal with foreign defense policy or intelligence have got the security clearances, the fact is there is a very, very strong reluctance on the part of the executive branch, based on past history, to even engage people on that level. So if you have a committee of 45 members, I mean, the likelihood of them wanting to engage that committee on the most sensitive operational activities that they may be contemplating is pretty slim, unless some new millennium has occurred that, based on new experiences, that we are not fully aware of.

#### 9. No War

#### a) Economic interdependence

Greg Austin Senior visiting fellow in the department of War Studies at King’s College London and Franz-Stefan Gady, adjunct research assistant at the Institute for National Strategies Studies of the National Defense University, 2012 (CYBER DEtEntE BEtWEEn tHE UnItED StAtES AnD CHInA: SHAPING THE AGENDA, EastWest Institute, <http://www.ewi.info/system/files/detente.pdf>)

The cost to global economic stability would likely be very high if there were a major confrontation between China and the United States. Sustained or repeated interruptions in connectivity, corruption of transaction data, or deletion of commercial records on a large scale could have major negative repercussions for the global economy. Whether confidence after such attacks could be restored remains an open question. These costs would be so high that they should at least dampen if not fully deter states from resorting to cyber war. Cyberspace only amplifies traditional interdependence in trade.

#### b) Different goals

Brandon Valeriano and Ryan Maness, 2012 (In Derek S. Reveron, 2012 (Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, Georgetown University Press, accessed via Project Muse, Chapter 9)

Along with offensive cyber capabilities comparable to those of the United States, the Chinese government also has complete control of its Internet infrastructure.23 If China were to come under a serious cyber attack, the government could shut off access to all international web portals, thus containing and suppressing the attack. This capability is not something that the United States can claim because the multi­ple access points are privately owned by a number of diverse firms over which the government has no control. Therefore, in terms of cyberwar capabilities, it can be argued that China has a definite advantage over the United States. Nevertheless, we have a problem with a potential cyber conflict between the United States and China; these two countries are not considered to be rivals under any rivalry dataset. There is no history of serious disputes on the level of historic examples such as the United States and the Soviet Union or India and Pakistan. Despite claims by pundits, China and the United States are not on a collision course. China's main foreign policy objective seems to be economic expansion, and there is little chance it will be able to compete militarily or economically

with the United States in the near future.24 If the two main heavyweights often thought to be likely to fight in the near future are not rivals and are thus unlikely to fight, what danger is there from their immense cyber capabilities?

# 2NC

## T

### Emory OCO T: Overview 2NC

#### Bidirectionality – Absent prohibition they can create conditions that functionally increase authority

Posner 12 (Eric, University of Chicago Law, “Deference to the Executive in the United States After September 11: Congress, the Courts, and the Office of Legal Counsel”, <http://ericposner.com/DEFERENCE%20TO%20THE%20EXECUTIVE.pdf>)

To see why, consider an example in which the President must choose an action that lies on a continuum, such as electronic surveillance. At one extreme, the President can engage in actions that are clearly lawful—for example, spying on criminal suspects after obtaining warrants from judges. At the other extreme, the President can engage in actions that are clearly unlawful—for example, spying on political opponents. OLC opinions will not affect Congress's or the public's reaction to either the obviously lawful or the obviously unlawful actions. But then there are middle cases. Consider Policy L, which is just barely legal, and Policy I, which is just barely illegal. The President would like to pursue Policy L but fears that Congress and others will mistakenly believe that Policy L is illegal. As a result, political opposition to Policy L will be greater than it would be otherwise. In such a case, a favorable advisory opinion from a neutral legal body that has credibility with Congress will help the President.\* OLC approval of Policy L would cause political opposition (to the extent that it is based on the mistaken belief that Policy L is unlawful) to melt away. Thus, the OLC enables the President to engage in Policy L, when without OLC participation that might be impossible. True, the OLC will not enable the President to engage in Policy I, assuming OLC is neutral. Indeed, OLC's negative reaction to Policy / might stiffen Congress's resistance. Nevertheless, the President will use the OLC only because he believes that on average, the OL C will strengthen his hand. An analogy to contract law might be illuminating. People enter contracts because they enable them to do things ex ante by imposing constraints on them ex post. For example, a debtor can borrow money from a creditor only because a court will force the debtor to repay the money ex post. It would be strange to say that contract law imposes "constraints" on people because of ex post enforcement. In fact, contract law enables people to do things that they could not otherwise do—it extends their power. If it did not, people would not enter contracts.

#### Broad interpretations cause unmanageable research burdens

Taylor III, now a JD from William and Mary, 2005

(Jarred, “Searching for a More Perfect Union,” https://docs.google.com/document/d/1ypiOXjRVPWzNxDsFVJ0S1n-QfIGtXzp7Y59meEwd-bE/edit?hl=en\_US)

**It would take even the most seasoned scholar years of research and hundreds of pages to** adequately **analyze** the development of **any presidential power** over the course of American history; **war power is** certainly **no exception**. Every President since George Washington has interpreted the martial prerogatives of his office in different ways, and most have set some sort of precedent for succeeding officeholders. Nevertheless, some of the major changes in executive military power bear highlighting.

## DETERR

### Deterrence: Ext 1/U Strong Deterrent Now

#### US cyber deterrence is strong now

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

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

### Deterrence: Ext 2-4/Links

#### No time to consult congress – attack too fast – deterrent capabilities requires fast action

Stephen Dycus (Proffesor at Vermont Law School) August 11 2010 “Congress’s Role in Cyber Warfare,” <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>

In other ways, cyber weapons are critically different from their nuclear ¶ counterparts. For one thing, the time frame for response to a cyber attack ¶ might be much narrower. A nuclear weapon delivered by a land-based ¶ ICBM could take 30 minutes to reach its target. An electronic attack would ¶ arrive instantaneously, and leave no time to consult with or even inform ¶ anyone outside the executive branch before launching a counterstrike, if ¶ that were U.S. policy

#### Rapid response key to deterrence

Defense News March 24 2012

<http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive>

The offensive cyber weapons that have long been wielded by centralized authorities, but whose existence was rarely acknowledged, are being distributed to regional combatant commanders as part of a new emphasis on deployment and deterrence.¶ “Our capabilities represent key components of deterrence,” Army Gen. Keith Alexander, National Security Agency (NSA) and U.S. Cyber Command (CYBERCOM) chief, wrote in prepared remarks delivered to the House Armed Services emerging threats and capabilities subcommittee as part of a routine budget hearing March 20. The new initiative did not come up during the hearing.¶ “I can assure you that, in appropriate circumstances and on order from the National Command Authority, we can back up the department’s assertion that any actor threatening a crippling cyber attack against the United States would be taking a grave risk,” he wrote.¶ Part of that aggressive posture comes in the form of arming combatant commanders, allowing for broader access to capabilities, more rapid action, and the pairing of traditional kinetic attacks with newly developed cyber capabilities

#### No link turns—US threat of use causes defensive buildup, not offensive

Libicki 2012(Martin, Senior Management Scientist at the RAND Corporation, "Crisis and Escalation in Cyberspace", http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND\_MG1215.pdf)

Nevertheless, the logic that states have to develop offensive cyber-weapons because their rivals do has little basis in theory or fact. First, states have little knowledge of exactly what weapons, as such, are in the arsenal of their rivals. 13 Indeed, if they actually knew precisely what weapons their foes had, they might well know what vulnerabilities such weapons targeted and would fix such vulnerabilities, thereby nullify-ing these weapons. Second, as noted, the best response to an offensive weapon is a defensive weapon, not another offensive weapon. Third, the whole notion of offense-versus-offense requires that the underlying dynamic of attack and retaliation actually makes sense as a warfight-ing and war-termination strategy. Were that so, deterrence would be primary. But deterrence is a very difficult notion in cyberspace. 14 States wanting to hide their own tracks in a cyberattack have a wealth of ways to do so and, often, more than enough motive. Incidentally, it is hard to imagine how an arms race in cyberspace could come close to having a major economic impact. The intellectual skills required to compete in this contest are so specialized that states will run out of such people well before they run out of money paying them.

