### 1st Off

#### Interpretation: Restrict means to limit

Supreme Court of Delaware 83 (THE MAYOR AND COUNCIL OF NEW CASTLE, a municipal corporation of the State of Delaware, Plaintiff Below, Appellant, v. ROLLINS OUTDOOR ADVERTISING, INC., Defendant Below, Appellee, No. 155, 1983, 475 A.2d 355; 1984 Del. LEXIS 324, November 21, 1983, Submitted, April 2, 1984, Decided)

The term "restrict" is defined as: To restrain within bounds; to limit; [\*\*9] to confine. Id. at 1182. The Supreme Court of the United States has recognized that HN5the term "regulate" necessarily entails a possible prohibition of some kind. That Court has stated: "It is an oft-repeated truism that every regulation necessarily speaks as a prohibition." Goldblatt v. Hempstead, 369 U.S. 590, 592, 8 L. Ed. 2d 130, 82 S. Ct. 987 (1962). The Supreme Court of Massachusetts in reviewing a statute containing language similar to that found in 22 Del.C. § 301 (which empowered municipalities to "regulate and restrict" outdoor advertising on public ways, in public places, and on private property within public view) held that the statute in question authorized a town to provide, through amortization, for the elimination of nonconforming off-site signs five years from the time the ordinance was enacted. The court held that the Massachusetts enabling act: Conferred on the Legislature plenary power to regulate and restrict outdoor advertising . . . . Although the word "prohibit" was omitted from [the enabling act], it was recognized that the unlimited and unqualified power to regulate and restrict can be, for practical purposes, the power to prohibit [\*\*10] "because under such power the thing may be so far restricted that there is nothing left of of it." (Citations omitted.) The court continued its discussions of the two terms by stating: The distinction between regulation and outright prohibition is often considered to be a narrow one: "that regulation may take the character of prohibition, in proper cases, is well established by the decisions of this court" . . . quoting from United States v. Hill, 248 U.S. 420, 425, 63 L. Ed. 337, 39 S. Ct. 143 (1919). John Donnelly and Sons, Inc. v. Outdoor Advertising Board, Mass. Supr., 369 Mass. 206, 339 N.E.2d 709 (1975). We hold that, through Article II, Section 25 of the Delaware Constitution and 22 Del.C. § 301, the General Assembly has authorized New Castle to terminate nonconforming off-site signs upon reasonable notice, that is, by what has come to be known as amortization. We hold that the power to "regulate and restrict" as such term applies to zoning matters includes the power, upon reasonable notice, to prohibit some of those uses already in existence.

#### Violation- the aff doesn’t RESTRICT anything- it shifts authority horizontally from title 50 to title 10

#### B. Standards:

#### 1. Limits – The topic is already huge – 4 areas times 2 mechanisms all with separate literature and unique advantages – its an impossible research burden.

#### 2. Bidirectionality – Absent restrictions they can create conditions that functionally increase authority

Wilson Center No Date

(War Powers Proposal Gives the President Even More Authority, <http://www.wilsoncenter.org/publication/war-powers-proposal-gives-the-president-even-more-authority)>

A privately organized Commission on War Powers recommended last week that the 1973 War Powers Resolution be repealed and replaced by a Congressional Joint Committee on Consultation and new procedures to approve or disapprove a "significant armed conflict."¶ The 12-member, bipartisan commission, co-chaired by former Secretaries of State Warren Christopher and James Baker, said the current law is flawed. In fact, every president since Richard Nixon has refused to comply with the War Powers Resolution on the grounds that it is an unconstitutional infringement on the president's powers as commander in chief. Among other things, the current act authorizes Congress to terminate combat operations by adopting a concurrent resolution. The Supreme Court ruled in the 1983 Chadha immigration case that one-house and two-house legislative vetoes do not conform to the Constitution's lawmaking requirements of two-house passage and presentment to the president. ¶ Under the substitute law proposed by the commission, the president must, prior to committing troops to "a significant armed conflict" (one likely to last more than a week), submit a classified report to the new joint committee justifying the need for action. The president is then required to consult at least once every 60 days with the committee. ¶ Within 30 days after the conflict begins, if Congress has not enacted a declaration of war or a law authorizing the use of force, a privileged concurrent resolution approving the troop commitment must be brought to a vote in both chambers. If either chamber rejects the approval resolution, any Member can then offer a privileged joint resolution disapproving the commitment. If the joint resolution is vetoed by the president, a two-thirds override vote by both chambers would be necessary to terminate the commitment. ¶ If I were either of the current presidential candidates, I would endorse the commission proposal in a heartbeat. It proposes to vastly expand presidential powers and options beyond current practice. In the "use of force" joint resolutions for Iraq (1991 and 2002) and Afghanistan (2001), Congress was able to negotiate conditions and limitations on the use of force with the president, who then signed the resolutions into law. ¶ That will not be the case if Congress uses the concurrent resolution of approval approach. No matter how many conditions Congress might try to place on the president's use of force in such a concurrent resolution, the president would be under no legal obligation to comply because the provisions would have no force or effect outside Congress. This is because concurrent resolutions are mere sense-of-Congress expressions. (Who's going to charge the president with failing to faithfully execute a non-law?) ¶ It stands to reason that, given this option, no future president will ask for a declaration of war or use of force law when the alternative is a nonbinding sense-of-Congress resolution approving the commitment of troops to combat. Never mind that such a resolution is probably unconstitutional under the Chadha decision requiring two-house passage and presentment to the president. (It's unlikely the court would directly rule on the issue since in recent times it has sidestepped war powers disputes between the branches on the grounds that they present political questions best left to the president and Congress to resolve.) ¶ Another clear advantage to the president presented by the commission's proposed law is the unique relationship that would be established with the 20-member, bipartisan joint committee. Its members would include the Speaker of the House, Senate Majority Leader, House and Senate Minority Leaders and the chairmen and ranking members of eight key committees. Whereas the administration must currently answer to several committees for its war policies, often in public hearings, the new arrangement will give the president both the incentive and justification to deal exclusively with the joint committee in closed sessions. This is something administrations have wanted for years given the burden of officials delivering duplicative testimony in open forums before multiple committees and subcommittees. ¶ The real losers in this new arrangement, of course, will be the rest of the House and Senate and the American people, all of whom will be left in the dark about what is said and done in the closed-door committee consultations with the president. They will be left to trust the judgment of committee members on the necessity for war and its subsequent conduct. ¶ The Commission on War Powers understandably reflects the leadership and views of two former secretaries of State who no doubt see Congress as many of their predecessors have: as an ill-informed, noisy, quarrelsome and meddling micro-manager when it comes to deciding the great issues of war and peace. If the administration must accommodate Congress in some way before making such decisions, they reason, it is best done among a few power elites in Congress, behind closed doors and shielded by classified briefings and documents.

#### Vote negative- Topicality is a prima facie burden and should be evaluated as a question of competing interpretations.

### 2nd Off

#### The Executive Branch of the United States should not conduct and/or direct offensive cyber operations pursuant to Title 50 United States Code and should not conduct cyber operations about which Congress has not been notified, except in response to the use of cyber weapons that can be traced with high confidence to a state, person or organized sponsor.

#### The United States Air Force should not significantly invest in automatic counterattack capabilitie-s and doctrine, including but not limited to taking retaliatory systems off of launch-on-warning.

#### The Department of Defense should increase training and rehearsals to effectively inculcate the ethos of the staffing rules of engagement for the cyber domain. (Carter)

#### Congress should ask for clarification on the funding and exercising direction and control over offensive cyber operations and establish a single joint intelligence committee with appropriating function. (wall)

#### De Facto and De Jure self-binding create accountability from the courts and risk political alienation for going back on promises

Posner and Vermeule 2010 **[Eric A. ,** Professor of Law at the University of Chicago Law School and Editor of The Journal of Legal Studies; **Adrian , Harvard Law Professor, The Executive Unbound: After the Madisonian Republic, Oxford Press, p. 138-139//wyo-sc]**

Many of our mechanisms are unproblematic from a legal perspective, as they involve presidential actions that are clearly lawful. But a few raise legal questions; in particular, those that involve self-binding.59 Can a president bind himself to respect particular first-order policies? With qualifications, the answer is "yes, at least to the same extent that a legislature can." Formally, a duly promulgated executive rule or order binds even the executive unless and until it is validly abrogated, thereby establishing a new legal status quo.60 The legal authority to establish a new status quo allows a president to create inertia or political constraints that will affect his own future choices. In a practical sense, presidents, like legislatures, have great de facto power to adopt policies that shape the legal landscape for the future. A president might commit himself to a long-term project of defense procurement or infrastructure or foreign policy, narrowing his own future choices and generating new political coalitions that will act to defend the new rules or policies. More schematically, we may speak of formal and informal means of selfbinding: 1. The president might use formal means to bind himself. This is possible in the sense that an executive order, if otherwise valid, legally binds the president while it is in effect and may be enforced by the courts. It is not possible in the sense that the president can always repeal the executive order if he can bear the political and reputational costs of doing so. 2. The president might use informal means to bind himself. This is not only possible but frequent and important. Issuing an executive rule providing for the appointment of special prosecutors, as Nixon did, is not a formal self-binding.61 However, there may be political costs to repealing the order. This effect does not depend on the courts' willingness to enforce the order, even against Nixon himself. Court enforcement makes the order legally binding while it is in place, but only political and reputational enforcement can protect it from repeal. Just as a dessert addict might announce to his friends that he is going on a no-dessert diet in order to raise the reputational costs of backsliding and thus commit himself, so too the repeal of an executive order may be seen as a breach of faith even if no other institution ever enforces it. In what follows, we will invoke both formal and informal mechanisms. For our purposes, the distinction between the authority to engage in de jure self-binding (legally limited and well-defined) and the power to engage in de facto self-binding (broad and amorphous) is secondary. So long as policies are deliberately chosen with a view to generating credibility, and do so by constraining the president’s own future choices in ways that impose greater costs on ill-motivated presidents than on well-motivated ones, it does not matter whether the constraint is formal or informal.

### 3rd Off

#### Obama’s campaigning is staving off new sanctions on Iran despite growing support – prevents damaging presidential authority and undermining the sanctions regime resulting in war.

Dennis 1-13

(Steven, reporter for Roll Call. “Obama Redoubles Push Against Iran Sanctions Bill” 1-13-14 http://blogs.rollcall.com/wgdb/obama-redoubles-push-against-iran-sanctions-bill//wyoccd)

The White House’s campaign to keep Congress from messing with its carefully constructed talks with Iran over its nuclear program have stepped into overdrive after support for a new round of sanctions threatens to reach veto-proof majorities.¶ On Monday, Press Secretary Jay Carney repeatedly advised Congress against acting now — one day after President Barack Obama declared he would veto a sanctions bill while announcing the latest agreement with Iran on interim steps to limit its nuclear program. Carney had earlier said that Obama would veto the sanctions bill, but that hasn’t stopped backers from pushing forward.¶ Carney called legislation unnecessary because Congress could act very quickly to impose new sanctions if talks fall apart.¶ “We’re very confident Tehran understands that failure to abide by its commitments in the implementation agreement or failure to reach comprehensive resolution would result in action by the United States and by the international community,” Carney said.¶ The Iran sanctions push pits several members of top Democratic leadership — notably Sen. Charles E. Schumer of New York, the No. 3 Democrat, and Foreign Relations Chairman Robert Menendez of New Jersey — against the president, creating a particularly tense and unusual situation for Obama. The White House is more accustomed to knocking down House opposition while relying on a friendly Senate as its backstop.¶ So far, the bill, which would impose new sanctions against Iran if it does not reach a comprehensive nuclear deal, remains effectively in Senate Majority Leader Harry Reid’s legislative closet, and aides suggest the Nevada Democrat will keep it there for now.¶ “There is not a big clamor for a vote” at the moment, said a senior Democratic aide, who noted that while many senators have voiced support for the bill, not all of them are all demanding immediate action.¶ Another senior aide predicted last week that the bill wouldn’t come up anytime soon and denied a CNN report that it could come up the week of the president’s State of the Union address.¶ Reid at one point last year said the Senate would address the issue, only to apparently change his mind and move to other matters instead. The House already passed additional Iran sanctions last year, leaving the Senate as the president’s backstop.¶ The administration is desperate to keep it that way, repeatedly warning of disaster if Congress interferes with the delicate talks.¶ “Why would you put all of that progress at risk to pass a sanctions bill that the administration is not asking for and that risks dividing the international community?” a senior administration official asked reporters over the weekend as the administration announced the latest agreement. “Because in fact, not only do we think that a new sanctions bill could derail these talks. Ultimately, a new sanctions bill could undermine the sanctions regime that we have built so meticulously over the course of the last several years, because, essentially, if the talks are derailed by new U.S. unilateral sanctions, Iran would take that case to the international community and seek to create divisions in the international community.”¶ In addition to the fear of a broader diplomatic disaster, a congressional smack down of Obama on foreign policy — an area where presidents usually have primary authority — would damage the institution more generally and hurt his ability to negotiate any number of other international deals.¶ Then there is the other fear in the White House — that the collapse of talks could lead to a costly war.¶ “Frankly, this is our opportunity to achieve a peaceful resolution to this issue,” the senior official warned. “And because of that opportunity, Congress should not take action that closes the door on diplomacy.”¶

#### Fighting to defend his war power will sap Obama’s capital- trades off with agenda

**Kriner, 10**

--- assistant professor of political science at Boston University

(Douglas L. Kriner, “After the Rubicon: Congress, Presidents, and the Politics of Waging War”, University of Chicago Press, Dec 1, 2010, page 68-69)

**While congressional support leaves the president’s reserve of political capital intact, congressional criticism saps energy from other initiatives on the home front by forcing the president to expend energy and effort defending his international agenda. Political capital spent shoring up support for a president’s foreign policies is capital that is unavailable for his future policy initiatives**. Moreover, any weakening in the president’s political clout may have immediate ramifications for his reelection prospects, as well as indirect consequences for congressional races.59 Indeed, Democratic efforts to tie congressional Republican incumbents to President George W. Bush and his war policies paid immediate political dividends in the 2006 midterms, particularly in states, districts, and counties that had suffered the highest casualty rates in the Iraq War. 60 **In addition to boding ill for the president’s perceived political capital and reputation, such partisan losses in Congress only further imperil his programmatic agenda, both international and domestic.** Scholars have long noted that President Lyndon **Johnson’s dream of a Great Society also perished in the rice paddies of Vietnam. Lacking** the requisite funds in a war-depleted treasury and **the political capital needed to sustain his legislative vision, Johnson gradually let his domestic goals slip away** as he hunkered down in an effort first to win and then to end the Vietnam War. In the same way, **many of** President **Bush’s highest second-term domestic proprieties, such as Social Security and immigration reform, failed perhaps in large part because the administration had to expend so much energy and effort waging a rear-guard action against congressional critics of the war in Iraq.**61 **When making their cost-benefit calculations, presidents surely consider these wider political costs of congressional opposition to their military policies.** If congressional opposition in the military arena stands to derail other elements of his agenda, all else being equal, the president will be more likely to judge the benefits of military action insufficient to its costs than if Congress stood behind him in the international arena.

#### Loss of political capital causes Democrats flop and support sanctions

Kraushaar 1-22

(Josh Kraushaar, staff writer at the National Journal. “The Iran Deal Puts Pro-Israel Democrats in a Bind” 1-22-14 http://www.nationaljournal.com/magazine/the-iran-deal-puts-pro-israel-democrats-in-a-bind-20131122//wyoccd)

All of this puts Democrats, who routinely win overwhelming support from Jewish Americans on Election Day, in an awkward position. Do they stand with the president on politically sensitive foreign policy issues, or stake their own course? That difficult dynamic is currently playing out in Congress, where the Obama administration is resisting a Senate push to maintain tough sanctions against Iran. This week, Obama met with leading senators on the Banking and Foreign Relations committees to dissuade them from their efforts while diplomacy is underway. "There's a fundamental disagreement between the vast majority of Congress and the president when it comes to increasing Iran sanctions right now," said one Democratic operative involved in the advocacy efforts. "Pro-Israel groups, like AIPAC, try to do things in a bipartisan way; they don't like open confrontation. But in this instance, it's hard." That awkwardness has been evident in the lukewarm reaction from many of Obama's Senate Democratic allies to the administration's outreach to Iran. Senate Foreign Relations Committee Chairman Robert Menendez of New Jersey said last week he was concerned that the administration seems "to want the deal almost more than the Iranians." Normally outspoken Sen. Chuck Schumer of New York, a reliable ally of Israel, has been conspicuously quiet about his views on the negotiations. In a CNN interview this month, Democratic Rep. Debbie Wasserman Schultz of Florida, whose job as chairwoman of the Democratic National Committee is to defend the president, notably declined to endorse the administration's approach, focusing instead on Obama's past support of sanctions. This, despite the full-court press from Secretary of State John Kerry, a former congressional colleague. On Tuesday, after meeting with Obama, Menendez and Schumer signed a bipartisan letter to Kerry warning the administration about accepting a deal that would allow Iran to continue its nuclear program. The letter was also signed by Sens. John McCain, R-Ariz., Lindsey Graham, R-S.C., Susan Collins, R-Maine, and Robert Casey, D-Pa. Democrats, of course, realize that the president plays an outsized role in the policy direction of his party. Just as George W. Bush moved the Republican Party in a more hawkish direction during his war-riven presidency, Obama is nudging Democrats away from their traditionally instinctive support for the Jewish state. "I can't remember the last time the differences [between the U.S. and Israel] were this stark," said one former Democratic White House official with ties to the Jewish community. "There's now a little more freedom [for progressive Democrats] to say what they want to say, without fear of getting their tuchus kicked by the organized Jewish community." A Gallup survey conducted this year showed 55 percent of Democrats sympathizing with the Israelis over the Palestinians, compared with 78 percent of Republicans and 63 percent of independents who do so. A landmark Pew poll of American Jews, released in October, showed that 35 percent of Jewish Democrats said they had little or no attachment to Israel, more than double the 15 percent of Jewish Republicans who answered similarly. At the 2012 Democratic National Convention, many delegates booed a platform proposal supporting the move of the U.S. Embassy in Israel from Tel Aviv to Jerusalem. In 2011, Democrats lost Anthony Weiner's heavily Jewish, solidly Democratic Brooklyn House seat because enough Jewish voters wanted to rebuke the president's perceived hostility toward Israel. Pro-Israel advocacy groups rely on the mantra that support for Israel carries overwhelming bipartisan support, a maxim that has held true for decades in Congress. But most also reluctantly acknowledge the growing influence of a faction within the Democratic Party that is more critical of the two countries' close relationship. Within the Jewish community, that faction is represented by J Street, which positions itself as the home for "pro-Israel, pro-peace Americans" and supports the Iran negotiations. "Organizations that claim to represent the American Jewish community are undermining [Obama's] approach by pushing for new and harsher penalties against Iran," the group wrote in an action alert to its members. Some supporters of Israel view J Street with concern. "There's a small cadre of people that comes from the progressive side of the party that are in the business of blaming Israel first. There's a chorus of these guys," said a former Clinton administration foreign policy official. "But that doesn't make them the dominant folks in the policy space of the party, or the Hill." Pro-Israel activists worry that one of the ironies of Obama's situation is that as his poll numbers sink, his interest in striking a deal with Iran will grow because he'll be looking for any bit of positive news that can draw attention away from the health care law's problems. Thus far, Obama's diminished political fortunes aren't deterring Democrats from protecting the administration's prerogatives. Congressional sources expect the Senate Banking Committee, chaired by South Dakota Democrat Tim Johnson, to hold off on any sanctions legislation until there's a resolution to the Iranian negotiations. But if Obama's standing continues to drop, and if Israel doesn't like the deal, don't be surprised to see Democrats become less hesitant about going their own way.