#### The link takes out solvency—perception of credible deterrent is key to deter cheating

Stewart **Baker**, 9/30/**11** (Denial of Service, Foreign Policy, <http://www.foreignpolicy.com/articles/2011/09/30/denial_of_service>)

American lawyers' attempts to limit the scope of cyberwar are just as certain to fail as FDR's limits on air war -- and perhaps more so. It's true that half a century of limited war has taught U.S. soldiers to operate under strict restraints, in part because winning hearts and minds has been a higher priority than destroying the enemy's infrastructure. But it's unwise to put too much faith in the notion that this change is permanent. Those wars were limited because the stakes were limited, at least for the United States. Observing limits had a cost, but one the country could afford. In a way, that was true for the Luftwaffe, too, at least at the start. They were on offense, and winning, after all. But when the British struck Berlin, the cost was suddenly too high. Germans didn't want law and diplomatic restraint; they wanted retribution -- an eye for an eye. When cyberwar comes to America and citizens start to die for lack of power, gas, and money, it's likely that they'll want the same. More likely, really, because Roosevelt's bargain was far stronger than any legal restraints we're likely to see on cyberwar. Roosevelt could count on a shared European horror at the aerial destruction of cities. The modern world has no such understanding -- indeed, no such shared horror -- regarding cyberwar. Quite the contrary. For some of America's potential adversaries, the idea that both sides in a conflict could lose their networked infrastructure holds no horror. For some, a conflict that reduces both countries to eating grass sounds like a contest they might be able to win. What's more, cheating is easy and strategically profitable. America's compliance will be enforced by all those lawyers. Its adversaries' compliance will be enforced by, well, by no one. It will be difficult, if not impossible, to find a return address on their cyberattacks. They can ignore the rules and say -- hell, they are saying -- "We're not carrying out cyberattacks. We're victims too. Maybe you're the attacker. Or maybe it's [Anonymous](http://anonops.blogspot.com/). Where's your proof?" Even if all sides were genuinely committed to limiting cyberwar, as they were in 1939, history shows that it only takes a single error to break the legal limits forever. And error is inevitable. Bombs dropped by desperate pilots under fire go astray -- and so do cyberweapons. Stuxnet infected thousands of networks as it searched blindly for Iran's uranium-enrichment centrifuges. The infections lasted far longer than intended. Should we expect fewer errors from code drafted in the heat of battle and flung at hazard toward the enemy? Of course not. But the lesson of all this for the lawyers and the diplomats is stark: Their effort to impose limits on cyberwar is almost certainly doomed. No one can welcome this conclusion, at least not in the United States. The country has advantages in traditional war that it lacks in cyberwar. Americans are not used to the idea that launching even small wars on distant continents may cause death and suffering at home. That is what drives the lawyers -- they hope to maintain the old world. But they're being driven down a dead end. If America wants to defend against the horrors of cyberwar, it needs first to face them, with the candor of a Stanley Baldwin. Then the country needs to charge its military strategists, not its lawyers, with constructing a cyberwar strategy for the world we live in, not the world we'd like to live in. That strategy needs both an offense and a defense. The offense must be powerful enough to deter every adversary with something to lose in cyberspace, so it must include a way to identify attackers with certainty. The defense, too, must be realistic, making successful cyberattacks more difficult and less effective because resilience and redundancy has been built into U.S. infrastructure. Once the United States has a strategy for winning a cyberwar, it can ask the lawyers for their thoughts. But it can't be done the other way around. In 1941, the British sent their most modern battleship, the Prince of Wales, to Southeast Asia to deter a Japanese attack on Singapore. For 150 years, having the largest and most modern navy was all that was needed to project British power around the globe. Like the American lawyers who now oversee defense and intelligence, British admirals preferred to believe that the world had not changed. It took Japanese bombers 10 minutes to put an end to their fantasy, to the Prince of Wales, and to hundreds of brave sailors' lives. We should not wait for our own Prince of Wales moment in cyberspace.

### Extension 1NC 5 attribution

#### Lack of attribution makes cyber law ineffective

Moss 4/19/13 – 1AC Author (Trefor, covers Asian politics, defence and security, and was Asia-Pacific Editor at Jane’s Defence Weekly until 2009 The Diplomat- - “Is Cyber War the New Cold War?”, http://thediplomat.com/2013/04/19/is-cyber-war-the-new-cold-war/3/, zzx)

However, cyber complicates the application of the existing law in two ways. The victim of a cyber attack might hide the fact that the attack ever took place so as not to reveal its vulnerability to other potential aggressors. Even more importantly, it is hard to attribute a cyber attack to another state in a way that would satisfy international law, given the attacking state’s likely use of proxies. The first challenge that states face is therefore proving the origin of an attack. Secondly, states have to decide how to respond legally and effectively to cyber crime and cyber espionage. So far the governments have seemed inclined either to accept such attacks as a fact of interconnected life, or to try to retaliate with cyber operations of their own. The former approach only encourages further aggression, while the latter probably breaches international law if the original hack was not an example of the use of force. In future, the victims of virtual theft might instead focus on gathering evidence and then seek reparations at the World Trade Organisation or the International Court of Justice, much as they would do in cases of IP theft or breaches of sovereignty.

### Extension 1NC 6 Congress Not Key

#### And, Dycus is wrong—Congress not needed

**Brecher, 2012**. (Aaron, Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations, 111 Michigan Law Review, No 3, p 423, L/N)

Some scholars have proposed a contrary view. On this view, the speed with which cyberspace events can play out makes it important for the legislative role to be clearly established via statutory reform in advance of any cyberattack by the United States. [n157](http://www.lexisnexis.com.ezp1.lib.umn.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1374611534093&returnToKey=20_T17845089181&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.59498.56057527503#n157) Thus, proposals for extensive legislative intervention would help ensure Congress's appropriate role in deciding whether or not to go to war. [n158](http://www.lexisnexis.com.ezp1.lib.umn.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1374611534093&returnToKey=20_T17845089181&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.59498.56057527503#n158) The notion of congressional participation is well in line with the view of shared constitutional war powers articulated earlier in this Note. [n159](http://www.lexisnexis.com.ezp1.lib.umn.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1374611534093&returnToKey=20_T17845089181&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.59498.56057527503#n159) Moreover, congressional participation comports with an ideal of government decisionmaking where the branch most immediately accountable to voters has been given a chance to express its view. Discussing the covert action regime, Stephen Dycus, professor of law at Vermont Law School, expresses concern that only the smaller group of intelligence committee leaders and the leaders of each House will be informed, and that in general the reporting requirements do not ensure that Congress will obtain the information it needs to play a meaningful role in the discussion. [n160](http://www.lexisnexis.com.ezp1.lib.umn.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1374611534093&returnToKey=20_T17845089181&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.59498.56057527503#n160) Additionally, there are concerns regarding the traditional military activities exception to the reporting requirements in the covert action statute. [n161](http://www.lexisnexis.com.ezp1.lib.umn.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1374611534093&returnToKey=20_T17845089181&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.59498.56057527503#n161) Specifically, the worry is that the military might classify clandestine cyberwarfare activities as "operational preparation of the environment" and thereby skirt the reporting requirements, being accountable instead to the congressional armed services committees - which could create confusion. [n162](http://www.lexisnexis.com.ezp1.lib.umn.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1374611534093&returnToKey=20_T17845089181&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.59498.56057527503#n162) Dycus's proposed legislative reforms include designating particular congressional committees to receive reports, forming a lead federal agency for cybersecurity, banning automated offensive responsive to a cyberattack, and crafting procedures to aid private networks that come under attack. [n163](http://www.lexisnexis.com.ezp1.lib.umn.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1374611534093&returnToKey=20_T17845089181&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.59498.56057527503#n163) However, this position is flawed because it dismisses the covert action statute as wholly inadequate to protecting the value of congressional participation, and gives short shrift to the non-warlike dimensions of many [\*450] cyberattacks. The worry that motivates some of the proposals seems to ignore the many examples of cyberattacks - such as manipulation of electronic ballots in a foreign election or disseminating false information through foreign networks to affect media reports - that, outside normal contexts, could not plausibly fall under the military activities exception. Moreover, they underestimate the potential power of a presumption by the executive in favor of the covert action regime. An executive order establishing such a presumptive posture of reporting could go a long way toward bringing Congress into the process. First, an order establishing written findings and congressional reporting as the default rule could cause momentum to settle around title 50 procedures for initiating cyberattacks. [n164](http://www.lexisnexis.com.ezp1.lib.umn.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1374611534093&returnToKey=20_T17845089181&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.59498.56057527503#n164) Also, one scholar has argued that the most effective way to ensure congressional notification might not be changing the actual rules of who is to be notified and when, but rather implementing changes that encourage the executive branch to comply with existing requirements. [n165](http://www.lexisnexis.com.ezp1.lib.umn.edu/lnacui2api/frame.do?reloadEntirePage=true&rand=1374611534093&returnToKey=20_T17845089181&parent=docview&target=results_DocumentContent&tokenKey=rsh-20.59498.56057527503#n165)

### Extension 1NC 8-10 Cyberwar Infeasbale

We don’t have to prove that a cyber attack is impossible, just that high costs will cause enemies to seek alternatives

Rid, reader in war studies – King's College London, and McBurney, professor – Agents and Intelligent Systems Group – Department of Informatics @ King's College, ‘12 (Thomas and Peter, “Cyber-Weapons,” *The RUSI Journal* Volume 157, Issue 1, p. 6-13)

A thorough conceptual analysis and a detailed examination of the empirical record corroborates our hypothesis: developing and deploying potentially destructive cyber-weapons against hardened targets will require significant resources, hard-to-get and highly specific target intelligence, and time to prepare, launch and execute an attack. Attacking secured targets would probably require the resources or the support of a state actor; terrorists are unlikely culprits of an equally unlikely cyber-9/11. The scant empirical record also suggests that the greatest benefit of cyber-weapons may be using them in conjunction with conventional or covert military strikes, as Israel did when it blinded the Syrian air defence in 2007. This leads to a second conclusion: the cost-benefit payoff of weaponised instruments of cyber-conflict may be far more questionable than generally assumed: target configurations are likely to be so specific that a powerful cyber-weapon may only be capable of hitting and acting on one single target, or very few targets at best. The equivalent would be a HARM missile that can only destroy one unique emitter, not a set of targets emitting at the same frequency. But in contrast to the missile – where only the seeker needs to be specifically reprogrammed and the general aviation and propulsion systems remain functional – the majority of modular components of a potent cyber-weapon, generic and specific, would have a rather short shelf-life after discovery. Two findings contravene the debate's received wisdom. One insight concerns the dominance of the offence. Most weapons may be used defensively and offensively. But the information age, the argument goes since at least 1996, has ‘offence-dominant attributes’.37 A 2011 Pentagon report on cyberspace again stressed ‘the advantage currently enjoyed by the offense in cyberwarfare’.38 But when it comes to cyber-weapons, the offence has higher costs, a shorter shelf-life than the defence, and a very limited target set.39 All this drastically reduces the coercive utility of cyber-attacks. Any threat relies on the offender's credibility to attack, or to repeat a successful attack. Even if a potent cyber-weapon could be launched successfully once, it would be highly questionable if an attack, or even a salvo, could be repeated in order to achieve a political goal. At closer inspection cyber-weapons do not seem to favour the offence. A second insight concerns the risk of electronic arms markets. One concern is that sophisticated malicious actors could resort to asymmetric methods, such as employing the services of criminal groups, rousing patriotic hackers, and potentially redeploying generic elements of known attack tools. Worse, more complex malware is likely to be structured in a modular fashion. Modular design could open up new business models for malware developers. In the car industry, for instance,40 modularity translates into a possibility of a more sophisticated division of labour. Competitors can work simultaneously on different parts of a more complex system. Modules could be sold on underground markets. But if our analysis is correct, potential arms markets pose a more limited risk: the highly specific target information and programming design needed for potent weapons is unlikely to be traded generically. To go back to our imperfect analogy: paintball pistols will continue to be commercially available, but probably not pre-programmed warheads of smart missiles.

#### That’s a key framing issue—probability (not magnitude) is key for cyberwar

Cavelty, October 22, 2012 (Myriam Dunn, The Militarisation of Cyber Security as a Source of Global Tension, <http://isn.ch/Digital-Library/Articles/Special-Feature/Detail/?lng=en&id=153888&tabid=1453349960&contextid774=153888&contextid775=153887> )

Since the potentially devastating effects of cyber attacks are so scary, the temptation is very high not only to think about worst-case scenarios, but also to give them a lot of (often too much) weight despite their very low probability. However, most experts agree that strategic cyber war remains highly unlikely in the foreseeable future, mainly due to the uncertain results such a war would bring, the lack of motivation on the part of the possible combatants, and their shared inability to defend against counterattacks. Indeed, it is hard to see how cyber attacks could ever become truly effective for military purposes: It is exceptionally difficult to take down multiple, specific targets and keep them down over time. The key difficulty is proper reconnaissance and targeting, as well as the need to deal with a variety of diverse systems and be ready for countermoves from your adversary. Furthermore, nobody can be truly interested in allowing the unfettered proliferation and use of cyber war tools, least of all the countries with the offensive lead in this domain. Quite to the contrary, strong arguments can be made that the world’s big powers have an overall strategic interest in developing and accepting internationally agreed norms on cyber war, and in creating agreements that might pertain to the development, distribution, and deployment of cyber weapons or to their use (though the effectiveness of such norms must remain doubtful). The most obvious reason is that the countries that are currently openly discussing the use of cyber war tools are precisely the ones that are the most vulnerable to cyber warfare attacks due to their high dependency on information infrastructure. The features of the emerging information environment make it extremely unlikely that any but the most limited and tactically oriented instances of computer attacks could be contained. More likely, computer attacks could ‘blow back’ through the interdependencies that are such an essential feature of the environment. Even relatively harmless viruses and worms would cause considerable random disruption to businesses, governments, and consumers. This risk would most likely weigh much heavier than the uncertain benefits to be gained from cyber war activities. Certainly, thinking about (and planning for) worst-case scenarios is a legitimate task of the national security apparatus. Also, it seems almost inevitable that until cyber war is proven to be ineffective or forbidden, states and non-state actors who have the ability to develop cyber weapons will try to do so, because they appear cost-effective, more stealthy, and less risky than other forms of armed conflict. However, cyber war should not receive too much attention at the expense of more plausible and possible cyber problems. Using too many resources for high- impact, low-probability events – and therefore having less resources for the low to middle impact and high probability events – does not make sense, neither politically, nor strategically and certainly not when applying a cost-benefit logic.

### Extension 1NC 11 No Space War

#### Redundancy checks

**Forden, 7** – writer for Arms Control Today (Geoffrey, “After China's Test: Time For a Limited Ban on Anti-Satellite Weapons. Arms Control Today, April 2007, <http://www.armscontrol.org/act/2007_04/Forden>**)**

On the other hand, an attacker would have to destroy a considerable number of satellites in order to have an immediate effect on military operations. There are on average about 10 GPS satellites visible at any given time and point on the Earth's surface even though a high positional accuracy requires only six. An attacker would have to destroy at least six satellites to affect precision-guided munitions even momentarily because other GPS satellites would soon appear as their orbits took them into view. A country would need to disable nearly one-half of the United States' 24 NAVSTAR/GPS satellites currently in orbit to eliminate the ability to employ precision-guided munitions for more than a few hours each day.[[**9**](http://www.armscontrol.org/act/2007_04/Forden.asp#Note9)] Likewise, the United States has a number of alternatives for communications satellites in the short term. Other space assets, such as weather and mapping satellites, although important in the long term, are not as time critical.