#### The bill shatters international enforcement and greenlights an Israeli strike

**Klass, 12/31**/13

– retired USAF Colonel; Lt. General (USA Ret.) Robert Gard, the chairman of the Center for Arms Control and Non-Proliferation, contributed to this piece (Richard, Huffington Post, “The Road to Wars” <http://www.huffingtonpost.com/richard-klass/the-road-to-wars_b_4524280.html>)

Senator Robert Menendez (D-NJ), chairman of the Senate Foreign Relations Committee, has introduced legislation that sets the United States on the road to war with Iran and the road to an internal war within the Democratic Party. The bill (S.1881), which has many Democratic co-sponsors, increases the chances for war in two major ways. First, it undercuts ongoing negotiations to build on the first-step nuclear agreement with Iran by adding additional sanctions before the current six month negotiating period plays out. Iran has threatened to withdraw from these negotiations if a bad faith act, such as adding new sanctions, transpires. The U.S. would do the same if, for example, Iran's parliament passed legislation to open a new nuclear production facility. If the first-step deal collapses, there will be no problem in quickly instituting new sanctions. And there will certainly be calls for military action, no matter how short-term the results would be. But if the collapse is triggered by a U.S. unilateral action, the coalition now enforcing those sanctions could well collapse. This undermining of the president's negotiating authority and international cooperation is as unprecedented as it is dangerous. The second danger in this bill is that it encourages an Israeli attack on Iran. The bill states that "... if the Government of Israel is compelled to take military action in legitimate self-defense against Iran's nuclear weapon program, the United States Government should stand with Israel and provide ..., diplomatic, military, and economic support to the Government of Israel in its defense of its territory, people, and existence...." While the language is "should," not "must," and there are bows to the Constitution and congressional authority, this is a clear signal to Israel that it can count on U.S. support for a "unilateral" air strike. And Iran cannot be blamed if it takes it that way. No one should doubt who will determine if the Iranian program provides an existential threat to Israel. The Israeli government's position is that any enrichment in Iran is such a threat. Yet reaching any agreement with Iran will undoubtedly require some residual domestic enrichment capability. Military experts agree that Israel would need substantial U.S. help for any effective attack. This would include not only intelligence and aerial refueling, but also combat search and rescue for downed Israeli pilots, possible suppression of enemy air defenses and other direct combat missions. In short, war. This language, while not requiring that the U.S. support an Israeli attack, certainly will be taken that way in Israel and Iran. Also, it just might be enough to doom a diplomatic settlement and unleash the dogs of war.

#### Global war

-Strikes fail: intel gap and buried

-Iran second strike = nuclear

-Economy: stops oil

-Hegemony: Balancers

-Miscalc/Escalation: Forces on nuclear alter

**Reuveny, 10** – professor in the School of Public and Environmental Affairs at Indiana University (Rafael, “Unilateral strike could trigger World War III, global depression” Gazette Xtra, 8/7, - See more at: <http://gazettextra.com/news/2010/aug/07/con-unilateral-strike-could-trigger-world-war-iii-/#sthash.ec4zqu8o.dpuf>)

A unilateral Israeli strike on Iran’s nuclear facilities would likely have dire consequences, including a regional war, global economic collapse and a major power clash.¶ For an Israeli campaign to succeed, it must be quick and decisive. This requires an attack that would be so overwhelming that Iran would not dare to respond in full force.¶ Such an outcome is extremely unlikely since the locations of some of Iran’s nuclear facilities are not fully known and known facilities are buried deep underground.¶ All of these widely spread facilities are shielded by elaborate air defense systems constructed not only by the Iranians but also the Chinese and, likely, the Russians as well.¶ By now, Iran has also built redundant command and control systems and nuclear facilities, devloped early warning systems, acquired ballistic and cruise missiles and upgraded and enlarged its armed forces.¶ Because Iran is well-prepared, a single, conventional Israeli strike—or even numerous strikes—could not destroy all of its capabilities, giving Iran time to respond.¶ Unlike Iraq, whose nuclear program Israel destroyed in 1981, Iran has a second-strike capability comprised of a coalition of Iranian, Syrian, Lebanese, Hezbollah, Hamas, and, perhaps, Turkish forces. Internal pressure might compel Jordan, Egypt and the Palestinian Authority to join the assault, turning a bad situation into a regional war.¶ During the 1973 Arab-Israeli War, at the apex of its power, Israel was saved from defeat by President Nixon’s shipment of weapons and planes. Today, Israel’s numerical inferiority is greater, and it faces more determined and better-equipped opponents. After years of futilely fighting Palestinian irregular armies, Israel has lost some of its perceived superiority—bolstering its enemies’ resolve.¶ Despite Israel’s touted defense systems, Iranian coalition missiles, armed forces, and terrorist attacks would likely wreak havoc on its enemy, leading to a prolonged tit-for-tat.¶ In the absence of massive U.S. assistance, Israel’s military resources may quickly dwindle, forcing it to use its alleged nuclear weapons, as it had reportedly almost done in 1973.¶ An Israeli nuclear attack would likely destroy most of Iran’s capabilities, but a crippled Iran and its coalition could still attack neighboring oil facilities, unleash global terrorism, plant mines in the Persian Gulf and impair maritime trade in the Mediterranean, Red Sea and Indian Ocean.¶ Middle Eastern oil shipments would likely slow to a trickle as production declines due to the war and insurance companies decide to drop their risky Middle Eastern clients. Iran and Venezuela would likely stop selling oil to the United States and Europe.¶ From there, things could deteriorate as they did in the 1930s. The world economy would head into a tailspin; international acrimony would rise; and Iraqi and Afghani citizens might fully turn on the United States, immediately requiring the deployment of more American troops.¶ Russia, China, Venezuela, and maybe Brazil and Turkey—all of which essentially support Iran—could be tempted to form an alliance and openly challenge the U.S. hegemony.¶ Russia and China might rearm their injured Iranian protege overnight, just as Nixon rearmed Israel, and threaten to intervene, just as the U.S.S.R. threatened to join Egypt and Syria in 1973. President Obama’s response would likely put U.S. forces on nuclear alert, replaying Nixon’s nightmarish scenario.¶ Iran may well feel duty-bound to respond to a unilateral attack by its Israeli archenemy, but it knows that it could not take on the United States head-to-head. In contrast, if the United States leads the attack, Iran’s response would likely be muted.¶ If Iran chooses to absorb an American-led strike, its allies would likely protest and send weapons but would probably not risk using force.¶ While no one has a crystal ball, leaders should be risk-averse when choosing war as a foreign policy tool. If attacking Iran is deemed necessary, Israel must wait for an American green light. A unilateral Israeli strike could ultimately spark World War III.

### 4th Off

#### The US has established Cyber Deterrence

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

#### Congressional restrictions kill cyber effectiveness—speed and flex key.

Walker 10

(Paul, Operations Law Attorney, U.S. Cyber Command, “Traditional Military Activities in Cyberspace: Preparing for Netwar,” http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2245061)

These legal and policy disputes over the employment of Special Operations forces and information-based actions, such as the attack on the jihadist website, will grow increasingly important in the coming years. The United States faces an agile, networked adversary. The age of netwar is upon us.8 Speed and flexibility will be essential to meeting and defeating networked enemies, such as al Qaeda. John Arquilla, the foremost thinker about networked warfare, recently called for the military to develop new rules for confronting such enemies.9 In a nutshell, Arquilla‘s rules are: ―Many and small‖ forces finding rather than flanking the adversary by swarming, not surging.10 Special Operations forces are in the forefront of today‘s military in this style of warfare. Special Operations units are normally broken down into twelve-man ―A teams‖ or squads, depending on the service.11 The teams train as a unit and are often called on to carry out operations that would require greater numbers of regular troops.12 Likewise, information-based warfare assumes greater prominence and dominance in a world dominated by networks. Warfare using the network of networks—the Internet—will be the ultimate force multiplier against networked adversaries, whether they are international terrorists, international drug traffickers, or the armed forces of adversary states. In order to respond with the speed and agility required in a networked environment, legal rules and authorities must keep pace with technology and changing methods of warfare. The first step in achieving this speed and agility is recognizing that there are a vast array of traditional military activities that can occur in the Internet and other information environments that do not need to be reported to Congress as ―covert actions. Although one may argue with it as a policy decision,13 this Article argues that the military‘s decision to conduct a cyber action against the CIA and Saudi-monitored website was well within the norms of traditional military activity. Because the action occurred during the course of an armed conflict against al Qaeda, there would also be no need to acknowledge such an action when it was directed by a military commander. This Article explores the array of traditional military activities that may occur in the Internet and other information environments without triggering covert action reporting requirements through the prism of a historical examination of two types of military activity that contribute to the accomplishment of strategic surprise: positioning of forces and deception operations.

#### Offensive Cyber capabilities are key to an effective deterrent

Jari Rantapelkonen & Mirva Salminen, ’13 (“THE FOG OF CYBER DEFENCE”, National Defence University Department of Leadership and Military Pedagogy Publication Series 2 Article Collection n:o 10)

Offensive Weaponry is Required for Credibility and Deterrence¶ Discussion on offensive cyber weaponry should begin. As emphasized, currently there is no credible status for the armed forces and the nation states without cyber capabilities – this includes the offensive capability. The arms race is on and accelerating, even if we would like to turn a blind eye to it. The most frantic contemporary race is about talented individuals. When it comes to the creation of cyber capabilities, the question is not about the number of people one employs but about the talent the employed have. The US, China, Russia and many other countries are actively recruiting promising hackers. So are, most likely, Al Qaeda and other organizations. The real cyber question is about the talent and about creating cyber capabilities with the help of the most talented individuals.¶ It is not very popular or even desirable to talk publicly about offensive cyber weaponry in most countries. However, it has become necessary to explain the logic of offensive cyber capabilities to the general public. Naturally, this has to be done in various ways in different countries due to cultural and national reasons. The reasons why countries are developing offensive weapons and why they need them can be summarized into the following four points.¶ First, if one wishes to be a credible actor both in the military battlefield and in world politics, one must have offensive capabilities – as one must have defensive capabilities and the ability to be resilient. One simply cannot have a credible cyber defence without offensive abilities.¶ Second, in order to achieve and raise her deterrence, one must possess offensive capabilities. The ability to act offensively includes a strong preventive message to the others – provided that they understand it and believe it. Offensive capabilities represent the key component of deterrence.¶ Third, offensive thinking and building offensive weaponry are vital in order to create a strong and credible defence. With just “defence thinking” one will not succeed. One has to have an understanding of how the attacker acts, and one should try to find all possible vulnerabilities in her own defence. It is also a matter of developing one’s defensive potentials, testing the current defence and training one’s forces. All this becomes much more efficient if one can test it with her own capabilities. Without the ability to act as an attacker, no country can build an effective and credible cyber defence.

#### Cyber Deterrence is ultimate deterrent- prevents Great Power War

Jari Rantapelkonen & Mirva Salminen, ’13 (“THE FOG OF CYBER DEFENCE”, National Defence University Department of Leadership and Military Pedagogy Publication Series 2 Article Collection n:o 10)

Based on that logic, cyber deterrence should play a similar role in the digitalized world. However, anonymity, advantage of attacks, global reach and interconnectedness greatly reduce the efficiency of cyber deterrence. Simultaneously, there is a lot of suspicion and rumours travelling around: what kind of capabilities the others might have and how they are using them already?¶ In the kinetic world, it is much easier to evaluate the opponent’s capabilities. It is quite easy to make a valid estimate on how many tanks, interceptors or submarines a country possesses. Countries also openly expose their arsenal, for example, in military parades, as well as their operational skills, for example, by organizing large military exercises. In the logic of deterrence, it is even more important to manifest force than to have real capabilities – yet the others have to know it.¶ Awareness Prevents Conflicts¶ Deterrence depends upon effective communication between the state and the entity it wishes to deter. One has to convince the others that if they attack, one has the capability and the capacity to do something about it. This is also the case in the cyber domain. If a country wants to be a credible actor in this domain, it should openly declare its offensive policy and expose its offensive capabilities. The policy acts as the rules for engagement. This is the trend some countries are already moving toward. For example, for the first time since the Second World War, Germany has publicly disclosed that it is developing offensive cyber weapons.5 In addition, in the latest Cyber Strategy of the United States, offensive cyber policy is strongly emphasized, and it has been said in public that the US Defense Advanced Research Projects Agency (DARPA) is focusing its research on offensive cyber capabilities.6 It has also been announced by many countries that a response to a cyber attack is not limited to the cyber domain, which is very understandable. The world needs to start talking openly about offensive cyber capabilities and the readiness levels – just as we discuss missile arsenals, air force, submarine fleets, or doctrines. We talk about great military exercises taking place in the kinetic world, but there is very little public discussion on things happening in cyberspace. Today, countries are aware of and appreciate the kinetic capacities which the others have. This is one reason why there are so few on- going wars in the world. Awareness prevents conflicts – at least, between the nation states – and it raises the threshold for conducting an attack. The defence policy of many countries is based on this assumption – if you have and if you are able to expose strong enough military capability, the likelihood of being attacked decreases.

# Solvency

#### Prez will circumvent-

#### [1.] invokes state secrets to avoid oversight

Posner and Vermeule 2010 [Eric A. , Professor of Law at the University of Chicago Law School and Editor of The Journal of Legal Studies; Adrian , Harvard Law Professor, The Executive Unbound: After the Madisonian Republic, Oxford Press, p. 24//wyo-sc]

Monitoring the executive requires expertise in the area being monitored. In many cases, Congress lacks the information necessary to monitor discretionary policy choices by the executive. Although the committee system has the effect, among others, of generating legislative information and expertise,18 and although Congress has a large internal staff, there are domains in which no amount of legislative expertise suffices for effective oversight. Prime among these are areas of foreign policy and national security. Here the relative lack of legislative expertise is only part of the problem; what makes it worse is that the legislature lacks the raw information that experts need to make assessments. The problem would disappear if legislators could cheaply acquire information from the president, but they cannot. One obstacle is a suite of legal doctrines protecting executive secrecy and creating deliberative privileges— doctrines that may or may not be justified from some higher-order systemic point of view as means for producing optimal deliberation within the executive branch. Although such privileges are waivable, the executive often fears to set a bad institutional precedent. Another obstacle is the standard executive claim that Congress leaks like a sieve, so that sharing secret information with legislators will result in public disclosure. The problem becomes most acute when, as in the recent controversy over surveillance by the National Security Agency, the executive claims that the very scope or rationale of a program cannot be discussed with Congress, because to do so would vitiate the very secrecy that makes the program possible and beneficial. In any particular case the claim might be right or wrong; legislators have no real way to judge, and they know that the claim might be made either by a wellmotivated executive or by an ill-motivated executive, albeit for very different reasons.

#### [3.] Empirics on presidents ignoring WPR prove the trend

Isaacs 2011

[John Isaacs, 2011, executive director of Council for a Livable World, War Powers Resolution consistently ignored, <http://thehill.com/blogs/congress-blog/foreign-policy/172803-war-powers-resolution-consistently-ignored>, uwyo//amp]

President Harry F. Truman ignored Congress when in 1950 he sent troops to Korea to stave off a North Korean advance into the South. Almost 1.8 million Americans fought in Korea, with some 33,600 American deaths. But there never was a congressional authorization, and Congress continued to appropriate funds to prosecute the war. The War Powers Resolution also appeared to be a check against Nixon’s power, a President recently overwhelmingly re-elected who was becoming more and more enmeshed in the Watergate scandal. Indeed, I played only a bit role, helping to convince some liberals such as Representatives Bella Abzug (D-NY) and Robert Drinan (D-Mass.) that Congress was not ceding additional power to the President by giving him or her 60 or 90 days to conduct war without approval of Congress. Fast forward to today. Every President since 1973, including Barack Obama, has decided to ignore the law as an unconstitutional assertion of power.

#### [4.] Cancels testimony, Justice Department ignores oversight requests

Victor ‘03

[Kirk Victor, writer for government executive.com, 2003, Congress in eclipse as power shifts to executive branch, <http://www.govexec.com/management/2003/04/congress-in-eclipse-as-power-shifts-to-executive-branch/13800/>, uwyo//amp]

Senate Finance Committee Chairman Charles Grassley, R-Iowa, agreed in an interview that "getting information from the Justice Department under Ashcroft is like pulling teeth." But Grassley sees it as an institutional problem, and said it had also been difficult to get responses when Janet Reno led the department. Grassley said he has had no problem in asserting his oversight powers with the executive branch. As for his colleagues who worry about presidential usurpation of Congress's powers, Grassley added, "It doesn't matter to me what the president thinks, unless I want to take it into consideration. He didn't elect me-the people of Iowa elected me. I am a trustee of the people, not a messenger boy for the president." But Leahy had a far more negative, withering take on the Bush administration's actions to avoid oversight. He and some other Senate Judiciary Committee members have sent the Justice Department 28 requests for oversight information, dating back to July 2001. The department has not responded to any of them. Ashcroft "basically ignores most of the requests, but at least I give him credit for being bipartisan-he ignores Republican requests, too," Leahy said in the interview. "And this is the man who [when he was a senator] thought he should hold up judicial nominations and everything else when the attorney general didn't give us what we wanted." Several members of the Senate Foreign Relations Committee also reacted angrily when the administration canceled, at the last minute, testimony by the top official in charge of reconstruction and humanitarian assistance in Iraq, who was to appear at a March 11 hearing. They also were surprised to learn from that day's newspapers that the administration was seeking bids from U.S. corporations on reconstruction contracts for Iraq.

# Advantage One

#### No risk of cyberterror – groups lack capabilities

Fisher 2009 – editor of threatpost.com [Dennis, 10/23. “Report: Cyber-Terror Not A Credible Threat.” ThreatPOST: http://threatpost.com/en\_us/blogs/cyberte rror-not-credible-threat-102309]

A new report by a Washington policy think tank dismisses out of hand the idea that terrorist groups are currently launching cyber attacks and says that the recent attacks against U.S. and South Korean networks were not damaging enough to be considered serious incidents. The report, written by James Lewis of the [Center for Strategic and International Studies](http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf" \t "_blank), looks at cyber-war through the prism of the Korean attacks, which many commentators have speculated originated in North Korea. However, there has been little in the way of proof offered for this assessment, and Lewis doesn't go down that road. Instead, he focuses on whether the attacks constituted an act of war and whether they could have been the work of a terrorist group. "The July event was not a serious attack. It was more like a noisy demonstration. The attackers used basic technologies and did no real damage. To date, we have not seen a serious cyber attack. That is only because the political circumstances that would justify such attacks by other militaries have not yet occurred and because most non-state actors have not yet acquired the necessary capabilities. As an aside, this last point undermines the notion of cyber terrorism. The alternative to the conclusion that terrorist groups currently lack the capabilities to launch a cyber attack is that they have these capabilities but have chosen not to use them. This alternative is nonsensical," Lewis writes.

#### Cyberterror is not a threat

McKeay 2005 - CISSP and QSA with over a decade's experience in security [Martin, 12/12. “Cyber-terror Not A Real Threat,” http://www.mckeay.net/2005/12/12/cyberterror-not-a-real-threat/]

Is there such a thing as a cyber-terror attack? If you believe what this article tells you, then the answer is no. And seeing as how people like [Bruce Schneier](http://www.schneier.com/blog/" \t "_blank) have been saying the same thing for several years, I’m tempted to agree. This isn’t to say it’s not possible to make a cyber-attack on any country, even America, but it such an attack won’t be based on terror. One of the things a terrorist attack needs is a visceral, heart-rending reality that cannot be attained by attacking data streams. Sure, people will be hurt by the secondary effects of a virtual war, but secondary effects don’t have the ability to affect emotions that pure physical destruction does. I only recognized a couple of the names from this article, but I think they hit the nail on the head. At some point another large country might take a shot at the United States through our infrastructure, but not some terrorist group. First, there’s still too much diversity to make such an attack feasible. Yes, I know I’ve backed the ‘monoculture argument before, but that was at the desktop level not the infrastructure level. Second, the resources necessary to make such an attack are beyond most countries, let alone a small group. Bottom line: we will see attacks against the Internet infrastructure at some point, but it won’t be a terror-based attack. Those will stay in the real world.