## LOAC

### LOAC: Ext 1/No Modeling

#### Plan doesn't solve norms – 2 reasons

#### 1. Unclear retaliation policy

**Harris** 7/15/**13**

Shane Harris, Senior Writer, Foreign Policy magazine; Author of The Watchers: The Rise of America's Surveillance State, Foreign Policy, July 15, 2013, "Meet the Air Force's Top Cyberwarrior", http://killerapps.foreignpolicy.com/posts/2013/07/01/air\_forces\_cyber\_chief\_for\_frank\_discussion\_about\_rules\_of\_network\_war

The general who oversees the Air Force's online warriors says there needs to be a "frank discussion" among nations to keep misunderstandings in cyberspace from escalating into a broader conflict. "We still have to get our hands around deterrence," said Lt. Gen. Michael Basla, the Air Force's chief of information dominance and its chief information officer, in an interview with Foreign Policy. **There are no hard lines that tell an adversary what response ~~he~~ can expect after taking action against a U.S. network**, Basla explained. Nor is there a full understanding of "signaling" by a cyber-adversary -- that is, how to tell the difference between an action that may look provocative, but is actually more benign. Basla's title reflects how priorities have changed for the Air Force in a short period of time. In June 2012, he became the first chief information officer (CIO) to hold that second title putting him in charge of "information dominance" -- read cyber-operations. In many organizations, the CIO is the guy in charge of keeping the network running. He's like the plumber. Basla's a kind of plumber too, but he's figuring out how to take out an adversary's networks, at the same time that he tries to defend the Air Force's. Basla's comments about deterrence **echo those of other cybersecurity experts** who say that there is currently **no cyber-analog to the strategy of nuclear deterrence, whereby nations understand what aggressive steps they might take but still stop short of** a **full exchange** of nuclear weapons.

#### 2. No definitions

**Kaminski 10**

Ryan T. Kaminski, Columbia University School of International and Public Affairs, “ESCAPING THE CYBER STATE OF NATURE: CYBER DETERRENCE AND INTERNATIONAL INSTITUTIONS,” NATO Cooperative Cyber Defence Center of Excellence, published 2010, http://www.ccdcoe.org/publications/2010proceedings/Kaminski%20-%20Escaping%20the%20Cyber%20State%20of%20Nature%20Cyber%20deterrence%20and%20International%20Institutions.pdf

2.1 LACK OF A UNIVERSALLY ACCEPTED CYBERWARFARE LEXICON Anyone reading lay articles, think-tank studies, published manuscripts, or even government reports on cyber attacks is likely to ﬁnd a dizzying array of terms sometimes referring to the same concept. For example, should a DDoS attack that causes disruptions to a government website, yet does not steal any sensitive information, be considered an act of cyberwar, cyber espionage, or cyber vandalism? The implications of lacking a generally accepted vocabulary in this area are twofold. First, depending on what lexical framework is used, international and customary law can be interpreted to permit vastly different reactions to the same cyber attack. For example, if two states have contrasting lexicons concerning cyberwarfare, one could view a cyber attack as an act of war, while the other could conceptualize it merely as an act of cyber vandalism (“Marching Oﬀ,” 2008). Second, given that some states even lack a universally accepted cyber glossary among their various domestic civilian and military agencies, the possibility of misinterpreting a potential cyber attack on the national level also **remains high** (Shanker & Markoff, 2009). Looking at the Estonian and Georgian cases, this problem is uniquely apparent. Tohn (2009), for one, hyperbolizes the attacks against both states as “cyber-blitzkriegs,” regardless of such a term’s connotation with an all-out military attack from World War II (p. 17). Former US Deputy Assistant Secretary of Defense Peter Brookes (2008) even classiﬁes the attack on Estonia as a “pre-emptive digital strike” despite the lack of any signiﬁcant evidence that Estonia was planning a cyber attack on Russia. Jaak Aaviksoo, Estonia’s Defense Minister, also declared that the cyber attack against his country “cannot be treated as hooliganism, but has to be treated as an attack against the state” (“Marching Oﬀ,” 2008). Even though Estonia did not end up invoking Article V of the NATO charter which commits states to treat an attack on one member as an attack on themselves, the defense minister’s comments nonetheless illuminate major problems associated with the lack of a comprehensive cyberwarfare lexicon. While Estonia did construct a NATO-sponsored facility in its capital to study cyber security, this also may do **little good** if non-NATO members like China and Russia are relying upon **an entirely different cyber language**.

#### Other countries say no

#### a) perception of strategic value to weapons

James Andrew Lewis, senior fellow and Program Director at the Center for Strategic and International Studies (CSIS), 2011 (Confidence-building and international agreement in cybersecurity, disarmament forum, <http://citizenlab.org/cybernorms2012/Lewis2011.pdf>)

The immense utility of cyber action will shape any international agreement on cybersecurity. States will not give up this new tool for state power. Cyber attack is cheap and offers strategic advantage. First, the importance of information superiority in warfare and the ability to gain real military advantage from the use of information assets makes digital infrastructures too valuable a target to be declared off limits or for cyber attacks to be renounced. The necessary technologies are either commercial or easily derived from widely available commercial products—a laptop computer, an internet connection and a few computer programs. We cannot control the “precursors” for assembling these “weapons”. They are cheap, small, portable, easy to conceal and, for sophisticated programmers in or out of government, easy to construct. Special purpose tools for cyber attack are widely available on thriving cybercrime black markets. It is unlikely that any state will renounce the use of cyber attacks.

#### Norms fail—cheating and miscalc

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

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

### LOAC 1NC 7-8 China

#### No offense here--Even Chinese sources agree agree

Greg Austin Senior visiting fellow in the department of War Studies at King’s College London and Franz-Stefan Gady, adjunct research assistant at the Institute for National Strategies Studies of the National Defense University, 2012 (CYBER DEtEntE BEtWEEn tHE UnItED StAtES AnD CHInA: SHAPING THE AGENDA, EastWest Institute, <http://www.ewi.info/system/files/detente.pdf>)

China sees itself as lagging well behind in technology. It knows how difficult it is for a country to achieve a level of technological preparedness in its armed forces that is significantly different from the technological foundations of the society as a whole (talent base, research and development climate, investment levels). A number of Chinese and international studies have consistently given China fairly low grades in terms of advanced information technology.28

#### No China threat

Moss 4/19/13 – 1AC Author (Trefor, covers Asian politics, defence and security, and was Asia-Pacific Editor at Jane’s Defence Weekly until 2009 The Diplomat- - “Is Cyber War the New Cold War?”, http://thediplomat.com/2013/04/19/is-cyber-war-the-new-cold-war/3/, zzx)

Cyberspace is anarchic, and incidents there span a hazy spectrum from acts of protest and criminality all the way to invasions of state sovereignty and deliberate acts of destruction. Cyber attacks that might be considered acts of war have so far been rare. It is certainly hard to characterise the rivalry between China and the U.S. as it stands as cyber warfare, argues Adam Segal, a senior fellow at the Council on Foreign Relations. “I tend to stay away from the term ‘cyber war’ since we have seen no physical destruction and no deaths,” he explains. Segal accepts that there is a conflict of sorts between China and the U.S. in cyberspace, though he says it is “likely to remain below a threshold that would provoke military conflict.”.= While there is no internationally accepted categorization of different kinds of cyber activity (individual states have varying definitions), it is self-evident that some episodes are more serious than others. NATO’s Cooperative Cyber Defence Centre of Excellence (CCDCOE) – a unit based, not by accident, in Estonia, which experienced a massive cyber-attack from Russia in 2007 – distinguishes between “cyber crime,”“cyber espionage,” and “cyber warfare.” China’s cyber operations, for all their notoriety, have essentially been acts of theft – either criminals attempting to extract privileged data, or incidents of state-sponsored espionage (some of which, admittedly, had national security implications, such as the extraction of blueprints for the F-35 Joint Strike Fighter). But these operations did not seek to cause any physical destruction, and so would be hard to interpret as acts of war. This may explain why the U.S. government has been quite tolerant of Chinese hacking until now, seeing it as an irritant rather than as anything more provocative.

# 1NR

### o/v impact stuff

#### collapse by November if we don’t raise the debt ceiling

Sahadi 9/10 Jeanne, “Debt ceiling 'X date' could hit Oct. 18”, <http://money.cnn.com/2013/09/10/news/economy/debt-ceiling-bills-coming-due/index.html>, MCR

A new analysis by a think tank shows that **Washington's drop-dead deadline for the debt ceiling could hit as soon as Oct. 18**.¶ Estimating exactly when the Treasury Department will be unable to pay all the bills coming due if Congress fails to raise the nation's legal borrowing limit is notoriously difficult.¶ That's why, in an analysis released Tuesday, the Bipartisan Policy Center put the "X date" between Oct. 18 and Nov. 5.¶ Treasury Secretary Jack Lew has warned that **by mid-October the agency will have only $50 billion in cash on top of incoming revenue.**¶That may sound like a lot. But, as the Bipartisan Policy Center details, **it won't last very long**.¶ If the "X" date turns out to be Oct. 18, Treasury would run about $106 billion short of the money it owes between then and Nov.15. That means it wouldn't be able to pay the equivalent of a third of all the bills due during that period.¶ Here's why: Treasury handles about 80 million payments a month. Those payments are not evenly spaced out so on some days more is owed than on others. And the revenue flowing into federal coffers is unpredictable and varies from day to day.¶ Payments include IRS refunds, Social Security and veterans benefits, Medicare reimbursements for doctors and hospitals, bond interest owed investors, payments to contractors and paychecks for federal workers and military personnel.¶ If Congress fails to act in time, Treasury will have to make difficult -- and legally questionable -- decisions about who should get paid and who should be stiffed. It may decide to pay some bills in full and on time and not others.¶ Or it may decide to delay all payments due on a given day until it has sufficient revenue on hand to pay in full. in a Treasury Inspector General's report that this might be the most plausible and least harmful approach.¶ But under that scenario, **delays would grow over time from a day or two to several weeks**. For example, the payments due to seniors, veterans and active duty military personnel on Nov. 1 wouldn't go out until Nov. 13.¶ In any case, the expectation is that the agency will try to prioritize payments to bond investors over everyone else, lest the financial markets go haywire. Politically, of course, that carries risk, said Steve Bell, the senior director of the Bipartisan Policy Center's economic policy project.¶ "There's a political danger you'll be accused of paying bondholders over Social Security recipients," Bell said.¶ On both Oct. 23 and Nov. 14, $12 billion in Social Security benefits come due, while another $25 billion comes due on Nov. 1, according to the analysis.¶ Meanwhile, on Oct. 24, Treasury will have to roll over $57 billion in outstanding debt and another $115 billion on Oct. 31. Normally that's not a problem, because U.S. Treasury auctions attract a lot of buyers willing to purchase bonds at low rates.¶ But if those rollover dates come after the "X" date, and **the perception is that the United States is defaulting on some of its obligations, Treasury could have trouble finding enough buyers or investors could demand higher interest rates**.¶ The debt ceiling is currently set at $16.7 trillion. That ceiling was reached on May 19, and ever since Treasury has been using a host of special measures to keep the country's borrowing at or below that ceiling. But those measures will be exhausted by mid-October, according to Treasury.¶ If lawmakers want to raise the ceiling enough to get past the 2014 midterm elections in November, the Bipartisan Policy Center estimates they will have to raise it by $1.1 trillion to $17.8 trillion. To top of page

#### C. Controlling impact --- only economic collapse can make major war fashionable again.

Donald Kagan, Senior Associate @ Carnegie Endowment for International Peace, Summer 1999 [“Is Major War obsolete? An Exchange," Survival]

There is yet another more critical factor that cannot be taken for granted: the continuous prosperity that underlies the current situation. It is 70 years since the last world-wide depression began. Will this prosperous condition without such world-wide depressions last forever? What will happen if it does not? Europe and the world had trouble sin the 1920s, but it took the Great Depression to blow away liberal regimes in Germany and Japan, and to unleash monstrous bellicose forces. Are we sure that would not happen again? Since we cannot be sure that it will not, we must face the real possibility that major war may yet again come into fashion, and that it will take considerable effort, especially by the US, to keep it at bay.

### uq

#### Tentative breakthrough on debt limit—Boehner stresses importance of bipartisan negotiations

Fox News, 10/4, (Tom Cohen. Deirdre Walsh and Ed Payne, “Hope for debt limit deal rises while shutdown standoff remains mired”, 10/4/2013, <http://fox13now.com/2013/10/04/hope-for-debt-limit-deal-rises-while-shutdown-standoff-remains-mired/>)

House Speaker John Boehner and fellow GOP lawmakers meet to discuss the government shutdown Friday, a day after the Republican leader reportedly told fellow legislators that he won’t allow the United States to default on its debt. Congressional Republicans remain divided over how to structure legislation to raise the nation’s borrowing level, and with only two weeks before the debt ceiling deadline, there is still no plan to avoid a default. But at a meeting Thursday with House GOP members, Boehner said he would not allow a default to happen, even if it means getting help from Democrats, according to a Republican House member who requested anonymity to talk about the private meeting. A Boehner aide said Thursday that the speaker “has always said the United States will not default on its debt, so that’s not news.” Democratic Sen. Charles Schumer of New York cheered the prospect of the GOP leader refusing to block at least this measure, which President Barack Obama and his fellow Democrats strongly support. “This could be the beginnings of a significant breakthrough,” Schumer said in a statement. “Even coming close to the edge of default is very dangerous, and putting this issue to rest significantly ahead of the default date would allow everyone in the country to breathe a huge sigh of relief.” The potential breakthrough — at least on the debt limit — came two weeks before the government is set to run out of money to cover its roughly $16.7 trillion debt. If the debt ceiling isn’t bumped up, the country goes into default. Conservative Republicans want budget cuts in exchange for upping the credit limit. Boehner wrote this week in USA Today that “there is no way Congress can or should pass (a debt ceiling increase) without spending cuts and reforms to deal with the debt and deficit and help get our economy moving again.” He accused the president of refusing to negotiate; Obama and Democratic leaders have since said they are open to talks on any and all budgetary matters, but only after the government is reopened.