**Cyber-terrorism is unlikely**

**Poulsen ’07**

[Kevin, Wired News, “Cyberwar,” Aug 22, http://blog.wired.com/27bstroke6/2007/08/cyber-war-and-e.html]

Even those **attacks fell short of cyberwar, at least as experts have defined the term for over a decade. Cyberwars were supposed to target critical infrastructures beyond the internet**, like the [SCADA](http://en.wikipedia.org/wiki/SCADA) systems that control elements of the power grid; air traffic control networks; nuclear power plant safety systems. In other words,  **real cyberwarriors aren't interested in clogging the public internet like spammers; they use the internet as a path to sensitive, private networks where sabotage has some hope of causing physical, real-world mayhem that outlasts the attack**. (DDoS barely rated a walk-on role in DHS's comprehensive [Cyber Storm exercise](http://blog.wired.com/27bstroke6/2006/08/when_hippies_tu.html) last year.) **I'm skeptical that real cyberwar, or cyberterrorism, will ever take place.**

**Despite years of warnings, there have been no attacks to the power grid – critical infrastructure is more susceptible to natural disaster than cyberterror**

**Singel 09**

[Ryan, staff writer for Wired.com, Threat Level blog co-founder, “Is the Hacking Threat to National Security Overblown?” Threat Level, Wired.com, 6-3, <http://www.wired.com/threatlevel/2009/06/cyberthreat/>, uwyo//amp]

Is hacking a real threat to the United States or is it just the latest overblown threat to national security, whose magnitude is being exaggerated to expand government budgets and power? That’s the question asked by Threat Level editor Kevin Poulsen at a panel in Computers, Freedom and Privacy in Washington, D.C., Wednesday. And it’s important because the government is spending billions of dollars on computer security, and President Obama is elevating cybersecurity to a national priority, using language that makes even security experts wince. Amit Yoran, a former Bush Administration cybersecurity czar, argues the answer is easy. “Is hacking a national security threat?” Yoran said. “The one word answer is ‘Yes.’” As proof, Yoran pointed to stories about the denial-of-service attacks in Estonia, attacks on government contractor Booz Allen Hamilton and the recently reported breach of defense contractor computers that let hackers get at information on the Joint Strike Fighter. “Cyber 9-11 has happened over the last 10 years, but it’s happened slowly so we don’t see it,” Yoran said**. Poulsen called the threat of cyber-terrorism “preposterous,” citing the long-standing warnings that hackers would attack the power grid — despite the fact that it has never happened. And he argued that calling such intrusions national security threats means information about attacks gets classified unnecessarily. “If we can’t publicly share info that the attackers already have — since it’s about them — then we are doing far more harm than good,” Poulsen said, arguing that classification makes it impossible for the security community at large to analyze or prepare defenses for such attacks**. Moreover, he pointed out the Joint Strike fighter example involved only unclassified information. But security expert Bruce Schneier (a Wired.com columnist) said there are going to be cyberattacks that actually affect the real world, even though **the risk is currently overblown**. “Remove the word cyber. It’s just a new theater,” Schneier said. “Of course there is espionage, and as data moves online, there is cyber-espionage. But is it a real threat?” Schneier’s answer is yes, but not as big a threat to infrastructure as natural disasters or bad code. “We have to be robust against hackers and Murphy,” Schneier said, referring to Murphy’s law. Dr. Herb Lin, a cyberattack expert at the National Research Council, called the scoffing naive, saying he could imagine hackers getting into classified command-and-control systems, for one. But he lamented that much of the current dialogue is about about cyberwar and cyber-terror, when the largest threat is in cyber-espionage — which is not considered an act of war. “We can see why the press and government agencies talk about cyber-terror and cyberwar,” Lin said, referring ostensibly to page views and budgets, respectively. “But we don’t consider spies inside the United States to be an attack on the United States.” Yoran did admit that cyber-terrorism was improbable, but stuck to his point that there are significant national security threats from hackers.

# Advantage Two

### AT: Scenario 1

#### Automation is WAY far off—multiple barriers prevent development—and automated retailiation isn’t even on the agenda

Jackson, 6-17-13

[William, freelance writer and the author of the CyberEye blogNIST, DHS push security automation to the next stage, http://gcn.com/articles/2013/06/17/nist-dhs-push-security-automation.aspx] /Wyo-MB

The future of network security is automation, using various tools to monitor systems and network traffic for signs of trouble, alert administrators and even respond to attacks on their own. Automation can handle jobs that otherwise would have to be done by IT staff members, who are then freed up for other tasks.¶ Agencies face challenges in getting to an automated environment, however, whether because of tight budgets, complex systems or automated tools that don’t necessarily work together. The federal government is supporting the effort by developing the standards that are necessary for interoperable tools and offering intrusion detection and prevention as a service to agencies.¶ SCAP¶ The government is working to create a standards-based security environment through the Security Content Automation Protocol (SCAP), a suite of interoperable specifications developed at the National Institute of Standards and Technology in collaboration with the public- and private-sector security community.¶ Although NIST’s agenda for security automation goes beyond vulnerability management, SCAP in its present form, Version 1.2, deals primarily with endpoint compliance for configuration requirements. The specifications, contained in Special Publication 800-126, support automated configuration, vulnerability and patch checking, technical control compliance and security measurement.¶ “In the U.S. government it has been a challenge to implement configuration management,” said NIST’s Dave Waltermire, SCAP architect. “There is often a tension between allocating resources to manage systems and developing configuration management policies, procedures and baselines.”

#### Automation WONT be used for auto-retaliation—it will be used to detect insecurity and block malicious attacks prior to entering US networks—the result stabilizes security

Jackson, 6-17-13

[William, freelance writer and the author of the CyberEye blogNIST, DHS push security automation to the next stage, http://gcn.com/articles/2013/06/17/nist-dhs-push-security-automation.aspx] /Wyo-MB

While NIST is building a framework for interoperable vendor products that agencies can implement within their systems, the Homeland Security Department is developing an intrusion detection and prevention system to be offered as a managed service through agencies’ Internet service providers.¶ Einstein was initially deployed in 2004 to detect and block malicious activity across the .gov domain. The first version analyzed network flow information from participating agencies to provide a high-level view for observing potential malicious activity. Its second iteration, Einstein 2, launched in 2008, is a passive, automated system that incorporates intrusion detection based on custom signatures of known or suspected threats, and is able to alert US-CERT of malicious activity. It relies primarily on commercial tools for detection.¶ Einstein 2 now is deployed at 17 of 18 agencies that are using a Trusted Internet Connection provider, and at 52 other agencies using Managed Trusted IP Services (MTIPS) under the Networx contract. DHS officials say the department is on track to meet its milestone of providing Einstein 2 service to 70 percent of executive branch agencies by the end of fiscal 2013 as legacy networking contracts expire and agencies that are not yet served move to MTIPS. That 70 percent figure for agencies could include as much as 90 percent of .gov network traffic, officials said.¶ Einstein 2 already has shown its value for detecting and alerting, department officials said. As analytical capabilities grow its value is expected to increase, and alerting will be expanded from US-CERT to agency security operations centers as well. This is expected to happen in 2014.¶ In its next iteration, Einstein 3 will be a managed service through service providers to not only detect but also automatically block malicious traffic before it enters government networks. § Marked 08:26 § Under the direction of DHS, service providers will administer threat-based decisions on traffic entering and leaving participating agency networks. Agencies will enter into agreements with DHS to authorize use of intrusion prevention capabilities through service providers.¶ Einstein 3 includes three major activities. The first, operational today, is the ability to connect analysts with the data that will be used to block malicious traffic. The second activity is the segregation and aggregation of .gov traffic by ISPs for analysis. Four contracts for this function have been awarded; one is fully operational and two more are expected to become operational this summer. The fourth contract is being finalized and should be operational by the end of September.¶ The final activity is the trickiest one: automated blocking of malicious traffic. One contract for this was awarded to an ISP in March, but it is not yet operational. Other contracts with ISPs are in the works, and service delivery plans are being developed.¶ Initially there will be two countermeasures used by service providers against malicious traffic.¶ Domain Name Server sinkholing will block malware in .gov networks from communicating with known or suspected malicious domains, redirecting the traffic to safe sinkhole servers. ISPs will have access only to information about the DNS request for this traffic and not to the contents.¶ E-mail filtering will scan incoming mail addressed to .gov networks for malicious attachments, URLs and other malicious content. Infected e-mails could be quarantined or redirected for further inspection and analysis by DHS.¶ Even without enterprisewide systems such as Einstein and large-scale frameworks such as SCAP, individual tools have demonstrated the power of automation to improve both network security and management.

#### Low risk of cyber attacks sufficient to cause launch on warning

Rid 13

[Thomas, reader in war studies at King’s College London, “Cyber War Will Not take Place”, Journal of Strategic Studies, October 2011, <http://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.608939>, wyo-bw]

But is it? Are the Cassandras of cyber warfare on the right side of¶ history? Is cyber war really coming? This article argues that cyber war will not take place. That statement does not come with a Giraudouxian¶ twist and irony. It is meant literally – as a statement about the past, the¶ present, and the likely future: Cyber war has never happened in the past. Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future. Instead, all past and¶ present political cyber attacks are merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage. That is improbable to change in the years ahead.¶ If the use of force in war is violent, instrumental, and political, then there is no cyber offense that meets all three criteria. But more than¶ that, there are very few cyber attacks in history that meet only one of¶ these criteria.¶ ¶ The first conclusion is about subversion. In the past and present, not high-tech but low-tech has been more likely to lead to an escalation of violence, instability, and ultimately even war. In the twenty-first century, the one type of political offence with the greatest potential to unleash instability and violence may not be technologically highly¶ sophisticated sabotage, but technically rather primitive subversion. Yet¶ the Internet facilitates an unexpected effect: specific social and political¶ causes may persist in subcultures and niche groups, either temporarily¶ or over an extended time, either violently or non-violently – and they¶ may never cease attracting followers yet never go mainstream. These¶ movements may be cause-driven to a significant extent, and less¶ dependent on leaders, organization, and mass support than classical¶ insurgent groups. Weak causes become stronger in the sense that they¶ garner enough support to persist over an extended period of time,¶ constantly maintaining a self-sufficient, self-recruiting, but also self limiting¶ number of supporters and activists.¶.¶ In the 1950s and 1960s, when Giraudoux was translated into¶ English, the world faced another problem that many thought was¶ inevitable: nuclear exchange. Herman Kahn, Bill Kaufmann, and Albert¶ Wohlstetter were told that nuclear war could not be discussed publicly,¶ as Richard Clarke pointed out in his alarmist book, Cyber War. He rightly concluded that as with nuclear security, there should be more public discussion on cyber security because so much of the work has been stamped secret. But in many ways the comparison between¶ nuclear war and cyber conflict, although often made, is misplaced and problematic. This should be obvious when the Pearl Harbor comparison or the Hiroshima-analogy is given a second thought: unlike the nuclear theorists in the 1950s, cyber war theorists of the 2010s have never experienced the actual use of a deadly cyber weapon,¶ let alone a devastating one like Little Boy. There was no and there is no¶ Pearl Harbor of cyber war. Unless significantly more evidence and¶ significantly more detail are presented publicly by more than one¶ agency, we have to conclude that there will not be a Pearl Harbor of¶ cyber war in the future either.70 Then the heading of this article should¶ not be understood with Giraudoux’s sense of fine irony, but literally.¶ Needless to say, Cassandra could still have the last word.¶

#### No communications breakdowns sufficient to cause the impact

**Gartzke 12**

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

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

#### No actual launch on warning policy exists – the US maintains the option to communicate deterrence – but it’s not part of US doctrine

Ford 8

(Christopher, Director @ Center for Technology and Global Security, “Dilemmas of Nuclear Force ‘De-Alerting’,” Hudson Institute, AD: 8-30-09, http://www.hudson.org/files/documents/De-Alerting%20FINAL2%20%282%29.pdf)

This argument seems somewhat less compelling, however, when one realizes that it is based upon a confusion: U.S. and Russian nuclear postures apparently do not actually assume that launch orders will be given upon warning of attack. In fact, though the United States has always refused absolutely to *rule out* a launch-on- warning posture, apparently believing that ambiguity on this score complicates Russian planning scenarios and enhances thus deterrence10 – and although U.S. alert forces could launch on such short notice if the President actually gave the order – U.S. strategic planners appear never to have adopted such a position. Indeed, the United States has spent many billions of dollars to build and maintain an extremely capable ballistic missile submarine (SSBN) force as the backbone of its deterrent posture, precisely because of the presumed invulnerability to preemptive attack of deployed U.S. submarines on “deterrentpatrol.”11 Having such a survivable force available for retaliatory strikes necessarily means that when confronted with what appears to be an incoming Russian attack, U.S. leaders would notnecessarily face irresistible “use it or lose it” pressures to launch immediately. Since the end of the Cold War, moreover, the U.S. force posture has evolved further away from maintaining a rapid reaction capability and high alert levels, and today few of the operationally deployed U.S. nuclear forces are maintained on a ready alert status capable of immediate launch even if this were American policy. The United States carefully maintains the ability to respond promptly to any attack in order to complicate any adversary’s planning and thereby enhance deterrence, but it does not assume LOW. (Nor, however, does it ever discuss precisely what its actual alert status is. No nuclear weapons state does.12) A the U.S. Ambassador to the CD quipped at one point, in response to a request that the United States abandon its “hair- trigger” alert policy, “Frankly, in order to take action to comply with this request, we would first have to put our weapons on ‘hair-trigger alert,’ so we could then de-alert them. The fact is that U.S. nuclear forces are not and have never been on ‘hair-trigger alert.’”

#### These factors reduce the risk of accidental launch to zero

Slocombe, 09

Walter B. Slocombe, J.D. Harvard Law, Former Under Secretary of Defense for Policy and Senior advisor for the Coalition Provisional Authority in Baghdad, 21-23 June 2009, “De-Alerting: Diagnoses, Prescriptions, and Side-Effects\*” Discussion paper presented at the seminar on “Re-framing De-Alert: Decreasing the Operational Readiness of Nuclear Weapons Systems in the U.S.-Russia Context” in Yverdon, Switzerland http://www.ewi.info/system/files/Slocombe.pdf

These arrangements – PALs and their equivalents coupled with continued observance of the agreement made in the mid-90s on “de-targeting” – do not eliminate the possibility of technical or operator-level failures, but they come very close to providing absolute assurance that such errors cannot lead to a nuclear explosion or be interpreted as the start of a deliberate nuclear attack.6 The advantage of such requirements for external information to activate weapons is of course that the weapons remain available for authorized use but not susceptible of appropriation or mistaken use. The drawback from a deterrence and operational point of view is, of course, that the system for transmitting the information must not be susceptible of interruption – that is, there must be assurance that an authorized decision maker will be able to act and have the decision – and the accompanying authenticated orders and unlock combinations – communicated to and received by the operators of the weapon systems. Accordingly, a system of combination-locked safeties requires a highly survivable network for decision and communication with the operators. Otherwise there would be pressures for early transmission of the codes, with their insertion subject to a later execute order or even more dangerous, pre-delegation of authority to issue the execute orders. In this, as in other aspects of measures to meet the “never” requirement, a highly capable and highly survivable command and control system is essential.

#### 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 extraordinarilydifficult**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.

### AT: Scenario Two

**US can’t solve modeling – the development of offensive capabilities is inevitable.**

**Libicki 2009**

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

Historically, **arms control has always gone hand in hand with deter- rence and crisis stability, but it would be difficult to be optimistic about its prospects in cyberspace**. A good deal depends on what one means by arms control. If the model were to be something like the treaties signed between the United States–NATO and the Soviet Union– Warsaw Pact, which limited certain classes of weapons and banned others, there is little basis for hope. 1 If, instead, the goal were a framework of international agreements and norms that could raise the diffi- culty of certain types of cyberattacks, some progress can be made. Why is it nearly impossible to limit or ban cyberweapons? First, **although the purpose of “limiting” arms is to put an inventory-based lid on how much damage they can do in a crisis, such a consideration is irrelevant in a medium in which duplication is instantaneous**. 2 Second, banning attack methods is akin to banishing “how-to” information, which is inherently impossible (like making advanced mathematics illegal). The same holds for banning knowledge about vulnerabilities. Third, **banning attack code is next to impossible**. Such code has many legitimate purposes, not least of which is in building defenses against attack from others. These others include individuals and nonstate actors, so **the argument that one does not need defenses because offenses have been outlawed is unconvincing§ Marked 08:27 § . In many, per- haps most cases, such attack code is useful for espionage, an activity that has yet to be banned by treaty. Furthermore, finding such code is a hopeless quest.** The world’s information storage capacity is immense; much of it is legitimately encrypted; and besides, bad code does not emit telltale odors. If an enforcement entity could search out, read, and decrypt the entire database of the world, it would doubtless find far more interesting material than malware. **Exhuming digital informa- tion from everyone else’s systems is hard enough when the authorities with arrest powers try it; it may be virtually impossible when outsiders try**. The only barely feasible approach is to ban the activity of writing attack code, then hope that the fear of being betrayed by an insider who goes running to international authorities prevents governments from organizing small groups of elite hackers from engaging in such nefarious activities. **If the international community had the manpower and access to enforce such norms, it could probably enforce a great many other, and more immediately practical, norms** (e.g., against cor- ruption). **Such a world does not exist.**

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

**Libicki 9**

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

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

**Escalation is unlikely due to deterrence and international checks**

**Gartzke 12**

(Erik, Associate Professor in Political Science at UC-San Diego. “The Myth of Cyberwar” Page 23 12-7-12 http://dss.ucsd.edu/~egartzke/papers/cyberwar\_12062012.pdf//wyoccd)

**An open question exists in any crisis about how far competitors are willing to escalate, but an¶ ability to counter cyber attack with other, more kinetic forms of military violence serves alternately¶ to deter or to facilitate the use of cyber capabilities, giving those nations with terrestrial military¶ power yet another option that, even if available to their opponents, may prove extraordinarily¶ dangerous to practice**. **As we see today with U.S. drone attacks and special operations raids on¶ foreign sovereign territory, the power to do much more ensures that an opponent maintains a level¶ of discretion in its response to provocation**. Few can doubt the reaction of the United States, for¶ example, if **Pakistan were to attempt to conduct a commando raid on U.S. territory. Nations that¶ can physically punish others for transgressions in any domain, electronic or otherwise, are better¶ able to operate in all domains**. Once one distinguishes between simple vulnerability and actual¶ threats, terrestrial capabilities become pivotal in determining who exercises cyber capabilities.¶

**The impacts of a cyber attack would be small and temporary**

**Gartzke 12**

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

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

### AT: Scenario 3

**Weak Obama on cybersecurity emboldens Chinese cyber attacks**

**Davis 2013**

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

**American foreign policy is usually the sole province of the executive branch** - treaty ratification and Congressional resolutions authorizing the use of force notwithstanding. In a world that is still decades -- and in some cases centuries -- behind Western civilization with respect to openness, tolerance, and human rights, **American foreign policy works best when we have a president who grasps** Theodore Roosevelt's **"big stick" doctrine**. Moreover, **the president must,** in the words of John F. Kennedy, "**Let every nation know**, whether it wishes us well or ill, **that we shall pay any price, bear any burden,** meet any hardship, support any friend, **oppose any foe to assure the survival and the success of liberty.**" President Barack **Obama is failing miserably** on both accounts **when it comes to Chinese cyber security**. Last month, the security firm Mandiant released a report that concluded **the Chinese military "has systematically stolen hundreds of terabytes of data** from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously." Moreover, the report notes that the observed thefts are but a fraction of what has likely been stolen since at least 2006. In other words, **Obama is fiddling while our technology is being pilfered**. Michigan's own U.S. Rep. Mike Rogers, R-Brighton, said in a statement the same day the report was released: "The Chinese government's direct role in cyber theft is rampant and the problems have grown exponentially. The Mandiant report provides vital insights into the Chinese government’s economic cyber espionage campaign against American companies. **It is crucial that the Administration begin bilateral discussions to ensure that Beijing understands § Marked 08:27 § that there are consequences for state sponsored economic espionage."** Rogers is a tough, no-nonsense former FBI agent. He's an expert on international security. He and C.A. "Dutch" Ruppersberger, D-Maryland, have introduced legislation to help, but that doesn't make China -- or its ambitions with respect to American technology -- disappear. Rather, **the main person who needs to act -- and with a clear demonstration that Chinese predation of American technology will be punished severely -- is the president. It is his reaction to this crisis** (another one that has been all but ignored by the mainstream media, for the sake of the usual twaddle) **that will either thwart or encourage the Chinese.**