#### \*Debt limit will be raised now—Bipartisan deal key

CNN, 10/3, (Tom Cohen, Deirdre Walsh and Greg Botelho, “GOP legislator: Boehner won't let government default on its debt”, 10/30/2013, <http://www.cnn.com/2013/10/03/politics/government-shutdown-main/index.html>)

The federal government may not be hit with a double whammy on top of the ongoing shutdown, as House Speaker John Boehner told a group of fellow GOP legislators that he won't let the nation default on its debt, according to a House Republican. Boehner said that he'd set aside the "Hastert Rule" -- that Republicans would only bring measures up for a vote if they are backed by a majority of their caucus -- and rely on Democrats to pass a measure to raise the nation's debt limit, said the House member. This legislator attended a meeting Wednesday involving Boehner, but requested anonymity because that gathering was private. Congressional Republicans remain divided on how to structure legislation to raise the government's borrowing level. And an aide to the House speaker downplayed the development, saying, "Boehner has always said the United States will not default on its debt, so that's not news." Still, at least one Democrat -- Sen. Charles Schumer of New York -- cheered the prospect of the GOP leader refusing to block at least this measure that President Barack Obama and his fellow Democrats strongly support. "This could be the beginnings of a significant breakthrough," Schumer said in a statement. "Even coming close to the edge of default is very dangerous, and putting this issue to rest significantly ahead of the default date would allow everyone in the country to breathe a huge sigh of relief." GOP Rep.: You're beautiful but be honest Sen. Reid: I will not pick and choose GOP 'lemming caucus' blocking leadership The Ohio Republican's vow comes exactly two weeks before the government is set to run out of money to cover its roughly $16.7 trillion debt, unless Congress agrees to lift the so-called debt ceiling. That had long been routine in Washington -- until recently, that is, when conservative Republicans have pushed not to allow more borrowing without significant cuts. Boehner himself wrote earlier this week in USA Today that "there is no way Congress can or should pass (a debt ceiling hike) without spending cuts and reforms to deal with the debt and deficit and help get our economy moving again." He accused President Barack Obama of refusing to negotiate; Obama and fellow Democratic leaders have since said they are open to talks on any and all budgetary matters, but only after the government is reopened. Yet Boehner's comments signal that, at least on the debt ceiling issue, he's willing to allow a vote on a measure backed by top Democrats but not most Republicans in his chamber -- something he's refused to do with a Senate-passed measure to reopen the federal government, without any add-ons. Chief among those Democrats is Obama who, for all his strong rhetoric on ending the government shutdown, has said that avoiding a federal debt default is an even bigger necessity. He's insisted Congress pass such a measure, as is, without tying it to anything else. "As reckless as a government shutdown is, an economic shutdown that results from default would be dramatically worse," the president said in a speech Thursday in Rockville, Maryland. "There will be no negotiations over this." Obama challenges Boehner to allow 'yes-or-no vote' on shutdown While Boehner's comments suggest hope toward some common resolution on the debt ceiling, the government shutdown is another matter entirely.

### Cyber lx

#### Cyber ops get drawn into larger jurisdictional battles – causes massive fights

John W. Brennan, Lieutenant Colonel – United States Army, 3-15-2012, “United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?” http://nsfp.web.unc.edu/files/2012/09/Brennan\_UNITED-STATES-COUNTER-TERRORISM-CYBER-LAW-AND-POLICY.pdf

As a matter of current U. S. policy, the decision to label a computer network operation (CNO) as a traditional military activity (TMA), thereby falling under the purview of Title 10 of the United States Code (USC), or as a covert action under Title 50 of the USC, has spurred a great deal of discussion at the highest levels of the U. S. Government. 47 Although cyber warfare is only one aspect of the overall current Title 10/50 debate that is raging within Congress and the various departments within the executive branch, one cannot legitimately discuss the policies that govern the approvals to conduct CNOs without touching upon this current source of friction. 48 Much of the policy concerning the details of computer network operations is classified, but is gaining in importance such that many policy experts are speaking about it, some albeit from under the cloak of anonymity. 49 As Andru E. Wall suggests, the confusion over Title 10 and Title 50 authorities appears to have, “…more to do with congressional oversight and its attendant internecine power struggles than with operational or statutory authorities,” despite the fact that by design, Title 10 and 50 authorities are mutually supporting and were not intended to be competing.50 Retired Admiral Dennis C. Blair (former ODNI) proclaimed that, “This infuriating business about who’s in charge and who gets to call the shots is just making us look muscle-bound.” ADM Blair went on to bemoan the “over-legalistic” approach to CT cyber--despite the fact that current cyber laws are woefully inadequate to address the, …”complexity of the global information network.”51(Wall 2011101)

### Obama will fight

#### Obama will fight to defend offensive cyber operations – empirically proven

Walker 8/2/13 (Richard, “OBAMA EXPANDS WAR POWERS; CAN UNLEASH CYBERWAR ANY TIME”, <http://americanfreepress.net/?p=11966#sthash.hVcGGduE.dpuf>, CMR)

The very moment United States President Barack Obama authorized the “dropping” of an electronic bomb on Iran’s nuclear industry he crossed a line into a new kind of warfare that could have global consequences today and far into the future. The weapon used against Iran was built with the cooperation of Israel and was named Stuxnet. It was a “worm” that infected the computers running Iran’s nuclear industry. German systems control expert, Ralph Langer, who told the world about Stuxnet, remarked Stuxnet represented a dangerous capability and that its code could be used by hackers and others. In other words, Obama had unleashed a weapon that could be re-engineered by anyone to attack computer networks controlling American infrastructure.¶ Perhaps the most significant aspect of the Stuxnet attack was it demonstrated how Obama had given to himself new powers to launch a cyberwar against any country without Congressional approval. Unlike conventional war in which soldiers are sent to the front and bombs are dropped from the skies, cyberweapons silently and stealthily attack information systems, as well as financial and power centers. We do not know how many times Obama has used his new Cyber Command unit to attack nations other than Iran.¶ Obama’s Presidential Policy Directive 20, known as PPD 20, which he signed in October 2012, was a stark example of a power grab to accord to him special powers to launch a cyber war at a moment of his choosing. The Guardian newspaper, which first revealed the existence of the directive, claimed it sought a larger target list for cyber attacks and contemplated the use of cyber weapons within the U.S. if the president gave the green light and only in an emergency. But what kind of emergency remains unclear, as does the list of nations he might target in the future.¶ Hard Assets Alliance¶ The Electronic Privacy Information Center (EPIC) was unsuccessful in a legal bid to have the directive made public. EPIC feels the American people have a right to know what this president is doing with the country’s cyberpowers and how those powers could possibly be used against ordinary citizens, or how far he may go in an emergency to limit public access to the Internet.¶ The evidence Obama was bent on developing a cyber war capability he could personally control was there for all to see in the 2012 Fiscal Year National Defense Authorization Act. Obama had threatened to veto the bill until he realized part of it was something he craved, namely the power to use cyber weapons in an offensive capacity. The bill passed without a presidential veto and, as is the case with most bills, few people took time to read its 656 pages. Had they done so, they would have found a Section 954 entitled “Military Activities in Cyberspace.” It declared “Congress affirms that the Department of Defense has the capability, and upon direction by the president, may conduct offensive operations in cyberspace to defend our nation, allies and interests.”¶ An East European cyber war specialist, speaking on condition of anonymity to AMERICAN FREE PRESS, said he was unhappy with Obama’s refusal to work more closely with Russia on cyber threats. He pointed to the fact Obama abandoned a joint approach by U.S.–Russian experts, who issued a cyber-conflict report in 2011 under the auspices of the East-West Institute. It was the first joint effort of its kind designed to define the “rules of the road” for cyber conflict.¶ “Obama is more of as hawk in this field than people imagine. His cyber war policy has the potential for global consequences in which cyber wars will be launched by many nations and it will be impossible to identify the culprits. Russia wanted a cyber-partnership with America, but Obama wanted to go it alone with the exception of working with the Israelis on projects of mutual interest like Iran and now Syria. That should concern his allies as much as the American people,” he warned.

### Pc key

#### Political capital is finite and drives decisionmaking

**Schier 9**, Professor of Poliitcal Science at Carleton, (Steven, "Understanding the Obama Presidency," The Forum: Vol. 7: Iss. 1, Berkely Electronic Press, http://www.bepress.com/forum/vol7/iss1/art10)

In additional to formal powers, a president’s informal power is situationally derived and highly variable. Informal power is a function of the “political capital” presidents amass and deplete as they operate in office. Paul Light defines several components of political capital: party support of the president in Congress, public approval of the presidential conduct of his job, the President’s electoral margin and patronage appointments (Light 1983, 15).Richard Neustadt’s concept of a president’s “professional reputation” likewise figures into his political capital. Neustadt defines this as the “impressions in the Washington community about the skill and will with which he puts [his formal powers] to use” (Neustadt 1990, 185). In the wake of 9/11, George W. Bush’s political capital surged, and both the public and Washington elites granted him a broad ability to prosecute the war on terror. By the later stages of Bush’s troubled second term, beset by a lengthy and unpopular occupation of Iraq and an aggressive Democratic Congress, he found that his political capital had shrunk.Obama’s informal powers will prove variable, not stable, as is always the case for presidents. Nevertheless, he entered office with a formidable store of political capital. His solid electoral victory means he initially will receive high public support and strong backing from fellow Congressional partisans, a combination that will allow him much leeway in his presidential appointments and with his policy agenda. Obama probably enjoys the prospect of a happier honeymoon during his first year than did George W. Bush, who entered office amidst continuing controversy over the 2000 election outcome.Presidents usually employ power to disrupt the political order they inherit in order to reshape it according to their own agendas. Stephen Skowronek argues that “presidents disrupt systems, reshape political landscapes, and pass to successors leadership challenges that are different from the ones just faced” (Skowronek 1997, 6). Given their limited time in office and the hostile political alignments often present in Washington policymaking networks and among the electorate, presidents must force political change if they are to enact their agendas. In recent decades, Washington power structures have become more entrenched and elaborate (Drucker 1995) while presidential powers – through increased use of executive orders and legislative delegation (Howell 2003) –have also grown. The presidency has more powers in the early 21st century but also faces more entrenched coalitions of interests, lawmakers, and bureaucrats whose agendas often differ from that of the president. This is an invitation for an energetic president – and that seems to describe Barack Obama – to engage in major ongoing battles to impose his preferences.

#### Presidents perceive their capital as finite – our theory is true in practice

**Marshall and Prins 11**, BRYAN W. MARSHALL Miami University BRANDON C. PRINS University of Tennessee & Howard H. Baker, Jr. Center for Public Policy Power or Posturing? Policy Availability and Congressional Influence on U.S. Presidential Decisions to Use Force Presidential Studies Quarterly 41, no. 3 (September) 2011

We argue that the more important effect of Congress occurs because presidents anticipate how the use of force may affect the larger congressional environment in which they inevitably have to operate (Brulé, Marshall, and Prins 2010). It may be true that presidents consider the chances that Congress will react to a specific use of force with countervailing tools, but even more importantly they anticipate the likelihood that a foreign conflict may damage (or advantage) their political fortunes elsewhere—in essence, the presidential calculus to use force factors in how such actions might shape their ability to achieve legislative priorities. To be clear, presidents can and do choose to use force and press for legislative initiatives in Congress. Taking unilateral actions in foreign policy does not preclude the president from working the legislative process on Capitol Hill. However, political capital is finite so spending resources in one area lessens what the president can bring to bear in other areas. That is, presidents consider the congressional environment in their decision to use force because their success at promoting policy change in either foreign or domestic affairs is largely determined by their relationship with Congress. Presidents do not make such decisions devoid of calculations regarding congressional preferences and behavior or how such decisions may influence their ability to achieve legislative objectives. This is true in large part because presidential behavior is motivated by multiple goals that are intimately tied to Congress. Presidents place a premium on passing legislative initiatives. The passage of policy is integral to their goals of reelection and enhancing their place in history (Canes-Wrone 2001; Moe 1985). Therefore, presidents seek to build and protect their relationship with Congress.

### No xo

#### Obama will not use an XO

New York Times, 10/3, (Jackie Calmes, “Obama Will Not Unilaterally Raise Debt Limit”, 10/3/2013, <http://www.nytimes.com/news/fiscal-crisis/2013/10/03/obama-will-not-unilaterally-raise-debt-limit/>)

President Obama will not invoke a constitutional amendment to unilaterally increase the nation’s debt limit if an impasse with House Republicans causes that ceiling to be breached Oct. 17, his spokesman said. “We do not believe that the 14th amendment provides that authority to the president,” the White House press secretary, Jay Carney, said on Thursday. The president, he added, “completely” agrees with his advisers’ legal reasoning. The administration, and Mr. Obama himself, have said in past confrontations with Republicans that the president does not have the constitutional power to act without Congress. But the issue has surfaced yet again, as another and seemingly more intractable impasse between the White House and Republicans threatens a debt crisis. After Oct. 17, the Treasury Department has said, it will no longer be able to borrow money to cover the nation’s obligations, including to creditors, precipitating a potential financial and economic crisis with global ramifications. “Look,” Mr. Carney said, sounding slightly exasperated to reporters, “our view is, the Constitution gives Congress, not the president, the authority to borrow money, and only Congress can increase the debt ceiling. Which is why it’s time that they do their job and raise the debt ceiling – you know, authorize the Treasury to pay the bills that Congress racked up.” The fact that the question of the president’s 14th amendment authority is controversial, with constitutional scholars in disagreement, “means that it would not be a credible alternative,” Mr. Carney said. Treasury officials have described a potential situation in which if the president unilaterally raised the borrowing limit, and Treasury then held an auction for new bonds to raise money, few if any buyers would participate for fear that the bonds ultimately would be deemed illegal.

### Winners don’t win

#### Obama believes the link

Robert **Kuttner**, senior fellow, Demos, “Obama Has Amassed Enormous Political Capital, But He Doesn’t Know What to Do with It,” Alternet, 4—28—**09**, www.alternet.org/economy/138641/obama\_has\_amassed\_enormous\_political\_capital,\_but\_he\_doesn%27t\_know\_what\_to\_do\_with\_it/

We got a small taste of what a more radical break might feel like when Obama briefly signaled with the release of Bush's torture memos that he might be open to further investigation of the Bush's torture policy, but then backtracked and quickly asked the Democratic leadership to shut the idea down. Evidently, Obama's political self wrestled with his constitutional conscience, and won. Civil libertarians felt a huge letdown, but protest was surprisingly muted.Thus the most important obstacle for seizing the moment to achieve enduring change: Barack Obama's conception of what it means to promote national unity. Obama repeatedly declared during the campaign that he would govern as a consensus builder. He wasn't lying. However, there are two ways of achieving consensus. One is to split the difference with your political enemies and the forces obstructing reform. The other is to use presidential leadership to transform the political center and alter the political dynamics. In his first hundred days, Obama has done a little of both, but he defaults to the politics of accommodation.

#### Wins only build long-term capital

**Purdum 10**, Columnist for Vanity Fair, (Todd, “Obama Is Suffering Because of His Achievements, Not Despite Them,” 12-20 www.vanityfair.com/online/daily/2010/12/obama-is-suffering-because-of-his-achievements-not-despite-them.html)

With this weekend’s decisive Senate repeal of the military’s “Don’t Ask, Don’t Tell” policy for gay service members, can anyone seriously doubt Barack Obama’s patient willingness to play the long game? Or his remarkable success in doing so? In less than two years in office—often against the odds and the smart money’s predictions at any given moment—Obama has managed to achieve a landmark overhaul of the nation’s health insurance system; the most sweeping change in the financial regulatory system since the Great Depression; the stabilization of the domestic auto industry; and the repeal of a once well-intended policy that even the military itself had come to see as unnecessary and unfair.

So why isn’t his political standing higher?

Precisely because of the raft of legislative victories he’s achieved. Obama has pushed through large and complicated new government initiatives at a time of record-low public trust in government (and in institutions of any sort, for that matter), and he has suffered not because he hasn’t “done” anything but because he’s done so much—way, way too much in the eyes of his most conservative critics. With each victory, Obama’s opponents grow more frustrated, filling the airwaves and what passes for political discourse with fulminations about some supposed sin or another. Is it any wonder the guy is bleeding a bit? For his part, Obama resists the pugilistic impulse. To him, the merit of all these programs has been self-evident, and he has been the first to acknowledge that he has not always done all he could to explain them, sensibly and simply, to the American public.