#### ] New study find cyber war highly unlikely

Oxford ‘11

[PhysOrg.com, “Cyber war unlikely: study” 1.17.2011. <http://phys.org/news/2011-01-cyber-war.html>//wyo-hdm]

The study, by Dr. Ian Brown of the Oxford Internet Institute (OII), University of Oxford, and Professor Peter Sommer of the London School of Economics also concludes that it is highly unlikely there will ever be a pure ‘cyber war’ fought solely in cyberspace with equivalent effects to recent wars in Afghanistan, the Balkans or the Middle East. The report, part of a wider OECD project on Future Global Shocks, is aimed at governments, global businesses and policy makers. It looks at the nature of global catastrophes and then asks which possible cyber-events might create similar effects. In addition to the actions of governments and terrorists the study also considers criminals and accidents. There is a review of current government action, an examination of how governments interact with the private sector and a consideration of the prospects for international cooperation and treaties. The best protections are careful system design, the use of products to detect known viruses and system intrusions, and user education, says the report. It adds that it is also essential to have proper contingency plans for system recovery. Dr. Brown commented: "We think that a largely military approach to cybersecurity is a mistake. Most targets in the critical national infrastructure of communications, energy, finance, food, government, health, transport, and water are in the private sector. Because it is often difficult to be certain who is attacking you from cyberspace, defence by deterrence does not work." "That said, cyberweaponry in all its forms will play a key role alongside more conventional and psychological attacks by nation states in future warfare." "We don’t help ourselves using “cyberwar” to describe espionage or hacktivist blockading or defacing of websites, as recently seen in reaction to WikiLeaks," said Professor Sommer, visiting professor at LSE. "Nor is it helpful to group trivially avoidable incidents like routine viruses and frauds with determined attempts to disrupt critical national infrastructure." The study says that many ‘cyber’ risks are real but that it is important to test each one to understand all the elements that are required before a potential threat causes real damage. How much research is required on the target, in writing computer code that won’t be detected, and how long will the event last before the attacked system is able to recover? It says this type of careful analysis helps us understand what we should really worry about and points the way to remedies. The study is part of a broader OECD review of Future Global Shocks which covers pandemics and further collapse of the world financial system. The UK Government has announced as part of its Strategic Defence and Security Review that £650m is available to address ‘cyber’ attacks, seen as a Tier One threat.

**[3] Defensive dominance prevents big attacks**

**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)

"Cyberweapons Can Create Massive Collateral Damage." **Very unlikely**. When news of Stuxnet broke, the New York Times reported that the most striking aspect of the new weapon was the "collateral damage" it created. The malicious program was "splattered on thousands of computer systems around the world, and much of its impact has been on those systems, rather than on what appears to have been its intended target, Iranian equipment," the Times reported. Such descriptions encouraged the view that computer viruses are akin to highly contagious biological viruses that, once unleashed from the lab, will turn against all vulnerable systems, not just their intended targets. But this metaphor is deeply flawed.**As the destructive potential of a cyberweapon grows, the likelihood that it could do far-reaching damage across many systems shrinks.**Stuxnet did infect more than 100,000 computers -- mainly in Iran, Indonesia, and India, though also in Europe and the United States. But it was so specifically programmed that it didn't actually damage those machines, afflicting only Iran's centrifuges at Natanz. The worm's aggressive infection strategy was designed to maximize the likelihood that it would reach its intended target. Because that final target was not networked, "all the functionality required to sabotage a system was embedded directly in the Stuxnet executable," the security software company Symantec observed in its analysis of the worm's code. So yes, Stuxnet was "splattered" far and wide, but it only executed its damaging payload where it was supposed to. Collateral infection, in short, **is not necessarily collateral damage**. A sophisticated piece of malware may aggressively infect many systems, but if there is an intended target, the infection will likely have a distinct payload that will be harmless to most computers. Especially in the context of more sophisticated cyberweapons, the image of inadvertent collateral damage doesn't hold up. They're more like a flu virus that only makes one family sick. "In Cyberspace, Offense Dominates Defense." **Wrong again**. The information age has "offense-dominant attributes," Arquilla and Ronfeldt wrote in their influential 1996 book, The Advent of Netwar. This view has spread through the American defense establishment like, well, a virus. A 2011 Pentagon report on cyberspace stressed "the advantage currently enjoyed by the offense in cyberwarfare." The intelligence community stressed the same point in its annual threat report to Congress last year, arguing that offensive tactics -- known as vulnerability discovery and exploitation -- are evolving more rapidly than the federal government and industry can adapt their defensive best practices. The conclusion seemed obvious: Cyberattackers have the advantage over cyberdefenders, "with the trend likely getting worse over the next five years." A closer examination of the record, however, reveals three factorsthat put the offense at a disadvantage. First is the **high cost** of developing a cyberweapon, in terms of time, talent, and target intelligence needed. Stuxnet, experts speculate, took a superb team and a lot of time. Second, the **potential for generic offensive weapons may be far smaller than assumed** for the same reasons, and significant investments in highly specific attack programs may be deployable only against a very limited target set. Third, once developed, an offensive tool is likely to have a far shorter half-life than the defensive measures put in place against it. Even worse, a weapon may only be able to strike a single time; once the exploits of a specialized piece of malware are discovered, the most critical systems will likely be patched and fixed quickly. And a weapon, even a potent one, is not much of a weapon if an attack cannot be repeated.**Any political threat relies on the credible threat to attack or to replicate a successful attack. If that were in doubt, the coercive power of a cyberattack would be drastically reduced**.

**[3] Their authors conflate threats**

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)

This increased focus on cyber-security has led to concern that **the perceived risk is greater than the actual risk**, a situation that has resulted in an imbalance between security and privacy and civil liberties (American Civil Liberties Union 2012). In 1993 a Rand Corporation paper predicted that “cyberwar is coming” and **twenty years later the prediction is the same** and critics argue that cyber-war is “more hype than hazard” (Rid 2012). A review of high profile cyberattacksshows that, with the exception of Stuxnet and the limited Israeli disruption of Syrian airdefense networks, **most cyber-attacks are**categorized as **information theft,** network compromise, **or website defacement**(Lewis 2012). Even the high profile threat of an “Electronic Pearl Harbor” (Bronk 2009), despite being repeated by senior government officials like U.S. Defense Secretary Leon Panetta (Rid 2012) , has been found to be **only aslight possibility**(Wilson 2005). There is no doubt that cyber-security is important. Businesses recognize this importance and spent more than $80 billion on computer network security in 2011 (Johnson 2012) and the federal government is expected to be spending $10.5 billion per year by 2015 (Brito and Watkins 2012). This response is appropriate when data shows that the vast majority of cyber-attacks arefocused on espionage and the theft of intellectual property. It is not clear why **senior governmentofficials**and corporate executives **focus on high-impact low-probability events and engage in “alarmist rhetoric**” (Brito and Watkins 2011) that skews the public perception of risk and createsan atmosphere of fear. The danger of an inappropriate response in reaction to an inflated threat and prevalence of misinformation is exemplified by the politicized intelligence that led to the invasion of Iraq in 2003 (Brito and Watkins 2011). Understanding how information on the risk posed by cyber-attacks is poorly communicated and the public reaction to an increased perception of risk – fear – is important in identifying when the perceived risk is greater than the actual risk; when risk is more hype than threat. Critics of current cyber-security policy believe that **threats are being conflated**; thisresults in a threat appearing larger than it is (Brito and Watkins 2012). In essence, a wide variety of cyber-activity – political and social activity, criminal activity for profit, espionage, and offensive cyber-attack – are treated as presenting the same level of threat. There is a wide dividebetween easily mounted and easily defended denial of service attacks on public websites andhigh-potential cyber-weapons capable of severely disrupting or destroying critical infrastructure(Rid and McBurney 2012). The rise of automated tools that allow for low-level cyber-attacks to be easily mounted has caused a significant increase in the number of cyber-attacks, **a statisticoften cited as proof of increased risk**,**but qualified cyber**-security **organizations have discarded the number of cyber-attacks as a metric and consider it to be meaningless** as a method of assessing the scope and effects of cyber-attacks (Wilson 2005). Without differentiatingbetween generic malicious software and highly specialized and targeted offensive cyber-attacks, the risk of cyber-attacks on critical infrastructure systems like the electrical grid **cannot be properly assessed.**

# 2nc

### Norms

#### International community is swayed by president as the “voice of america” even in the face of congressional opposition

Zbigniew Brzezinski, national security advisor under U.S. President Jimmy Carter, 12/3/12, Obama's Moment, www.foreignpolicy.com/articles/2012/12/03/obamas\_moment

In foreign affairs, the central challenge now facing President Barack Obama is how to regain some of the ground lost in recent years in shaping U.S. national security policy. Historically and politically, in America's system of separation of powers, it is the president who has the greatest leeway for decisive action in foreign affairs. He is viewed by the country as responsible for Americans' safety in an increasingly turbulent world. He is seen as the ultimate definer of the goals that the United States should pursue through its diplomacy, economic leverage, and, if need be, military compulsion. And the world at large sees him -- for better or for worse -- as the authentic voice of America.

To be sure, he is not a dictator. Congress has a voice. So does the public. And so do vested interests and foreign-policy lobbies. The congressional role in declaring war is especially important not when the United States is the victim of an attack, but when the United States is planning to wage war abroad. Because America is a democracy, public support for presidential foreign-policy decisions is essential. But no one in the government or outside it can match the president's authoritative voice when he speaks and then decisively acts for America.

This is true even in the face of determined opposition. Even when some lobbies succeed in gaining congressional support for their particular foreign clients in defiance of the president, for instance, many congressional signatories still quietly convey to the White House their readiness to support the president if he stands firm for "the national interest." And a president who is willing to do so publicly, while skillfully cultivating friends and allies on Capitol Hill, can then establish such intimidating credibility that it is politically unwise to confront him. This is exactly what Obama needs to do now.

**Constraints through executive coordination solves signaling**

**POSNER & VERMEULE 2006** --- \*Prof of Law at U Chicago, AND \*\* Prof of Law at Harvard (9/19/2006, Eric A. Posner & Adrian Vermeule, “The Credible Executive,” <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=931501)>)

IV. Executive Signaling: Law and Mechanisms

We suggest that the executive’s credibility problem can be solved by second-order mechanisms of executive signaling. In the general case, well-motivated executives send credible signals by taking actions that are more costly for ill-motivated actors than for well-motivated ones, thus distinguishing themselves from their ill-motivated mimics. Among the specific mechanisms we discuss, an important subset involve executive self-binding, whereby executives commit themselves to a course of action that would impose higher costs on ill-motivated actors. Commitments themselves have value as signals of benign motivations.

This departs from the usual approach in legal scholarship. Legal theory has often discussed self-binding by “government” or government officials. In constitutional theory, it is often suggested that constitutions represent an attempt by “the people” to bind “themselves” against their own future decisionmaking pathologies, or relatedly that constitutional prohibitions represent mechanisms by which governments commit themselves not to expropriate investments or to exploit their populations.71 Whether or not this picture is coherent,72 it is not the question we examine here, although some of the relevant considerations are similar.73 We are not concerned with binding the president so that he cannot abuse his powers, but with how he might bind himself or take other actions that enhance his credibility, so that he can generate support from the public and other members of the government.

Furthermore, our question is subconstitutional; it is whether a well-motivated executive, acting within an established set of constitutional and statutory rules, can use signaling to generate public trust. Accordingly we proceed by assuming that no constitutional amendments or new statutes will be enacted. Within these constraints, what can a well-motivated executive do to bootstrap himself to credibility? The problem for the well-motivated executive is to credibly signal his benign motivations; in general, the solution is to engage in actions that are less costly for good types than for bad types.

We begin with some relevant law; then examine a set of possible mechanisms, emphasizing both the conditions under which they might succeed and the conditions under which they might not; and then examine the costs of credibility.

A. A Preliminary Note on Law and Self-Binding

Many of our mechanisms are unproblematic from a legal perspective, as they involve presidential actions that are clearly lawful. But a few raise legal questions; in particular, those that involve self-binding.74 Can a president bind himself to respect particular first-order policies? With qualifications, the answer is “yes, at least to the same extent that a legislature can.” Formally, a duly promulgated executive rule or order binds even the executive unless and until it is validly abrogated, thereby establishing a new legal status quo.75 The legal authority to establish a new status quo allows a president to create inertia or political constraints that will affect his own future choices. In a practical sense, presidents, like legislatures, have great de facto power to adopt policies that shape the legal landscape for the future**.** A president might commit himself to a long-term project of defense procurement or infrastructure or foreign policy, narrowing his own future choices and generating new political coalitions that will act to defend the new rules or policies.

More schematically, we may speak of formal and informal means of self-binding:

(1) The president might use formal means to bind himself. This is possible in the sense that an executive order, if otherwise valid, legally binds the president while it is in effect and may be enforced by the courts. It is not possible in the sense that the president can always repeal the executive order if he can bear the political and reputational costs of doing so.

(2) The president might use informal means to bind himself. This is not only possible but frequent and important. Issuing an executive rule providing for the appointment of special prosecutors, as Nixon did, is not a formal self-binding.76 However, there may be large political costs to repealing the order. This effect does not depend on the courts’ willingness to enforce the order, even against Nixon himself. Court enforcement makes the order legally binding while it is in place, but only political and reputational enforcement can protect it from repeal. Just as a dessert addict might announce to his friends that he is going on a no-dessert diet in order to raise the reputational costs of backsliding and thus commit himself, so too the repeal of an executive order may be seen as a breach of faith even if no other institution ever enforces it.

In what follows, we will invoke both formal and informal mechanisms. For our purposes, the distinction between the authority to engage in de jure self-binding (legally limited and well-defined) and the power to engage in de facto self-binding (broad and amorphous) is secondary. So long as policies are deliberately chosen with a view to generating credibility, and do so by constraining the president’s own future choices in ways that impose greater costs on ill-motivated presidents than on well-motivated ones, it does not matter whether the constraint is formal or informal.

B. Mechanisms

What signaling mechanisms might a well-motivated executive adopt to credibly assure voters, legislators and judges that his policies rest on judgments about the public interest, rather than on power-maximization, partisanship or other nefarious motives? Intrabranch separation of powers. In an interesting treatment of related problems, Neal Katyal suggests that the failure of the Madisonian system counsels “internal separation of powers” within the executive branch.77 Abdication by Congress means that there are few effective checks on executive power; second-best substitutes are necessary. Katyal proposes some mechanisms that would be adopted by Congress, such as oversight hearings by the minority party, but his most creative proposals are for arrangements internal to the executive branch, such as redundancy and competition among agencies, stronger civil-service protections and internal adjudication of executive controversies by insulated “executive” decisionmakers who resemble judges in many ways.78Katyal’s argument is relevant because the mechanisms he discusses might be understood as signaling devices, but his overall approach is conceptually flawed, on two grounds. First, the assumption that second-best constraints on the executive should reproduce the Madisonian separation of powers within the executive branch is never defended. The idea seems to be that this is as close as we can get to the first-best, while holding constant everything else in our constitutional order. But the general theory of second-best states that approaching as closely as possible to the first-best will not necessarily be the preferred strategy;79 the best approach may be to adjust matters on other margins as well, in potentially unpredictable ways. If the Madisonian system has failed in the ways Katyal suggests, the best compensating adjustment might be, for all we know, to switch to a parliamentary system. (We assume that no large-scale changes of this sort are possible, whereas Katyal seemingly assumes that they are, or at least does not make clear his assumptions in this regard). Overall, Katyal’s view has a kind of fractal quality – each branch should reproduce within itself the very same separation of powers structure that also describes the whole system – but it is not explained why the constitutional order should be fractal.

Second, Katyal’s proposals for internal separation of powers are self-defeating: the motivations that Katyal ascribes to the executive are inconsistent with the executive adopting or respecting the prescriptions Katyal recommends.80 Katyal never quite says so explicitly, but he clearly envisions the executive as a power-maximizing actor, in the sense that the president seeks to remove all constraints on his current choices.81 Such an executive would not adopt or enforce the internal separation of powers to check himself. Executive signaling is not, even in principle, a solution to the lack of constraints on a power-maximizing executive in the sense Katyal implicitly intends. Although an illmotivated executive might bind himself to enhance his strategic credibility, as explained above, he would not do so in order to restore the balance of powers. Nor is it possible, given Katyal’s premise of legislative passivity or abdication, that Congress would force the internal separation of powers on the executive. In what follows, we limit ourselves to proposals that are consistent with the motivations, beliefs, and political opportunities that we ascribe to the well-motivated executive, to whom the proposals are addressed. This limitation ensures that the proposals are not self-defeating, whatever their costs.

The contrast here must not be drawn too simply. A well-motivated executive, in our sense, might well attempt to increase his power. The very point of demonstrating credibility is to encourage voters and legislators to increase the discretionary authority of the executive, where all will be made better off by doing so. Scholars such as Katyal who implicitly distrust the executive, however, do not subscribe to this picture of executive motivations. Rather, they see the executive as an unfaithful agent of the voters; the executive attempts to maximize his power even where fully-informed voters would prefer otherwise. An actor of that sort will have no incentive to adopt proposals intended to constrain that sort of actor.

Independent commissions. We now turn to some conceptually coherent mechanisms of executive signaling. Somewhat analogously to Katyal’s idea of the internal separation of powers, a well-motivated executive might establish independent commissions to review policy decisions, either before or after the fact. Presidents do this routinely, especially after a policy has had disastrous outcomes, but sometimes beforehand as well. Independent commissions are typically blue-ribbon and bipartisan.82

We add to this familiar process the idea that the President might gain credibility by publicly committing or binding himself to give the commission authority on some dimension. The president might publicly promise to follow the recommendations of such a commission, or to allow the commission to exercise de facto veto power over a policy decision before it is made, or might promise before the policy is chosen that the commission will be given power to review its success after the fact. To be sure, there will always be some wiggle room in the terms of the promise, but that is true of almost all commitments, which raise the costs of wiggling out even if they do not completely prevent it.

Consider whether George W. Bush’s credibility would have been enhanced had he appointed a blue-ribbon commission to examine the evidence for weapons of mass destruction in Iraq before the 2003 invasion, and publicly promised not to invade unless the commission found substantial evidence of their existence. Bush would have retained his preexisting legal authority to order the invasion even if the commission found the evidence inadequate, but the political costs of doing so would have been large. Knowing this, and knowing that Bush shared that knowledge, the public could have inferred that Bush’s professed motive – elimination of weapons of mass destruction – was also his real motive. Public promises that inflict reputational costs on badly motivated behavior help the well-motivated executive to credibly distinguish himself from the ill-motivated one.

The more common version of this tactic is to appoint commissions after the relevant event, as George W. Bush did to investigate the faulty reports by intelligence agencies that Iraq possessed weapons of mass destruction.83 If the president appoints after-the-fact commissions, the commissions can enhance his credibility for the next event—by showing that he will be willing, after that event, to subject his statements to scrutiny by public experts. Here, however, the demonstration of credibility is weaker, because there is no commitment to appoint any after-the-fact commissions in the future – merely a plausible inference that the president’s future behavior will track his past behavior.