But Obama is nowhere near so politically maladroit as his frustrated liberal supporters—or implacable right-wing opponents—like to claim. He proved as much, if nothing else, with his embrace of the one policy choice he surely loathed: his agreement to extend the Bush-era income tax cuts for wealthy people who don’t need and don’t deserve them. That broke one of the president’s signature campaign promises and enraged the Democratic base and many members of his own party in Congress. But it was a cool-eyed reflection of political reality: The midterm election results guaranteed that negotiations would only get tougher next month, and a delay in resolving the issue would have forced tax increases for virtually everyone on January 1—creating nothing but uncertainty for taxpayers and accountants alike. Obama saw no point in trying to score political debating points in an argument he knew he had no chance of winning.

Moreover, as The Washington Post’s conservative columnist Charles Krauthammer bitterly noted, Obama’s agreement to the tax deal amounted to a second economic stimulus measure—one that he could never otherwise have persuaded Congressional Republicans to support. Krauthammer denounced it as the “swindle of the year,” and suggested that only Democrats could possibly be self-defeating enough to reject it. In the end, of course, they did not.

Obama knows better than most people that politics is the art of the possible (it’s no accident that he became the first black president after less than a single term in the Senate), and an endless cycle of two steps forward, one step back. So he just keeps putting one foot in front of the other, confident that he can get where he wants to go, eventually. The short-term resultsare often messy and confusing. Just months ago, gay rights advocates were distraught because Obama wasn’t pressing harder to repeal “Don’t Ask, Don’t Tell.” Now he is apparently paying a price for his victory because some Republican Senators who’d promised to support ratification of the START arms-reduction treaty—identified by Obama as a signal priority for this lame-duck session of Congress—are balking because Obama pressed ahead with repealing DADT against their wishes. There is a price for everything in politics, and Obama knows that, too.

### Yes vote switch

#### Vote switching happens—even on unrelated legislation

Dmitri **Simes**, Executive Director, Nixon Center and Paul Saunders, “START of a Pyrrhic Victory,” NATIONAL INTEREST, 20**10**, http://nationalinterest.org/commentary/start-pyrrhic-victory-4626, accessed 10-2-11.

Had the lame-duck session not already been so contentious, this need not have been a particular problem. Several Senate Republicans indicated openness to supporting the treaty earlier in the session, including Senator Lindsey Graham and Senator John McCain. Senator Jon Kyl—seen by many as leading Republican opposition to the agreement—was actually quite careful to avoid saying that he opposed New START until almost immediately prior to the vote. Our own conversations with Republican Senate sources during the lame duck session suggested that several additional Republicans could have voted to ratify New START under other circumstances; Senator Lamar Alexander is quoted in the press as saying that Republican anger over unrelated legislation cost five to ten votes. By the time the Senate reached New START, earlier conduct by Senate Democrats and the White House had alienated many Republicans who could have voted for the treaty. That the administration secured thirteen Republican votes (including some from retiring Senators) for the treaty now—and had many more potentially within its grasp—makes clear what many had believed all along: it would not have been so difficult for President Obama to win the fourteen Republican votes needed for ratification in the new Senate, if he had been prepared to wait and to work more cooperatively with Senate Republicans. Senator Kerry’s comment that “70 votes is yesterday’s 95” ignores the reality that he and the White House could have secured many more than 70 votes had they handled the process differently and attempts to shift the blame for the low vote count onto Republicans.

### Debt k2 econ

#### This will destroy the U.S. and global economy

Davidson, 9/10 (Adam - co-founder of NPR’s “Planet Money” 9/10/2013, “Our Debt to Society,” <http://www.nytimes.com/2013/09/15/magazine/our-debt-to-society.html?pagewanted=all&_r=0)>)

This is the definition of a deficit, and it illustrates why the government needs to borrow money almost every day to pay its bills. Of course, all that daily borrowing adds up, and we are rapidly approaching what is called the X-Date — the day, somewhere in the next six weeks, when the government, by law, cannot borrow another penny. Congress has imposed a strict limit on how much debt the federal government can accumulate, but for nearly 90 years, it has raised the ceiling well before it was reached. But since a large number of Tea Party-aligned Republicans entered the House of Representatives, in 2011, raising that debt ceiling has become a matter of fierce debate. This summer, House Republicans have promised, in Speaker John Boehner’s words, “a whale of a fight” before they raise the debt ceiling — if they even raise it at all. If the debt ceiling isn’t lifted again this fall, some serious financial decisions will have to be made. Perhaps the government can skimp on its foreign aid or furlough all of NASA, but eventually the big-ticket items, like Social Security and Medicare, will have to be cut. At some point, the government won’t be able to pay interest on its bonds and will enter what’s known as sovereign default, the ultimate national financial disaster achieved by countries like Zimbabwe, Ecuador and Argentina (and now Greece). In the case of the United States, though, it won’t be an isolated national crisis. If the American government can’t stand behind the dollar, the world’s benchmark currency, then the global financial system will very likely enter a new era in which there is much less trade and much less economic growth. It would be, by most accounts, the largest self-imposed financial disaster in history. Nearly everyone involved predicts that someone will blink before this disaster occurs. Yet a small number of House Republicans (one political analyst told me it’s no more than 20) appear willing to see what happens if the debt ceiling isn’t raised — at least for a bit. This could be used as leverage to force Democrats to drastically cut government spending and eliminate President Obama’s signature health-care-reform plan. In fact, Representative Tom Price, a Georgia Republican, told me that the whole problem could be avoided if the president agreed to drastically cut spending and lower taxes. Still, it is hard to put this act of game theory into historic context. Plenty of countries — and some cities, like Detroit — have defaulted on their financial obligations, but only because their governments ran out of money to pay their bills. No wealthy country has ever voluntarily decided — in the middle of an economic recovery, no less — to default. And there’s certainly no record of that happening to the country that controls the global reserve currency. Like many, I assumed a self-imposed U.S. debt crisis might unfold like most involuntary ones. If the debt ceiling isn’t raised by X-Day, I figured, the world’s investors would begin to see America as an unstable investment and rush to sell their Treasury bonds. The U.S. government, desperate to hold on to investment, would then raise interest rates far higher, hurtling up rates on credit cards, student loans, mortgages and corporate borrowing — which would effectively put a clamp on all trade and spending. The U.S. economy would collapse far worse than anything we’ve seen in the past several years. Instead, Robert Auwaerter, head of bond investing for Vanguard, the world’s largest mutual-fund company, told me that the collapse might be more insidious. “You know what happens when the market gets upset?” he said. “There’s a flight to quality. Investors buy Treasury bonds. It’s a bit perverse.” In other words, if the U.S. comes within shouting distance of a default (which Auwaerter is confident won’t happen), the world’s investors — absent a safer alternative, given the recent fates of the euro and the yen — might actually buy even more Treasury bonds. Indeed, interest rates would fall and the bond markets would soar. While this possibility might not sound so bad, it’s really far more damaging than the apocalyptic one I imagined. Rather than resulting in a sudden crisis, failure to raise the debt ceiling would lead to a slow bleed. Scott Mather, head of the global portfolio at Pimco, the world’s largest private bond fund, explained that while governments and institutions might go on a U.S.-bond buying frenzy in the wake of a debt-ceiling panic, they would eventually recognize that the U.S. government was not going through an odd, temporary bit of insanity. They would eventually conclude that it had become permanently less reliable. Mather imagines institutional investors and governments turning to a basket of currencies, putting their savings in a mix of U.S., European, Canadian, Australian and Japanese bonds. Over the course of decades, the U.S. would lose its unique role in the global economy. The U.S. benefits enormously from its status as global reserve currency and safe haven. Our interest and mortgage rates are lower; companies are able to borrow money to finance their new products more cheaply. As a result, there is much more economic activity and more wealth in America than there would be otherwise. If that status erodes, the U.S. economy’s peaks will be lower and recessions deeper; future generations will have fewer job opportunities and suffer more when the economy falters. And, Mather points out, no other country would benefit from America’s diminished status. When you make the base risk-free asset more risky, the entire global economy becomes riskier and costlier.