Bipartisan appointments. In examples of the sort just mentioned, the signaling arises from public position-taking. The well-motivated executive might produce similar effects through appointments to office.84 A number of statutes require partisan balance on multimember commissions; although these statutes are outside the scope of our discussion, we note that presidents might approve them because they allow the president to commit to a policy that legislators favor, thus encouraging legislators to increase the scope of the delegation in the first place.85 For similar reasons, presidents may consent to restrictions on the removal of agency officials, because the restriction enables the president to commit to giving the agency some autonomy from the president’s preferences.86

Similar mechanisms can work even where no statutes are in the picture. As previously mentioned, during World War II, FDR appointed Republicans to important cabinet positions, making Stimson his Secretary of War. Clinton appointed William Cohen, a moderate Republican, as Secretary of Defense in order to shore up his credibility on security issues. Bipartisanship of this sort might improve the deliberation that precedes decisions, by impeding various forms of herding, cascades and groupthink;87 however, we focus on its credibility-generating effects. By (1) expanding the circle of those who share the president’s privileged access to information, (2) ensuring that policy is partly controlled by officials with preferences that differ from the president’s, and (3) inviting a potential whistleblower into the tent, bipartisanship helps to dispel the suspicion that policy decisions rest on partisan motives or extreme preferences, which in turn encourages broader delegations of discretion from the public and Congress.

A commitment to bipartisanship is only one way in which appointments can generate credibility. Presidents might simply appoint a person with a reputation for integrity, as when President Nixon appointed Archibald Cox as special prosecutor (although plausibly Nixon did so because he was forced to do so by political constraints, rather than as a tactic for generating credibility). A person with well-known preferences on a particular issue, even if not of the other party or widely respected for impartiality, can serve as a credible whistleblower on that issue. Thus presidents routinely award cabinet posts to leaders of subsets of the president’s own party, leaders whose preferences are known to diverge from the president’s on the subject; one point of this is to credibly assure the relevant interest groups that the president will not deviate (too far) from their preferences.

The Independent Counsel Statute institutionalized the special prosecutor and strengthened it. But the statute proved unpopular and was allowed to lapse in 1999.88 This experience raises two interesting questions. First, why have presidents confined themselves to appointing lawyers to investigate allegations of wrongdoing; why have they not appointed, say, independent policy experts to investigate allegations of policy failure? Second, why did the Independent Counsel Statute fail? Briefly, the statute failed because it was too difficult to control the behavior of the prosecutor, who was not given any incentive to keep his investigation within reasonable bounds.89 Not surprisingly, policy investigators would be even less constrained since they would not be confined by the law, and at the same time, without legal powers they would probably be ignored on partisan grounds. A commission composed of members with diverse viewpoints is harder to ignore, if the members agree with each other.

More generally, the decision by presidents to bring into their administrations members of other parties, or persons with a reputation for bipartisanship and integrity, illustrates the formation of domestic coalitions of the willing. Presidents can informally bargain around the formal separation of powers90 by employing subsets of Congress, or of the opposing party, to generate credibility while maintaining a measure of institutional control. FDR was willing to appoint Knox and Stimson, but not to give the Republicans in Congress a veto. Truman was willing to ally with Arthur Vandenbergh but not with all the Republicans; Clinton was willing to appoint William Cohen but not Newt Gingrich. George W. Bush likewise made a gesture towards credibility by briefing members of the Senate Intelligence Committee – including Democrats – on the administration’s secret surveillance program(s), which provided a useful talking point when the existence of the program(s) was revealed to the public.

Counter-partisanship. Related to bipartisanship is what might be called counterpartisanship: presidents have greater credibility when they choose policies that cut against the grain of their party’s platform or their own presumed preferences.91 Only Nixon could go to China, and only Clinton could engineer welfare reform. Voters and publics rationally employ a political heuristic: the relevant policy, which voters are incapable of directly assessing, must be highly beneficial if it is chosen by a president who is predisposed against it by convictions or partisan loyalty.92 Accordingly, those who wish to move U.S. terrorism policy towards greater security and less liberty might do well to support the election of a Democrat.93 By the same logic, George W. Bush is widely suspected of nefarious motives when he rounds up alleged enemy combatants, but not when he creates a massive prescription drug benefit.

Counter-partisanship can powerfully enhance the president’s credibility, but it depends heavily on a lucky alignment of political stars. A peace-loving president has credibility when he declares a military emergency but not when he appeases; a belligerent president has credibility when he offers peace but not when he advocates military solutions. A lucky nation has a well-motivated president with a belligerent reputation when international tensions diminish (Ronald Reagan) and a president with a pacific reputation when they grow (Abraham Lincoln, who opposed the Mexican War). But a nation is not always lucky.

Transparency. The well-motivated executive might commit to transparency, as a way to reduce the costs to outsiders of monitoring his actions.94 The FDR strategy of inviting potential whistleblowers from the opposite party into government is a special case of this; the implicit threat is that the whistleblower will make public any evidence of partisan motivations. The more ambitious case involves actually exposing the executive’s decisionmaking processes to observation. To the extent that an ill-motivated executive cannot publicly acknowledge his motivations or publicly instruct subordinates to take them into account in decisionmaking, transparency will exclude those motivations from the decisionmaking process. The public will know that only a well-motivated executive would promise transparency in the first place, and the public can therefore draw an inference to credibility.

Credibility is especially enhanced when transparency is effected through journalists with reputations for integrity or with political preferences opposite to those of the president. Thus George W. Bush gave Bob Woodward unprecedented access to White House decisionmaking, and perhaps even to classified intelligence,95 with the expectation that the material would be published. This sort of disclosure to journalists is not real-time transparency – no one expects meetings of the National Security Council to appear on CSPAN – but the anticipation of future disclosure can have a disciplining effect in the present. By inviting this disciplining effect, the administration engages in signaling in the present through (the threat of) future transparency.

There are complex tradeoffs here, because transparency can have a range of harmful effects. As far as process is concerned, decisionmakers under public scrutiny may posture for the audience, may freeze their views or positions prematurely, and may hesitate to offer proposals or reasons for which they can later be blamed if things go wrong.96 As for substance, transparency can frustrate the achievement of programmatic or policy goals themselves. Where security policy is at stake, secrecy is sometimes necessary to surprise enemies or to keep them guessing. Finally, one must take account of the incentives of the actors who expose the facts—especially journalists who might reward presidents who give them access by portraying their decisionmaking in a favorable light.97

We will take up the costs of credibility shortly.98 In general, however, the existence of costs does not mean that the credibility-generating mechanisms are useless. Quite the contrary: where the executive uses such mechanisms, voters and legislators can draw an inference that the executive is well-motivated, precisely because the existence of costs would have given an ill-motivated executive an excuse not to use those mechanisms.

#### Public announcement is sufficient

Singer 13

[Singer, director – Center for 21st Century Security and Intelligence @ Brookings, and Wright, senior fellow – Brookings, 2/7/’13

(Peter W. and Thomas, "Obama, own your secret wars", www.nydailynews.com/opinion/obama-secret-wars-article-1.1265620])

It is time for a new approach. And **all that is required** of the President is to do the thing that he does perhaps best of all: to speak.

Obama has a unique opportunity — in fact, an urgent obligation — to create a new doctrine, unveiled in a major presidential speech, for the use and deployment of these new tools of war.

While the Republicans tried to paint the President as weak on security issues in the 2012 elections, history will record instead that his administration pushed into new frontiers of war, most especially in the new class of technologies that move the human role both geographically and chronologically further from the point of action on the battlefield.

The U.S. military’s unmanned systems, popularly known as “drones,” now number more than 8,000 in the air and 12,000 on the ground. And in a parallel development, the U.S. Cyber Command, which became operational in 2010, has added an array of new (and controversial) responsibilities — and is set to quintuple in size.

This is not just a military matter. American intelligence agencies are increasingly using these technologies as the tips of the spear in a series of so-called “shadow wars.” These include not only the more than 400 drone strikes that have taken place from Pakistan to Yemen, but also the deployment of the Stuxnet computer virus to sabotage Iranian nuclear development, the world’s first known use of a specially designed cyber weapon.

Throughout this period, the administration has tried to have it both ways — leaking out success stories of our growing use of these new technologies but not tying its hands with official statements and set policies.

This made great sense at first, when much of what was happening was ad hoc and being fleshed out as it went along.

But that position has become unsustainable. The less the U.S. government now says about our policies, the more that vacuum is becoming filled by others, in harmful ways.

By acting but barely explaining our actions, we’re creating precedents for other states to exploit. More than 75 countries now have military robotics programs, while another 20 have advanced cyber war capacities. Rest assured that nations like Iran, Russia and China will use these technologies in far more crude and indiscriminate ways — yet will do so while claiming to be merely following U.S. footsteps.

In turn, international organizations — the UN among them — are pushing ahead with special investigations into potential war crimes and proposing new treaties.

Our leaders, meanwhile, stay mum, which isolates the U.S. and drains its soft power.

The current policy also makes it harder to respond to growing concerns over civilian casualties. Indeed, Pew polling found 96% levels of opposition to U.S. drones in the key battleground state of Pakistan, a bellwether of the entire region. It is indisputable than many civilians have been harmed over the course of hundreds of strikes. And yet it is also indisputable that various groups have incentives to magnify such claims.

Yet so far, U.S. officials have painted themselves into a corner — either denying that any collateral losses have occurred, which no one believes, or reverting to the argument that we cannot confirm or deny our involvement, which no one believes, either.

Finally, the domestic support and legitimacy needed for the use of these weapons is in transition. Polling has found general public support for drone strikes, but only to a point, with growing numbers in the “not sure” category and growing worries around cases of targeting U.S. citizens abroad who are suspected of being terrorists.

The administration is so boxed in that, even when it recently won a court case to maintain the veil of semi-silence that surrounds the drone strike program, the judge described the current policy as having an “Alice in Wonderland” feel.

The White House seems to be finally starting to realize the problems caused by this disconnect of action but no explanation. After years of silence, occasional statements by senior aides are acknowledging the use of drones, while lesser-noticed working level documents have been created to formalize strike policies and even to explore what to do about the next, far more autonomous generation of weapons.

These efforts have been good starts, but they have been disjointed and partial. Most important, they are missing the **much-needed stamp of the President’s voice and authority**, which is essential to turn tentative first steps into established policy.

Much remains to be done — and said — out in the open.

This is why it’s time for Obama’s voice to ring loud and clear. Much as Presidents Harry Truman and Dwight Eisenhower were able keep secret aspects of the development of nuclear weapons, even as they articulated how and when we would use them, Obama should publicly lay out criteria by which the United States will develop, deploy and use these new weapons.

The President has a strong case to make — if only he would finally make it. After all, the new weapons have worked. They have offered new options for military action that are more accurate and proportionate and less risky than previously available methods.

But they have also posed many new complications. Explaining our position is about embracing both the good and the bad. It is about acknowledging the harms that come with war regardless of what technology is being used and making clear what structures of accountability are in place to respond.

It’s also about finally defining where America truly stands on some of the most controversial questions. These include the tactics of “signature” strikes, where the identity is not firmly identified, and “double tap” strikes, where rescuers aiding victims of a first attack are also brought under fire. These have been reported as occurring and yet seem to run counter to the principles under which the programs have been defended so far.

The role of the President is not to conduct some kind of retrospective of what we have done and why, but to lay out a course of the future. What are the key strategic goals and ethical guidelines that should drive the development and use of these new technologies? Is current U.S. and international law sufficient to cover them?

There are also crucial executive management questions, like where to draw the dividing line between military and civilian intelligence agency use of such technologies, and how to keep a growing range of covert actions from morphing into undeclared and undebated wars.

And, finally, the President must help resolve growing tensions between the executive branch and an increasingly restive Congress, including how to handle situations where we create the effect of war but no U.S. personnel are ever sent in harm’s way.

Given the sprawling complexity of these matters, only the President can deliver an official statement on where we stand. If only we somehow had a commander in chief who was simultaneously a law professor and Nobel Peace Prize winner!

The President’s voice on these issues won’t be a cure-all. But it will lay down a powerful marker, shaping not just the next four years but the actions of future administrations.

### AT: LX to Politics F/L

#### First, CP is executive action—obviously avoids Congressional fights

Fine 12

Jeffrey A. Fine, assistant professor of political science at Clemson University. He has published articles in the Journal of Politics, Political Research Quarterly, and Political Behavior. Adam L. Warber is an associate professor of political science at Clemson University. He is the author of Executive Orders and the Modern Presidency, Presidential Studies Quarterly, June 2012, " Circumventing Adversity: Executive Orders and Divided Government", Vol. 42, No. 2, Ebsco

We also should expect presidents to prioritize and be strategic in the types of executive orders that they create to maneuver around a hostile Congress. There are a variety of reasons that can drive a president’s decision. For example, presidents can use an executive order to move the status quo of a policy issue to a position that is closer to their ideal point. By doing so, presidents are able to pressure Congress to respond, perhaps by passing a new law that represents a compromise between the preferences of the president and Congress. Forcing Congress’s hand to enact legislation might be a preferred option for the president, if he perceives Congress to be unable or unwilling to pass meaningful legislation in the ﬁrst place. While it is possible that such unilateral actions might spur Congress to pass a law to modify or reverse a president’s order, such responses by Congress are rare (Howell 2003, 113-117; Warber 2006, 119). Enacting a major policy executive order allows the president to move the equilibrium toward his preferred outcome without having to spend time lining up votes or forming coalitions with legislators. As a result, and since reversal from Congress is unlikely, presidents have a greater incentive to issue major policy orders to overcome legislative hurdles.

#### Second, unilateral executive action shifts incentives for opposition to sway to the President’s will—diffuses tensions in congress, avoiding a fight and lowering PC cost.

Bernstein 2013

[Jonathan Bernstein is a political scientist who writes about American politics, especially the presidency, Congress, parties and elections., January 17th, 2013, In the Three Branches, Sharing is Caring, http://prospect.org/article/three-branches-sharing-caring, uwyo//amp]

Given all that, both sides really can have incentives to cut a deal in many cases. It takes a president who is willing to use all the tools of his office…but also one who is good at negotiating. It also, and this might be the biggest problem for Obama, requires an opposition which is willing to cut a deal for incremental gains, even if it allows the president to walk away a winner (albeit less of an immediate policy winner than he might have been acting alone). It’s not clear that House Republicans are willing to do that. Congressional Republicans might not look right now as if they could be real bargaining partners, but we don’t really know how it will play out. Presidents can never force Congress to act – they can’t even always force the bureaucracy to act. And there’s little that they can do to affect public opinion; in this case, it’s especially unlikely that Barack Obama can affect the views of those constituents House Republicans are most responsive to. What presidents can do is to act where they have the authority to do so, and there’s plenty that entails in gun safety, for climate, for immigration, and on many other issues. And by threatening to act, they can at least try to change the incentives for opposition Members of Congress, pushing them to see that legislative gridlock might not be their best option. Obama hasn’t done nearly as much as he could do so far, but perhaps his efforts on gun violence are a sign of things to come in his second term. If so, it might be a lot more productive than a lot of people expect. All in all, however, whether it’s gun violence, immigration, or even health care, the combination of executive orders and negotiation with Congress can be a potent tool for any president. Barack Obama hasn’t used it much, yet; he didn’t need it too often in his first two years, and he didn’t turn to it much once Republicans took the House. But I suspect it’s going to be a major weapon for him during his second term. At least, it certainly should be.

### AT: Backlash

#### CP causes Congressional follow-on but avoids politics

Brecher 12

(Aaron, JD Candidate, University of Michigan Law, "Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations," October,[http://www.michiganlawreview.org/assets/pdfs/111/3/Brecher.pdf-http://www.michiganlawreview.org/assets/pdfs/111/3/Brecher.pdf)](http://www.michiganlawreview.org/assets/pdfs/111/3/Brecher.pdf-http:/www.michiganlawreview.org/assets/pdfs/111/3/Brecher.pdf)) KH

Cyberattacks present a challenge for U.S. policymakers: they are difficult to locate within a clear legal category and there is a significant risk of uncontrollable consequences associated with their use. As a result, policymakers must choose a paradigm to govern their use that will ensure that the executive branch is held accountable and shares information with legislators.

This Part argues that the federal government should adopt the presumption that cyberattacks will be carried out under the covert action statute, and that the best way forward is for the president to issue an executive order making the covert action regime the presumptive framework for cyberattacks. It includes a brief discussion of why a president might willingly constrain her discretion by issuing the proposed executive order. It also shows that while the internal executive processes associated with both military and intelligence legal frameworks help mitigate the risk of cyberattacks'misuse by the executive, only the covert action regime provides an adequate role for Congress. Finally, this Part argues that the executive order option is preferable to one alternative proposed by scholars - enacting legislation - because of the practical difficulties of passing new legislation.

The covert action regime is the best approach for committing cyberattacks under the current law, as it would facilitate cooperation among executive agencies. The debate over which agency and set of legal authorities govern cyberattacks has caused no small amount of confusion. [n145](http://www.lexisnexis.com.libproxy.uwyo.edu/lnacui2api/frame.do?tokenKey=rsh-20.944040.9540913237&target=results_DocumentContent&returnToKey=20_T18237149325&parent=docview&rand=1380161350325&reloadEntirePage=true#n145) Apparently, an Office of Legal Counsel ("OLC") memorandum declined to decide which legal regime should govern the use of cyberattacks, and the uncertainty has led to interagency squabbles, as well as confusion over how cyberattacks are to be regulated. [n146](http://www.lexisnexis.com.libproxy.uwyo.edu/lnacui2api/frame.do?tokenKey=rsh-20.944040.9540913237&target=results_DocumentContent&returnToKey=20_T18237149325&parent=docview&rand=1380161350325&reloadEntirePage=true#n146) Establishing a presumptive answer would go far toward resolving this dispute.

Most importantly, adopting the covert action framework as the presumptive legal regime would be a principled way to help ensure constitutional legitimacy when the president orders a cyberattack.[n147](http://www.lexisnexis.com.libproxy.uwyo.edu/lnacui2api/frame.do?tokenKey=rsh-20.944040.9540913237&target=results_DocumentContent&returnToKey=20_T18237149325&parent=docview&rand=1380161350325&reloadEntirePage=true#n147) There is also reason to believe that presidential power is intimately bound up in credibility, which in turn is largely dependent on the perception of presidential compliance with applicable domestic law. [n148](http://www.lexisnexis.com.libproxy.uwyo.edu/lnacui2api/frame.do?tokenKey=rsh-20.944040.9540913237&target=results_DocumentContent&returnToKey=20_T18237149325&parent=docview&rand=1380161350325&reloadEntirePage=true#n148) A practice of complying with the covert action  [\*448]  regime for cyberattacks, both when they do not constitute a use of force and when it is unclear whether they do, is most likely to be in compliance with the law. Compliance with the covert action regime would also encourage covert action procedures in close cases without unduly restricting the executive's choice to use military authorities in appropriate circumstances.

The executive might also issue the proposed order, even though it would limit her freedom in some ways, because of the possible benefits of constraining future administrations or preempting legislative intervention. [n149](http://www.lexisnexis.com.libproxy.uwyo.edu/lnacui2api/frame.do?tokenKey=rsh-20.944040.9540913237&target=results_DocumentContent&returnToKey=20_T18237149325&parent=docview&rand=1380161350325&reloadEntirePage=true#n149) For example, in this context, an administration may choose to follow the finding and reporting requirements in order to convince Congress that legislative intervention is unnecessary for proper oversight. This is acceptable if the covert action regime is in fact adequate on its own. Moreover, if greater statutory control over cyberattacks is needed, the information shared with Congress may give Congress the tools and knowledge of the issue necessary to craft related legislation. [n150](http://www.lexisnexis.com.libproxy.uwyo.edu/lnacui2api/frame.do?tokenKey=rsh-20.944040.9540913237&target=results_DocumentContent&returnToKey=20_T18237149325&parent=docview&rand=1380161350325&reloadEntirePage=true#n150) Additionally, while executive orders are hardly binding, the inertia following adoption of an order may help constrain future administrations, which may be more or less trustworthy than the current one. Creating a presumption through an executive order also establishes a stable legal framework for cyberattacks that allows law to follow policy in this new field, and permits decisionmakers to learn more about the nature of cyberoperations before passing detailed statutes that may result in unintended consequences.

# 1NR

#### 2.] Obama fights the plan – strongly supports war powers

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

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

#### [3.] The plan expends capital on a separate war powers issue – it’s immediate and forces a trade-off in prioritization

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

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

#### Strikes cause global economic instability and Middle East war

The Iran Project, group of interested former officials of the US government and professionals in US national security, includes folks like Richard Armitage, Zbigniew Brezezinski, and Paul Volker, “Weighing the Benefits and Costs of Military Action Against Iran”, Wilson Center, 9/11/2012

III. Costs. In addition to the financial costs of conducting military attacks against Iran, which would be significant (particularly if the U.S. had to carry out thousands of sorties and if it had to return to the use of force periodically for years to come), there would likely be near-term costs associated with Iranian retaliation, through both direct and surrogate asymmetrical attacks. Serious costs to U.S. interests would also be felt over the longer term, we believe, with problematic consequences for global and regional stability, including economic stability. A dynamic of escalation, action, and counteraction could produce serious unintended consequences that would significantly increase all of these costs and lead, potentially, to all-out regional war.

#### Escalates and causes extinction

Jeffrey **Steinberg**, Will Bush 'October Surprise' Scam Trigger World War III?” EXECUTIVE INTELLIGENCE REVIEW, August 11, 20**06**. “http://www.larouchepub.com/other/2006/3332oct\_surprise\_war.html

On Jan. 11, 2006, keynoting an international webcast in Washington, D.C., Lyndon LaRouche issued a pointed warning about the danger of a new Mideast war. In his remarks, LaRouche spoke of a possible "fake weapons of mass destruction" hoax, orchestrated by Vice President Dick Cheney and former Israeli Prime Minister Benjamin Netanyahu. LaRouche warned: "We also have a situation in Israel, which is extremely tricky and dangerous, and it involves Bush, but most specifically Cheney, Vice President Cheney. As you know, Ariel Sharon is very seriously ill, is crippled, and will probably never again participate in a government in Israel. Whether he will live or not, is also in question, given his condition. Or whether he's able to function at all, if he lives, is in question. "The threat is, that a Benjamin Netanyahu, who is one of the ugliest characters on the Israeli scene, of any significance, is in discussion with the circles of Vice President Cheney. And Vice President Cheney would like to have an attack on Syria, by Netanyahu. And if the Israeli forces in this strike attack into Syria, were to occupy some territory, they would haul some evidence from the desert where the Israelis are holding it, which they created for this purpose, to try to "prove" that Saddam Hussein had had weapons of mass destruction, but had moved them into Syria. But this "evidence" would be moved into Syria by the Israelis from the Israeli desert, where it's being housed in preparation for this operation. "That's what's going on. "We could have the entire region of Southwest Asia, blow up. And a lot more soldiers being killed suddenly, because of this complication—[more] U.S. soldiers—than there have been so far. "This is a grim situation, in which virtual treason by the Vice President of the United States, who is a known liar, threatens civilization, and our civilization here in particular." Our Decision To Publish Now, in recent weeks, EIR specialists have received a series of new reports from qualified U.S. and Israeli sources, suggesting that a desperate Bush-Cheney White House is pushing a number of "October Surprise" schemes, all aimed at salvaging the November 2006 midterm U.S. House and Senate elections for the Republican Party—regardless of the fact that any one of these reckless schemes could trigger a planetary plunge into war.

### 2NC- Obama PC Key

#### [1.] Political capital is key and being spent on preventing Iran sanctions now – extend 1NC Dennis and Krushaar.

#### Obama is using his political capital to hold off strong democrat support for sanctions now and keep Reid from calling it to the floor – signals of weakness and damages to Obama political capital cause democrats to turn their back on Obama, triggers a vote and sanctions.

#### [2.] Obama pressure is key to making Reids pressure on the senate effective- it is so close that any negative pressure on Obama forces a vote

Kaper 1-16

(Stacy, writer for National Journal. “Iran Hawks Flounder Against Reid-Obama Coalition” 1-16-14 http://www.nationaljournal.com/daily/iran-hawks-flounder-against-reid-obama-coalition-20140116//wyoccd)

Senate Iran hawks have lots of votes to back their sanctions legislation. What they lack is a plan to get the bill to the floor.¶ Fifty-nine senators—including 16 Democrats—have signed onto sanctions legislation from Democratic Sen. Robert Menendez and Republican Sen. Mark Kirk. The measure would punish Iran with sanctions if it reneges on an interim nuclear agreement or if that agreement does not ultimately abolish any nuclear-weapons capabilities for Iran.¶ That count has climbed rapidly since the bipartisan pair introduced their legislation in late December. But now it's unclear whether that support will be enough to clear the bill's next major hurdle: Senate Majority Leader Harry Reid.¶ Reid is siding with the White House, which has put intense pressure on lawmakers not to act on sanctions, arguing it could result in both a nuclear-armed and hostile Iranian state. And without Reid's backing, supporters of the Menendez-Kirk bill are unsure how to move the measure to the floor.¶ "I assume that if the Democrat senators put enough pressure on Senator Reid he might bring it to the floor," said Missouri Republican Sen. Roy Blunt. "But, you know, we are at a moment in the Senate where nothing happens that Senator Reid doesn't want to happen; and this is something at this moment that Senator Reid doesn't want to happen."¶ And for now, sanctions supporters are still mulling their strategy.¶ "We are talking amongst ourselves. There is a very active debate and discussion ongoing about how best to move forward," said Democratic Sen. Richard Blumenthal of Connecticut, a cosponsor of the bill. "There are a number of alternative strategies, but we're deliberating them."¶ While Reid has, at least for now, foiled their policy plans, sanctions supporters are still scoring the desired political points on the issue. They can report their efforts to their constituents while blaming Reid for the inaction.¶ But whatever pressure Reid is getting from his colleagues, he's also getting support from the commander in chief.¶ In a White House meeting Wednesday night, President Obama made a hard sell to Democrats on the issue, pleading with them to back off sanctions while his team worked on a nuclear pact.¶ "The president did speak passionately about how [we] must seize this opportunity, that we need to seize this six months … and that if Iran isn't willing to in the end make the decisions necessary to make it work, he'll be ready to sign a bill to tighten those sanctions—but we gotta give this six months," said Sen. Jeff Merkley of Oregon, after returning from the White House.¶ In the meantime, many bill supporters reason that Reid will eventually feel the heat.¶ "We'll just have to ratchet up the pressure, that's all," said Republican Sen. John McCain. "The president is pushing back, obviously, and he's appealing to the loyalty of Democrats, but there are a lot of other forces out there that are pushing in the other direction, so we'll see how they react."¶ Earlier this week Sen. Lindsey Graham, R-S.C., said he was hoping to find more Democratic cosponsors over the recess and was talking to House Majority Leader Eric Cantor about whether the Republican-controlled House might take up the Senate sanctions bill as a way to spur the Senate to act. But neither of Graham's approaches represents a broad, coordinated campaign.¶ Democrats, who have more power to drive the train in the Senate, seem to be in little hurry.¶ "I don't think there is any time schedule related to it at this point," said Democratic cosponsor Ben Cardin of Maryland. "We are all trying to figure out how we can be most helpful and make sure Iran does not become a nuclear-weapon state."¶

### Case

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

**Libicki 9**

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

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

**Escalation is unlikely due to deterrence and international checks**

**Gartzke 12**

(Erik, Associate Professor in Political Science at UC-San Diego. “The Myth of Cyberwar” Page 23 12-7-12 http://dss.ucsd.edu/~egartzke/papers/cyberwar\_12062012.pdf//wyoccd)

**An open question exists in any crisis about how far competitors are willing to escalate, but an¶ ability to counter cyber attack with other, more kinetic forms of military violence serves alternately¶ to deter or to facilitate the use of cyber capabilities, giving those nations with terrestrial military¶ power yet another option that, even if available to their opponents, may prove extraordinarily¶ dangerous to practice**. **As we see today with U.S. drone attacks and special operations raids on¶ foreign sovereign territory, the power to do much more ensures that an opponent maintains a level¶ of discretion in its response to provocation**. Few can doubt the reaction of the United States, for¶ example, if **Pakistan were to attempt to conduct a commando raid on U.S. territory. Nations that¶ can physically punish others for transgressions in any domain, electronic or otherwise, are better¶ able to operate in all domains**. Once one distinguishes between simple vulnerability and actual¶ threats, terrestrial capabilities become pivotal in determining who exercises cyber capabilities.¶

**The impacts of a cyber attack would be small and temporary**

**Gartzke 12**

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

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

### AT: Scenario 3

**Weak Obama on cybersecurity emboldens Chinese cyber attacks**

**Davis 2013**

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

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

#### ] New study find cyber war highly unlikely

Oxford ‘11

[PhysOrg.com, “Cyber war unlikely: study” 1.17.2011. <http://phys.org/news/2011-01-cyber-war.html>//wyo-hdm]

The study, by Dr. Ian Brown of the Oxford Internet Institute (OII), University of Oxford, and Professor Peter Sommer of the London School of Economics also concludes that it is highly unlikely there will ever be a pure ‘cyber war’ fought solely in cyberspace with equivalent effects to recent wars in Afghanistan, the Balkans or the Middle East. The report, part of a wider OECD project on Future Global Shocks, is aimed at governments, global businesses and policy makers. It looks at the nature of global catastrophes and then asks which possible cyber-events might create similar effects. In addition to the actions of governments and terrorists the study also considers criminals and accidents. There is a review of current government action, an examination of how governments interact with the private sector and a consideration of the prospects for international cooperation and treaties. The best protections are careful system design, the use of products to detect known viruses and system intrusions, and user education, says the report. It adds that it is also essential to have proper contingency plans for system recovery. Dr. Brown commented: "We think that a largely military approach to cybersecurity is a mistake. Most targets in the critical national infrastructure of communications, energy, finance, food, government, health, transport, and water are in the private sector. Because it is often difficult to be certain who is attacking you from cyberspace, defence by deterrence does not work." "That said, cyberweaponry in all its forms will play a key role alongside more conventional and psychological attacks by nation states in future warfare." "We don’t help ourselves using “cyberwar” to describe espionage or hacktivist blockading or defacing of websites, as recently seen in reaction to WikiLeaks," said Professor Sommer, visiting professor at LSE. "Nor is it helpful to group trivially avoidable incidents like routine viruses and frauds with determined attempts to disrupt critical national infrastructure." The study says that many ‘cyber’ risks are real but that it is important to test each one to understand all the elements that are required before a potential threat causes real damage. How much research is required on the target, in writing computer code that won’t be detected, and how long will the event last before the attacked system is able to recover? It says this type of careful analysis helps us understand what we should really worry about and points the way to remedies. The study is part of a broader OECD review of Future Global Shocks which covers pandemics and further collapse of the world financial system. The UK Government has announced as part of its Strategic Defence and Security Review that £650m is available to address ‘cyber’ attacks, seen as a Tier One threat.

**[3] Defensive dominance prevents big attacks**

**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)

"Cyberweapons Can Create Massive Collateral Damage." **Very unlikely**. When news of Stuxnet broke, the New York Times reported that the most striking aspect of the new weapon was the "collateral damage" it created. The malicious program was "splattered on thousands of computer systems around the world, and much of its impact has been on those systems, rather than on what appears to have been its intended target, Iranian equipment," the Times reported. Such descriptions encouraged the view that computer viruses are akin to highly contagious biological viruses that, once unleashed from the lab, will turn against all vulnerable systems, not just their intended targets. But this metaphor is deeply flawed.**As the destructive potential of a cyberweapon grows, the likelihood that it could do far-reaching damage across many systems shrinks.**Stuxnet did infect more than 100,000 computers -- mainly in Iran, Indonesia, and India, though also in Europe and the United States. But it was so specifically programmed that it didn't actually damage those machines, afflicting only Iran's centrifuges at Natanz. The worm's aggressive infection strategy was designed to maximize the likelihood that it would reach its intended target. Because that final target was not networked, "all the functionality required to sabotage a system was embedded directly in the Stuxnet executable," the security software company Symantec observed in its analysis of the worm's code. So yes, Stuxnet was "splattered" far and wide, but it only executed its damaging payload where it was supposed to. Collateral infection, in short, **is not necessarily collateral damage**. A sophisticated piece of malware may aggressively infect many systems, but if there is an intended target, the infection will likely have a distinct payload that will be harmless to most computers. Especially in the context of more sophisticated cyberweapons, the image of inadvertent collateral damage doesn't hold up. They're more like a flu virus that only makes one family sick. "In Cyberspace, Offense Dominates Defense." **Wrong again**. The information age has "offense-dominant attributes," Arquilla and Ronfeldt wrote in their influential 1996 book, The Advent of Netwar. This view has spread through the American defense establishment like, well, a virus. A 2011 Pentagon report on cyberspace stressed "the advantage currently enjoyed by the offense in cyberwarfare." The intelligence community stressed the same point in its annual threat report to Congress last year, arguing that offensive tactics -- known as vulnerability discovery and exploitation -- are evolving more rapidly than the federal government and industry can adapt their defensive best practices. The conclusion seemed obvious: Cyberattackers have the advantage over cyberdefenders, "with the trend likely getting worse over the next five years." A closer examination of the record, however, reveals three factorsthat put the offense at a disadvantage. First is the **high cost** of developing a cyberweapon, in terms of time, talent, and target intelligence needed. Stuxnet, experts speculate, took a superb team and a lot of time. Second, the **potential for generic offensive weapons may be far smaller than assumed** for the same reasons, and significant investments in highly specific attack programs may be deployable only against a very limited target set. Third, once developed, an offensive tool is likely to have a far shorter half-life than the defensive measures put in place against it. Even worse, a weapon may only be able to strike a single time; once the exploits of a specialized piece of malware are discovered, the most critical systems will likely be patched and fixed quickly. And a weapon, even a potent one, is not much of a weapon if an attack cannot be repeated.**Any political threat relies on the credible threat to attack or to replicate a successful attack. If that were in doubt, the coercive power of a cyberattack would be drastically reduced**.

**[3] Their authors conflate threats**

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)

This increased focus on cyber-security has led to concern that **the perceived risk is greater than the actual risk**, a situation that has resulted in an imbalance between security and privacy and civil liberties (American Civil Liberties Union 2012). In 1993 a Rand Corporation paper predicted that “cyberwar is coming” and **twenty years later the prediction is the same** and critics argue that cyber-war is “more hype than hazard” (Rid 2012). A review of high profile cyberattacksshows that, with the exception of Stuxnet and the limited Israeli disruption of Syrian airdefense networks, **most cyber-attacks are**categorized as **information theft,** network compromise, **or website defacement**(Lewis 2012). Even the high profile threat of an “Electronic Pearl Harbor” (Bronk 2009), despite being repeated by senior government officials like U.S. Defense Secretary Leon Panetta (Rid 2012) , has been found to be **only aslight possibility**(Wilson 2005). There is no doubt that cyber-security is important. Businesses recognize this importance and spent more than $80 billion on computer network security in 2011 (Johnson 2012) and the federal government is expected to be spending $10.5 billion per year by 2015 (Brito and Watkins 2012). This response is appropriate when data shows that the vast majority of cyber-attacks arefocused on espionage and the theft of intellectual property. It is not clear why **senior governmentofficials**and corporate executives **focus on high-impact low-probability events and engage in “alarmist rhetoric**” (Brito and Watkins 2011) that skews the public perception of risk and createsan atmosphere of fear. The danger of an inappropriate response in reaction to an inflated threat and prevalence of misinformation is exemplified by the politicized intelligence that led to the invasion of Iraq in 2003 (Brito and Watkins 2011). Understanding how information on the risk posed by cyber-attacks is poorly communicated and the public reaction to an increased perception of risk – fear – is important in identifying when the perceived risk is greater than the actual risk; when risk is more hype than threat. Critics of current cyber-security policy believe that **threats are being conflated**; thisresults in a threat appearing larger than it is (Brito and Watkins 2012). In essence, a wide variety of cyber-activity – political and social activity, criminal activity for profit, espionage, and offensive cyber-attack – are treated as presenting the same level of threat. There is a wide dividebetween easily mounted and easily defended denial of service attacks on public websites andhigh-potential cyber-weapons capable of severely disrupting or destroying critical infrastructure(Rid and McBurney 2012). The rise of automated tools that allow for low-level cyber-attacks to be easily mounted has caused a significant increase in the number of cyber-attacks, **a statisticoften cited as proof of increased risk**,**but qualified cyber**-security **organizations have discarded the number of cyber-attacks as a metric and consider it to be meaningless** as a method of assessing the scope and effects of cyber-attacks (Wilson 2005). Without differentiatingbetween generic malicious software and highly specialized and targeted offensive cyber-attacks, the risk of cyber-attacks on critical infrastructure systems like the electrical grid **cannot be properly assessed.**

### 2NC Strikes Bad – Middle East War

#### Strikes cause global economic instability and Middle East war

The Iran Project, group of interested former officials of the US government and professionals in US national security, includes folks like Richard Armitage, Zbigniew Brezezinski, and Paul Volker, “Weighing the Benefits and Costs of Military Action Against Iran”, Wilson Center, 9/11/2012

III. Costs. In addition to the financial costs of conducting military attacks against Iran, which would be significant (particularly if the U.S. had to carry out thousands of sorties and if it had to return to the use of force periodically for years to come), there would likely be near-term costs associated with Iranian retaliation, through both direct and surrogate asymmetrical attacks. Serious costs to U.S. interests would also be felt over the longer term, we believe, with problematic consequences for global and regional stability, including economic stability. A dynamic of escalation, action, and counteraction could produce serious unintended consequences that would significantly increase all of these costs and lead, potentially, to all-out regional war.

#### Escalates and causes extinction

Jeffrey **Steinberg**, Will Bush 'October Surprise' Scam Trigger World War III?” EXECUTIVE INTELLIGENCE REVIEW, August 11, 20**06**. “http://www.larouchepub.com/other/2006/3332oct\_surprise\_war.html

On Jan. 11, 2006, keynoting an international webcast in Washington, D.C., Lyndon LaRouche issued a pointed warning about the danger of a new Mideast war. In his remarks, LaRouche spoke of a possible "fake weapons of mass destruction" hoax, orchestrated by Vice President Dick Cheney and former Israeli Prime Minister Benjamin Netanyahu. LaRouche warned: "We also have a situation in Israel, which is extremely tricky and dangerous, and it involves Bush, but most specifically Cheney, Vice President Cheney. As you know, Ariel Sharon is very seriously ill, is crippled, and will probably never again participate in a government in Israel. Whether he will live or not, is also in question, given his condition. Or whether he's able to function at all, if he lives, is in question. "The threat is, that a Benjamin Netanyahu, who is one of the ugliest characters on the Israeli scene, of any significance, is in discussion with the circles of Vice President Cheney. And Vice President Cheney would like to have an attack on Syria, by Netanyahu. And if the Israeli forces in this strike attack into Syria, were to occupy some territory, they would haul some evidence from the desert where the Israelis are holding it, which they created for this purpose, to try to "prove" that Saddam Hussein had had weapons of mass destruction, but had moved them into Syria. But this "evidence" would be moved into Syria by the Israelis from the Israeli desert, where it's being housed in preparation for this operation. "That's what's going on. "We could have the entire region of Southwest Asia, blow up. And a lot more soldiers being killed suddenly, because of this complication—[more] U.S. soldiers—than there have been so far. "This is a grim situation, in which virtual treason by the Vice President of the United States, who is a known liar, threatens civilization, and our civilization here in particular." Our Decision To Publish Now, in recent weeks, EIR specialists have received a series of new reports from qualified U.S. and Israeli sources, suggesting that a desperate Bush-Cheney White House is pushing a number of "October Surprise" schemes, all aimed at salvaging the November 2006 midterm U.S. House and Senate elections for the Republican Party—regardless of the fact that any one of these reckless schemes could trigger a planetary plunge into war.

#### t’s case 1. Obama would turn our weapons on launch

2. Israeli strike induces China Russia draw-in from your 1AC

AP 2012

[Associated Press, January 23, 2012, EU adopts Iran oil embargo; China, Russia worried over US war threats, <http://timesofindia.indiatimes.com/world/europe/EU-adopts-Iran-oil-embargo-China-Russia-worried-over-US-war-threats/articleshow/11602863.cms>, uwyo//amp]

A leading state-run Chinese daily warned on Monday that Moscow and Beijing were seriously concerned over US attempts to go to war with Iran, IANS reported from Beijing. After Iraq and Afghanistan, the US "is preparing for a potential confrontation with Iran, and appears confident of another successful air strike. "Such a demonstration of armed might makes powers like Russia and China increasingly nervous," the commentary in the English language Global Times said. It said that "mainstream forces in Washington are trying to sell a ludicrous standpoint to the American people: that it is worthwhile to bear financial costs and even lose some lives to confront lurking dangers to US security in the Middle East. "This is not a rational analysis, but rather a pious belief in US politics. With an appetite for national security causes, the US becomes increasingly meticulous in eliminating potential challenges." The daily, which reflects the thinking in Chinese leadership, warned that by stirring up other powers' sense of insecurity, the US was actually undermining its own interests. "If the West slides into a war with Iran, the damages will not be any lower than the potential threat of Iran's nuclear power. "Perhaps the US is used to resorting to war to solve geopolitical problems," it said. "Many worry that such a mentality will sooner or later lead to a US clash with Russia and China." For Beijing and Moscow alike, it said, relations with the US had been stressful. In both countries, an increasing number of people now advocate a Moscow-Beijing alliance, Global Times said. "The two do have countermeasures against the US, and they are capable of deterring US allies," it added. "If they are really determined to join hands, the balance of power on many world issues will begin to shift."

#### We control time frame and magnitude – deal failure draws in global powers and goes nuclear within months

PressTV 11/13

Global nuclear conflict between US, Russia, China likely if Iran talks fail, 11/13/13,<http://www.presstv.ir/detail/2013/11/13/334544/global-nuclear-war-likely-if-iran-talks-fail/>

A global conflict between the US, Russia, and China is likely in the coming months should the world powers fail to reach a nuclear deal with Iran, an American analyst says.¶ “If the talks fail, if the agreements being pursued are not successfully carried forward and implemented, then there would be enormous international pressure to drive towards a conflict with Iran before [US President Barack] Obama leaves office and that’s a very great danger that no one can underestimate the importance of,” senior editor at the Executive Intelligence Review Jeff Steinberg told Press TV on Wednesday. ¶ “The United States could find itself on one side and Russia and China on the other and those are the kinds of conditions that can lead to miscalculation and general roar,” Steinberg said. ¶ “So the danger in this situation is that if these talks don’t go forward, we could be facing a global conflict in the coming months and years and that’s got to be avoided at all costs when you’ve got countries like the United States, Russia, and China with” their arsenals of “nuclear weapons,” he warned.

T

#### [a.] Obama not pushing

Laura Litvan, Bloomberg, “Senate Republicans Say Obama’s Silence Risks Trade Agenda”

1/16, 2014. http://www.bloomberg.com/news/2014-01-16/senate-republicans-say-obama-s-silence-risks-trade-agenda.html

Obama hasn’t publicly pressed Congress to act since a July 30 speech called for the authority. Others in the administration, including U.S. Trade Representative Michael Froman and Commerce Secretary Penny Pritzker, have been more engaged. White House Press Secretary Jay Carney yesterday said the bipartisan proposal is “welcome,” without endorsing it.

#### [b.] No vote

Michael **McAuliff**, Huff Post, **1/14**, "Harry Reid: Fast Track Free Trade Bill Goes Nowhere ," www.huffingtonpost.com/2014/01/14/harry-reid-fast-track\_n\_4598486.html

WASHINGTON -- The fast track trade bill introduced in the Senate last week will go **nowhere anytime soon**, Senate Majority Leader Harry Reid (D-Nev.) said Tuesday.

Sen. Max Baucus (D-Mont.), chair of the Senate Finance Committee and President Barack Obama's pick to be his next ambassador to China, offered the legislation last week, surprising many of his colleagues.

Baucus' bill, which would reauthorize 2002's Trade Promotional Authority, would essentially give the White House the power to present Congress with trade agreements that lawmakers could not amend. The fast track bill would ease the way for the controversial Trans-Pacific Partnership, a 12-nation trade deal that opponents contend would undermine labor, environmental and other protections.

But if those opponents were worried the fast-track measure might advance, Reid was emphatic in saying **it would** **not** -- at least for now.

Asked if he told Baucus that Reid would make time on the floor of the U.S. Senate to debate the measure, **Reid said "No," four times.**

"There's a lot of controversy on that, and I'm going to see how that plays out with my caucus and the Senate.," Reid told reporters on Capitol Hill.

Indeed, many Democrats are so unhappy with the current draft of the Trans-Pacific Partnership, they are willing to kill it **even though it is a key element of Obama's ambitious pivot toward Asia**.

#### [5.] Even if deal isn’t reached – it sets up another short term deal that can pave the way to continued progress through sticking points

Pace and Klapper 1-24

(Julie and Bradley, writer for the Associated Press. “US Eyes Difficulties in Next Round of Iran Talks” 1-24-14 http://abcnews.go.com/Politics/wireStory/us-eyes-difficulties-round-iran-talks-21642771//wyoccd)

For the United States and its negotiating partners, the next round of nuclear talks with Iran could present a difficult decision: to sign another temporary agreement or accept nothing less than an ambitious, multiyear accord to dismantle the Islamic republic's nuclear program.¶

#### **Senate Democratic leadership moving away from sanctions – Murray, Reid, Durbin, and Warrent**

Johnson 1-22

(Luke Johnson, staff writer for the Huffington Post “Patty Murray Comes Out Against Iran Sanctions Bill” 1-22-14 http://www.huffingtonpost.com/2014/01/22/iran-sanctions-bill-democrats\_n\_4646614.html//wyoccd)

Sen. Patty Murray (D-Wash.), a member of the Senate leadership, came out Wednesday against passing a bill to slap more sanctions on Iran during an interim six-month nuclear deal between that country and the world powers. "I believe the Administration should be given time to negotiate a strong verifiable comprehensive agreement," Murray said in a letter to her constituents. "However, if Iran does not agree to a comprehensive agreement that is acceptable, or if Iran does not abide by the terms of the interim agreement, I will work with my colleagues to swiftly enact sanctions in order to increase pressure on the Iranian regime." The Washington Post first obtained the letter, and Murray's office shared the missive with The Huffington Post but offered no additional comment. Murray's position is similar to that of President Barack Obama, who opposes further sanctions during the interim agreement -- to which the United States is party -- but has stated his willingness to pass them if the deal does not work out. Murray's public opposition to passing additional sanctions signals that the Senate Democratic leadership is moving away from the bill. Senate Majority Leader Harry Reid (D-Nev.) has delayed holding a vote on the bill, which has 43 Republican and 15 Democratic co-sponsors. On the other hand, Sen. Chuck Schumer (D-N.Y.), the chamber's third-ranking Democrat, is a co-sponsor. Senate Majority Whip Dick Durbin (D-Ill.) does not have an official position on the bill but has joined with Reid in opposing bringing it to the floor and backs giving diplomatic efforts more time. Wednesday's letter also suggests a shift in Murray's thinking. In October, she signed a saber-rattling letter -- along with such Iran hawks as Sens. Robert Menendez (D-N.J.), Lindsey Graham (R-S.C.) and John McCain (R-Ariz.) -- warning the president that "we are prepared to move forward with new sanctions to increase pressure on the government in Tehran."¶ The Post reported that Sen. Elizabeth Warren (D-Mass.) has likewise sent a letter to constituents opposing the bill. Warren had already voiced skepticism about the idea of adding more sanctions at a Dec. 13 hearing and has favored the interim deal.

#### Momentum has flipped – Obama’s pressure has significantly reduced the chances of new sanctions on Iran.

-Proves PC key – white house pressure is best explanation of change in momentum

Benen 1-17

(Steve, reporter for MSNBC. “Support for new Iran sanctions wanes” 1-17-14 http://www.msnbc.com/rachel-maddow-show/support-new-iran-sanctions-wanes//wyoccd)

As recently as last week, bipartisan congressional support for new sanctions on Iran, which were likely to sabotage diplomatic talks and move the world closer to a national security crisis, was growing, and momentum appeared to be on proponents’ side. As of this morning, the landscape looks far different.¶ Its Senate sponsors describe it as a “diplomatic insurance policy” that will help President Obama cut a better nuclear deal with Iran. The White House condemns it as a deal-killer that could put the United States on a path to war.¶ ¶ At issue is a 52-page Senate bill, the Nuclear Weapon Free Iran Act of 2013, which has become enshrouded in a fog of overheated talk, as the White House, Congress and a growing legion of lobbyists clash over the wisdom of passing new sanctions against Iran while pursuing diplomacy.¶ Iranian officials, who were brought to the negotiating table in the first place thanks to the efficacy of existing sanctions, have already said they’ll abandon diplomatic talks if the United States approves additional sanctions while negotiations are underway. In effect, Congress would be scuttling a historic opportunity, on purpose, without waiting to see whether diplomacy would work.¶ ¶ But the problems with the effort go even further. The proposed sanctions would also signal to the world that the United States is no longer interested in a peaceful solution and similarly disinterested in keeping our word. At the same time, the legislation represents a congressional effort to establish the parameters of any possible long-term deal with Iran – in effect, lawmakers would be imposing their own requirements on U.S. negotiators while talks are ongoing.¶ ¶ A week ago, it was practically a foregone conclusion that such a bill would pass the House and Senate; the question is whether President Obama’s veto could be overridden. Just of the last few days, however, the odds of such a bill even reaching the president’s desk have dropped unexpectedly.¶ ¶ The Hill, for example, reported yesterday that House Republicans “are moving away from a proposal to adopt new Iran sanctions.” House Democrats who were otherwise sympathetic to the idea became “irked” by GOP political tactics “and the idea appears to have been at least temporarily shelved.”¶ ¶ In the Senate, meanwhile, BuzzFeed reports that Sen. Bob Corker (R-Tenn.), a co-sponsor of the legislation, has “proposed the idea of scheduling a vote on Iran sanctions six months from now, after the interim nuclear agreement has run its course, instead of voting on sanctions right now.”¶ ¶ In other words, lawmakers could at least wait to see if the talks bear fruit before sabotaging them in advance. Corker’s idea isn’t ideal – it would reportedly lock in the Senate for a vote on July 21, exactly six months after the current deal is implemented, regardless of the status of the diplomacy – but in the larger context it suggests even sanctions supporters are starting to see value in waiting.¶ ¶ Indeed, an unnamed senator who supports the sanctions bill told Greg Sargent this week that opponents have the momentum. The senator added, “At the moment, there’s no rush to put the bill on the floor. I’m not aware of any deadline in anyone’s head.”¶ ¶ Keep in mind, the sanctions legislation was introduced in the Senate on Dec. 19 with a bipartisan group of 26 sponsors. Over the course of just three weeks, that total more than doubled to 59 sponsors. But the last addition was eight days ago – and no other senators have signed on since.¶ ¶ What changed the direction of the debate? To be sure, White House pressure has made a difference, reinforced by President Obama’s direct lobbying to Democratic senators this week. I also talked to a Senate staffer yesterday who said public pressure has also increased, with more voters contacting the Hill with phone calls and emails, voicing opposition to the bill.

#### .] Losers lose link – plan is a perceived loss for Obama that saps his capital

Loomis, 7 --- Department of Government at Georgetown

(3/2/2007, Dr. Andrew J. Loomis is a Visiting Fellow at the Center for a New American Security, “Leveraging legitimacy in the crafting of U.S. foreign policy,” pg 35-36, <http://citation.allacademic.com//meta/p_mla_apa_research_citation/1/7/9/4/8/pages179487/p179487-36.php>)

Declining political authority encourages defection. American political analyst Norman Ornstein writes of the domestic context, ¶ In a system where a President has limited formal power, perception matters. The reputation for success—the belief by other political actors that even when he looks down, a president will find a way to pull out a victory—is the most valuable resource a chief executive can have. Conversely, the widespread belief that the Oval Office occupant is on the defensive, on the wane or without the ability to win under adversity can lead to disaster, as individual lawmakers calculate who will be on the winning side and negotiate accordingly. In simple terms, winners win and losers lose more often than not. ¶ Failure begets failure. In short, a president experiencing declining amounts of political capital has diminished capacity to advance his goals. As a result, political allies perceive a decreasing benefit in publicly tying themselves to the president, and an increasing benefit in allying with rising centers of authority. A president’s incapacity and his record of success are interlocked and reinforce each other. Incapacity leads to political failure, which reinforces perceptions of incapacity. This feedback loop accelerates decay both in leadership capacity and defection by key allies. ¶ The central point of this review of the presidential literature is that the sources of presidential influence—and thus their prospects for enjoying success in pursuing preferred foreign policies—go beyond the structural factors imbued by the Constitution. Presidential authority is affected by ideational resources in the form of public perceptions of legitimacy. The public offers and rescinds its support in accordance with normative trends and historical patterns, non-material sources of power that affects the character of U.S. policy, foreign and domestic.¶ This brief review of the literature suggests how legitimacy norms enhance presidential influence in ways that structural powers cannot explain. Correspondingly, increased executive power improves the prospects for policy success. As a variety of cases indicate—from Woodrow Wilson’s failure to generate domestic support for the League of Nations to public pressure that is changing the current course of U.S. involvement in Iraq—the effective execution of foreign policy depends on public support. Public support turns on perceptions of policy legitimacy. As a result, policymakers—starting with the president—pay close attention to the receptivity that U.S. policy has with the domestic public. In this way, normative influences infiltrate policy-making processes and affect the character of policy decisions.¶ **Political capital is finite --- the plan would tradeoff with domestic economic priorities** ¶ **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.**

#### [3.] Presidential flexibility link - Independent of the political capital debate plan undermines negotiations with Iran because it sends signal that congress is taking greater foreign policy authority - Obama’s perceived flexibility is key to ensure diplomatic success.

**Benen**, writer for MSNBC and producer of the Rachel Maddow show, **9/20**/2013

(Steve, “When crises become opportunities,” http://maddowblog.msnbc.com/\_news/2013/09/20/20599445-when-crises-become-opportunities?lite)

When it comes to the Middle East, progress has never moved in a straight line. There are fits and starts, ebbs and flows. There are heartening breakthroughs and crushing disappointments, occasionally at the same time.¶ That said, while the domestic political establishment's attention seems focused elsewhere, there's reason to believe new opportunities are materializing in the region in ways that were **hard to even imagine up until very recently**.¶ This morning, for example, the Organization for the Prohibition of Chemical Weapons (OPCW) announced that Syria has taken its first steps towards detailing its stockpiles. Michael Luhan, a spokesperson for the Hague-based chemical weapons regulator, said in a statement, "The OPCW has received an initial disclosure from the Syrian Government of its chemical weapons programme, which is now being examined by the Technical Secretariat of the Organisation."¶ Meanwhile, Iranian President Hasan Rouhani has a new op-ed in the Washington Post arguing that the United States and the rest of the world "must work together to end the unhealthy rivalries and interferences that fuel violence and drive us apart" through a policy of "constructive engagement."¶ The New York Times added that **Iranian leaders**, "**seizing on perceived flexibility** in a private letter **from** President **Obama**, **have decided to gamble on** forging **a swift agreement over their nuclear program with the goal of ending crippling sanctions**."¶ David Sanger summarized the bigger picture nicely.¶ Only two weeks after Washington and the nation were debating a unilateral military strike on Syria that was also intended as a forceful warning to Iran about its nuclear program, President Obama finds himself at the opening stages of two unexpected diplomatic initiatives with America's biggest adversaries in the Middle East, each fraught with opportunity and danger.¶ Without much warning, diplomacy is suddenly alive again after a decade of debilitating war in the region. After years of increasing tension with Iran, there is talk of finding a way for it to maintain a face-saving capacity to produce a very limited amount of nuclear fuel while allaying fears in the United States and Israel that it could race for a bomb.¶ The surprising progress has come so suddenly that a senior American diplomat described this week's developments as "head spinning."¶ So what happens next?¶ The consensus among many foreign policy observers is that developments in Syria and Iran are linked in ways that may or may not be helpful to the United States. Max Fisher explained well yesterday that President **Obama's pragmatism** "**has sent exactly the right signals to Iran**, particularly **at this** very **sensitive moment**."¶ Obama has been consistently clear, even if some members of his administration were not, that his big overriding goal is for Syrian leader Bashar al-Assad to stop using chemical weapons. First he was going to do that with strikes, meant to coerce Assad. Then, in response to the Russian proposal, Obama signaled he would back off the strikes if Assad gave up his chemical weapons, which is exactly what Obama has always said he wants. **He's been consistent as well as flexible**, **which gave Assad big incentives to cooperate** when he might have otherwise dug in his heels.¶ There are some awfully significant -- and promising -- parallels here with the U.S. standoff with Iran. Obama has been clear that he wants Iran to give up its rogue uranium-enrichment program and submit to the kind of rigorous inspections that would guarantee that its nuclear program is peaceful. **He's** also **been clear that the U**nited **S**tates is using severe economic sanctions to coerce Tehran to cooperate and that it **would use military force if necessary**. The implicit (and sometimes explicit) message to Iran has been: If you abandon your enrichment program, we'll make it worth your while by easing off.¶ Here's where the parallel with Syria is really important: Iranian leaders distrust the United States deeply and fear that Obama would betray them by not holding up his end of the bargain. That's been a major hurdle to any U.S.-Iran nuclear deal. But seeing Assad's deal with Obama work out (so far) sends the message to Iran that it can trust the United States. It also sends the message that making concessions to the United States can pay off. **Iran's supreme leader has been talking a lot lately about** flexibility and **diplomacy toward the West**. **So it's an ideal moment for Obama to be demonstrating flexibility** and diplomacy toward the Middle East.

#### OCO causes contentious debates in congress-last year proves

Munoz 12

(Carlo, Staff Writer - Defense/Nat'l Security at The Hill. “Obama authorizes new cyber warfare directive” 11-4-12 http://thehill.com/blogs/defcon-hill/policy-and-strategy/267879-report-obama-authorizes-new-cyber-warfare-directive//wyoccd)

The White House has, for the first time, laid out specific ground rules for how and when the U.S. military can carry out offensive and defensive cyber operations against foreign threats. ¶ The guidelines were codified in a new White House directive signed by President Obama in mid-October, according to the The Washington Post. A senior Obama administration official confirmed to The Hill that the president has signed a directive on “cyber operations.”¶ “This step is part of the administration’s focus on cybersecurity as a top priority. The cyber threat has evolved since 2004, and we have new experiences to take into account,” the official said.¶ The senior administration official stressed that the directive does not create new powers for federal agencies or the military. ¶ “The directive establishes principles and processes for the use of cyber operations so that cyber tools are integrated with the fully array of national security tools we have at our disposal,” the official said. “It provides a whole-of-government approach consistent with the values that we promote domestically and internationally as we have previously articulated in the International Strategy for Cyberspace.”¶ The cyber rules of engagement, known inside the White House and Pentagon as Presidential Policy Directive 20, is the latest step by the administration to take the fight to state and non-state actors looking to attack U.S. government and civilian networks. ¶ The new directive also closes a critical policy gap at the DOD on cyber warfare that Congress failed to close earlier this year. ¶ In August, White House chief counterterrorism adviser John Brennan told reporters that the administration was considering exercising presidential authority to impose cybersecurity mandates after lawmakers failed to adopt legislation to implement those measures. ¶ Passing cybersecurity legislation was near the top of Defense Secretary Leon Panetta's legislative to-do list for Congress in the lame-duck session, behind a sequestration deal and approval of a Defense authorization bill. ¶ A cybersecurity bill co-sponsored by Sens. Joe Lieberman (I-Conn.) and Susan Collins (R-Maine) has remained stalled on Capitol Hill for months. ¶ Senate Majority Leader Harry Reid (D-Nev.) has called for a vote on the legislation in November, but observers are not optimistic that a final product will reach the president's desk, given ongoing partisan fighting over the legislation. ¶

#### President has to spend political capital defending war powers

Samples, 1 --- director of the Center for Representative Government at CATO

(10/27/2011, John, “Congress Surrenders the War Powers: Libya, the United Nations, and the Constitution,” <http://www.cato.org/sites/cato.org/files/pubs/pdf/pa687.pdf>))

But political representation has other fac-ets. It has given voice to public dissatisfaction about wars proper and limited wars. Con-gress “has historically been actively engaged in debates over the proper conduct of major military initiatives. It has proposed, publicly debated, and voted on various legislative initiatives to authorize or curtail the use of force.” Congress has also held hearings about the conduct of limited and proper wars. 215 Many believe that such legislative actions have little effect on the president. Yet such ac-tions can affect the cost-benefit calculations of the president in pursuing or failing to pur-sue a limited war. Congress can raise the costs of a policy by shaping and mobilizing public opinion against a war, thereby increasing the cost in political capital a president must pay to sustain a policy. Congressional actions also signal disunity (or unity) to foreign actors, who in turn act on their expectations, thereby raising the costs of a limited war. Congres-sional actions also affect presidential expec-tations about how the conduct of a war will be received in the legislature; Congress can thus influence presidential policies without directly overturning them. 216 Systematic evi-dence indicates that since 1945 Congress has been able to influence presidential policies through these means. 217 Although short of constitutional propriety, congressional voice can matter in war-making.

#### OCO operations led by the president are popular in congress-they find it consistent with his powers

Greenwald and MacAskill 13

(Glenn Greenwald is an American political commentator, lawyer, columnist, blogger, and author. Ewen, Guardian reporter. Former Washington bureau chief, diplomatic editor and chief political reporter. “Obama orders US to draw up overseas target list for cyber-attacks” 6-7-13 http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas//wyoccd)

One such bill currently pending in Congress, the Cyber Intelligence Sharing and Protection Act (Cispa), has prompted serious concerns from privacy groups, who say that it would further erode online privacy while doing little to enhance cyber security.¶ In a statement, Caitlin Hayden, national security council spokeswoman, said: "We have not seen the document the Guardian has obtained, as they did not share it with us. However, as we have already publicly acknowledged, last year the president signed a classified presidential directive relating to cyber operations, updating a similar directive dating back to 2004. This step is part of the administration's focus on cybersecurity as a top priority. The cyber threat has evolved, and we have new experiences to take into account.¶ "This directive establishes principles and processes for the use of cyber operations so that cyber tools are integrated with the full array of national security tools we have at our disposal. It provides a whole-of-government approach consistent with the values that we promote domestically and internationally as we have previously articulated in the International Strategy for Cyberspace.¶ "This directive will establish principles and processes that can enable more effective planning, development, and use of our capabilities. It enables us to be flexible, while also exercising restraint in dealing with the threats we face. It continues to be our policy that we shall undertake the least action necessary to mitigate threats and that we will prioritize network defense and law enforcement as the preferred courses of action. The procedures outlined in this directive are consistent with the US Constitution, including the president's role as commander in chief, and other applicable law and policies."

#### 2.] Obama fights the plan – strongly supports war powers

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

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

#### [3.] The plan expends capital on a separate war powers issue – it’s immediate and forces a trade-off in prioritization

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

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

#### Strikes cause global economic instability and Middle East war

The Iran Project, group of interested former officials of the US government and professionals in US national security, includes folks like Richard Armitage, Zbigniew Brezezinski, and Paul Volker, “Weighing the Benefits and Costs of Military Action Against Iran”, Wilson Center, 9/11/2012

III. Costs. In addition to the financial costs of conducting military attacks against Iran, which would be significant (particularly if the U.S. had to carry out thousands of sorties and if it had to return to the use of force periodically for years to come), there would likely be near-term costs associated with Iranian retaliation, through both direct and surrogate asymmetrical attacks. Serious costs to U.S. interests would also be felt over the longer term, we believe, with problematic consequences for global and regional stability, including economic stability. A dynamic of escalation, action, and counteraction could produce serious unintended consequences that would significantly increase all of these costs and lead, potentially, to all-out regional war.

#### Escalates and causes extinction

Jeffrey **Steinberg**, Will Bush 'October Surprise' Scam Trigger World War III?” EXECUTIVE INTELLIGENCE REVIEW, August 11, 20**06**. “http://www.larouchepub.com/other/2006/3332oct\_surprise\_war.html

On Jan. 11, 2006, keynoting an international webcast in Washington, D.C., Lyndon LaRouche issued a pointed warning about the danger of a new Mideast war. In his remarks, LaRouche spoke of a possible "fake weapons of mass destruction" hoax, orchestrated by Vice President Dick Cheney and former Israeli Prime Minister Benjamin Netanyahu. LaRouche warned: "We also have a situation in Israel, which is extremely tricky and dangerous, and it involves Bush, but most specifically Cheney, Vice President Cheney. As you know, Ariel Sharon is very seriously ill, is crippled, and will probably never again participate in a government in Israel. Whether he will live or not, is also in question, given his condition. Or whether he's able to function at all, if he lives, is in question. "The threat is, that a Benjamin Netanyahu, who is one of the ugliest characters on the Israeli scene, of any significance, is in discussion with the circles of Vice President Cheney. And Vice President Cheney would like to have an attack on Syria, by Netanyahu. And if the Israeli forces in this strike attack into Syria, were to occupy some territory, they would haul some evidence from the desert where the Israelis are holding it, which they created for this purpose, to try to "prove" that Saddam Hussein had had weapons of mass destruction, but had moved them into Syria. But this "evidence" would be moved into Syria by the Israelis from the Israeli desert, where it's being housed in preparation for this operation. "That's what's going on. "We could have the entire region of Southwest Asia, blow up. And a lot more soldiers being killed suddenly, because of this complication—[more] U.S. soldiers—than there have been so far. "This is a grim situation, in which virtual treason by the Vice President of the United States, who is a known liar, threatens civilization, and our civilization here in particular." Our Decision To Publish Now, in recent weeks, EIR specialists have received a series of new reports from qualified U.S. and Israeli sources, suggesting that a desperate Bush-Cheney White House is pushing a number of "October Surprise" schemes, all aimed at salvaging the November 2006 midterm U.S. House and Senate elections for the Republican Party—regardless of the fact that any one of these reckless schemes could trigger a planetary plunge into war.

#### [2.] Obama pressure is key to making Reids pressure on the senate effective- it is so close that any negative pressure on Obama forces a vote

Kaper 1-16

(Stacy, writer for National Journal. “Iran Hawks Flounder Against Reid-Obama Coalition” 1-16-14 http://www.nationaljournal.com/daily/iran-hawks-flounder-against-reid-obama-coalition-20140116//wyoccd)

Senate Iran hawks have lots of votes to back their sanctions legislation. What they lack is a plan to get the bill to the floor.¶ Fifty-nine senators—including 16 Democrats—have signed onto sanctions legislation from Democratic Sen. Robert Menendez and Republican Sen. Mark Kirk. The measure would punish Iran with sanctions if it reneges on an interim nuclear agreement or if that agreement does not ultimately abolish any nuclear-weapons capabilities for Iran.¶ That count has climbed rapidly since the bipartisan pair introduced their legislation in late December. But now it's unclear whether that support will be enough to clear the bill's next major hurdle: Senate Majority Leader Harry Reid.¶ Reid is siding with the White House, which has put intense pressure on lawmakers not to act on sanctions, arguing it could result in both a nuclear-armed and hostile Iranian state. And without Reid's backing, supporters of the Menendez-Kirk bill are unsure how to move the measure to the floor.¶ "I assume that if the Democrat senators put enough pressure on Senator Reid he might bring it to the floor," said Missouri Republican Sen. Roy Blunt. "But, you know, we are at a moment in the Senate where nothing happens that Senator Reid doesn't want to happen; and this is something at this moment that Senator Reid doesn't want to happen."¶ And for now, sanctions supporters are still mulling their strategy.¶ "We are talking amongst ourselves. There is a very active debate and discussion ongoing about how best to move forward," said Democratic Sen. Richard Blumenthal of Connecticut, a cosponsor of the bill. "There are a number of alternative strategies, but we're deliberating them."¶ While Reid has, at least for now, foiled their policy plans, sanctions supporters are still scoring the desired political points on the issue. They can report their efforts to their constituents while blaming Reid for the inaction.¶ But whatever pressure Reid is getting from his colleagues, he's also getting support from the commander in chief.¶ In a White House meeting Wednesday night, President Obama made a hard sell to Democrats on the issue, pleading with them to back off sanctions while his team worked on a nuclear pact.¶ "The president did speak passionately about how [we] must seize this opportunity, that we need to seize this six months … and that if Iran isn't willing to in the end make the decisions necessary to make it work, he'll be ready to sign a bill to tighten those sanctions—but we gotta give this six months," said Sen. Jeff Merkley of Oregon, after returning from the White House.¶ In the meantime, many bill supporters reason that Reid will eventually feel the heat.¶ "We'll just have to ratchet up the pressure, that's all," said Republican Sen. John McCain. "The president is pushing back, obviously, and he's appealing to the loyalty of Democrats, but there are a lot of other forces out there that are pushing in the other direction, so we'll see how they react."¶ Earlier this week Sen. Lindsey Graham, R-S.C., said he was hoping to find more Democratic cosponsors over the recess and was talking to House Majority Leader Eric Cantor about whether the Republican-controlled House might take up the Senate sanctions bill as a way to spur the Senate to act. But neither of Graham's approaches represents a broad, coordinated campaign.¶ Democrats, who have more power to drive the train in the Senate, seem to be in little hurry.¶ "I don't think there is any time schedule related to it at this point," said Democratic cosponsor Ben Cardin of Maryland. "We are all trying to figure out how we can be most helpful and make sure Iran does not become a nuclear-weapon state."¶

### Case

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

**Libicki 9**

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

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

**Escalation is unlikely due to deterrence and international checks**

**Gartzke 12**

(Erik, Associate Professor in Political Science at UC-San Diego. “The Myth of Cyberwar” Page 23 12-7-12 http://dss.ucsd.edu/~egartzke/papers/cyberwar\_12062012.pdf//wyoccd)

**An open question exists in any crisis about how far competitors are willing to escalate, but an¶ ability to counter cyber attack with other, more kinetic forms of military violence serves alternately¶ to deter or to facilitate the use of cyber capabilities, giving those nations with terrestrial military¶ power yet another option that, even if available to their opponents, may prove extraordinarily¶ dangerous to practice**. **As we see today with U.S. drone attacks and special operations raids on¶ foreign sovereign territory, the power to do much more ensures that an opponent maintains a level¶ of discretion in its response to provocation**. Few can doubt the reaction of the United States, for¶ example, if **Pakistan were to attempt to conduct a commando raid on U.S. territory. Nations that¶ can physically punish others for transgressions in any domain, electronic or otherwise, are better¶ able to operate in all domains**. Once one distinguishes between simple vulnerability and actual¶ threats, terrestrial capabilities become pivotal in determining who exercises cyber capabilities.¶

**The impacts of a cyber attack would be small and temporary**

**Gartzke 12**

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

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

### AT: Scenario 3

**Weak Obama on cybersecurity emboldens Chinese cyber attacks**

**Davis 2013**

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

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

#### ] New study find cyber war highly unlikely

Oxford ‘11

[PhysOrg.com, “Cyber war unlikely: study” 1.17.2011. <http://phys.org/news/2011-01-cyber-war.html>//wyo-hdm]

The study, by Dr. Ian Brown of the Oxford Internet Institute (OII), University of Oxford, and Professor Peter Sommer of the London School of Economics also concludes that it is highly unlikely there will ever be a pure ‘cyber war’ fought solely in cyberspace with equivalent effects to recent wars in Afghanistan, the Balkans or the Middle East. The report, part of a wider OECD project on Future Global Shocks, is aimed at governments, global businesses and policy makers. It looks at the nature of global catastrophes and then asks which possible cyber-events might create similar effects. In addition to the actions of governments and terrorists the study also considers criminals and accidents. There is a review of current government action, an examination of how governments interact with the private sector and a consideration of the prospects for international cooperation and treaties. The best protections are careful system design, the use of products to detect known viruses and system intrusions, and user education, says the report. It adds that it is also essential to have proper contingency plans for system recovery. Dr. Brown commented: "We think that a largely military approach to cybersecurity is a mistake. Most targets in the critical national infrastructure of communications, energy, finance, food, government, health, transport, and water are in the private sector. Because it is often difficult to be certain who is attacking you from cyberspace, defence by deterrence does not work." "That said, cyberweaponry in all its forms will play a key role alongside more conventional and psychological attacks by nation states in future warfare." "We don’t help ourselves using “cyberwar” to describe espionage or hacktivist blockading or defacing of websites, as recently seen in reaction to WikiLeaks," said Professor Sommer, visiting professor at LSE. "Nor is it helpful to group trivially avoidable incidents like routine viruses and frauds with determined attempts to disrupt critical national infrastructure." The study says that many ‘cyber’ risks are real but that it is important to test each one to understand all the elements that are required before a potential threat causes real damage. How much research is required on the target, in writing computer code that won’t be detected, and how long will the event last before the attacked system is able to recover? It says this type of careful analysis helps us understand what we should really worry about and points the way to remedies. The study is part of a broader OECD review of Future Global Shocks which covers pandemics and further collapse of the world financial system. The UK Government has announced as part of its Strategic Defence and Security Review that £650m is available to address ‘cyber’ attacks, seen as a Tier One threat.

**[3] Defensive dominance prevents big attacks**

**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)

"Cyberweapons Can Create Massive Collateral Damage." **Very unlikely**. When news of Stuxnet broke, the New York Times reported that the most striking aspect of the new weapon was the "collateral damage" it created. The malicious program was "splattered on thousands of computer systems around the world, and much of its impact has been on those systems, rather than on what appears to have been its intended target, Iranian equipment," the Times reported. Such descriptions encouraged the view that computer viruses are akin to highly contagious biological viruses that, once unleashed from the lab, will turn against all vulnerable systems, not just their intended targets. But this metaphor is deeply flawed.**As the destructive potential of a cyberweapon grows, the likelihood that it could do far-reaching damage across many systems shrinks.**Stuxnet did infect more than 100,000 computers -- mainly in Iran, Indonesia, and India, though also in Europe and the United States. But it was so specifically programmed that it didn't actually damage those machines, afflicting only Iran's centrifuges at Natanz. The worm's aggressive infection strategy was designed to maximize the likelihood that it would reach its intended target. Because that final target was not networked, "all the functionality required to sabotage a system was embedded directly in the Stuxnet executable," the security software company Symantec observed in its analysis of the worm's code. So yes, Stuxnet was "splattered" far and wide, but it only executed its damaging payload where it was supposed to. Collateral infection, in short, **is not necessarily collateral damage**. A sophisticated piece of malware may aggressively infect many systems, but if there is an intended target, the infection will likely have a distinct payload that will be harmless to most computers. Especially in the context of more sophisticated cyberweapons, the image of inadvertent collateral damage doesn't hold up. They're more like a flu virus that only makes one family sick. "In Cyberspace, Offense Dominates Defense." **Wrong again**. The information age has "offense-dominant attributes," Arquilla and Ronfeldt wrote in their influential 1996 book, The Advent of Netwar. This view has spread through the American defense establishment like, well, a virus. A 2011 Pentagon report on cyberspace stressed "the advantage currently enjoyed by the offense in cyberwarfare." The intelligence community stressed the same point in its annual threat report to Congress last year, arguing that offensive tactics -- known as vulnerability discovery and exploitation -- are evolving more rapidly than the federal government and industry can adapt their defensive best practices. The conclusion seemed obvious: Cyberattackers have the advantage over cyberdefenders, "with the trend likely getting worse over the next five years." A closer examination of the record, however, reveals three factorsthat put the offense at a disadvantage. First is the **high cost** of developing a cyberweapon, in terms of time, talent, and target intelligence needed. Stuxnet, experts speculate, took a superb team and a lot of time. Second, the **potential for generic offensive weapons may be far smaller than assumed** for the same reasons, and significant investments in highly specific attack programs may be deployable only against a very limited target set. Third, once developed, an offensive tool is likely to have a far shorter half-life than the defensive measures put in place against it. Even worse, a weapon may only be able to strike a single time; once the exploits of a specialized piece of malware are discovered, the most critical systems will likely be patched and fixed quickly. And a weapon, even a potent one, is not much of a weapon if an attack cannot be repeated.**Any political threat relies on the credible threat to attack or to replicate a successful attack. If that were in doubt, the coercive power of a cyberattack would be drastically reduced**.

**[3] Their authors conflate threats**

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)

This increased focus on cyber-security has led to concern that **the perceived risk is greater than the actual risk**, a situation that has resulted in an imbalance between security and privacy and civil liberties (American Civil Liberties Union 2012). In 1993 a Rand Corporation paper predicted that “cyberwar is coming” and **twenty years later the prediction is the same** and critics argue that cyber-war is “more hype than hazard” (Rid 2012). A review of high profile cyberattacksshows that, with the exception of Stuxnet and the limited Israeli disruption of Syrian airdefense networks, **most cyber-attacks are**categorized as **information theft,** network compromise, **or website defacement**(Lewis 2012). Even the high profile threat of an “Electronic Pearl Harbor” (Bronk 2009), despite being repeated by senior government officials like U.S. Defense Secretary Leon Panetta (Rid 2012) , has been found to be **only aslight possibility**(Wilson 2005). There is no doubt that cyber-security is important. Businesses recognize this importance and spent more than $80 billion on computer network security in 2011 (Johnson 2012) and the federal government is expected to be spending $10.5 billion per year by 2015 (Brito and Watkins 2012). This response is appropriate when data shows that the vast majority of cyber-attacks arefocused on espionage and the theft of intellectual property. It is not clear why **senior governmentofficials**and corporate executives **focus on high-impact low-probability events and engage in “alarmist rhetoric**” (Brito and Watkins 2011) that skews the public perception of risk and createsan atmosphere of fear. The danger of an inappropriate response in reaction to an inflated threat and prevalence of misinformation is exemplified by the politicized intelligence that led to the invasion of Iraq in 2003 (Brito and Watkins 2011). Understanding how information on the risk posed by cyber-attacks is poorly communicated and the public reaction to an increased perception of risk – fear – is important in identifying when the perceived risk is greater than the actual risk; when risk is more hype than threat. Critics of current cyber-security policy believe that **threats are being conflated**; thisresults in a threat appearing larger than it is (Brito and Watkins 2012). In essence, a wide variety of cyber-activity – political and social activity, criminal activity for profit, espionage, and offensive cyber-attack – are treated as presenting the same level of threat. There is a wide dividebetween easily mounted and easily defended denial of service attacks on public websites andhigh-potential cyber-weapons capable of severely disrupting or destroying critical infrastructure(Rid and McBurney 2012). The rise of automated tools that allow for low-level cyber-attacks to be easily mounted has caused a significant increase in the number of cyber-attacks, **a statisticoften cited as proof of increased risk**,**but qualified cyber**-security **organizations have discarded the number of cyber-attacks as a metric and consider it to be meaningless** as a method of assessing the scope and effects of cyber-attacks (Wilson 2005). Without differentiatingbetween generic malicious software and highly specialized and targeted offensive cyber-attacks, the risk of cyber-attacks on critical infrastructure systems like the electrical grid **cannot be properly assessed.**