### 1NC

#### A. Interpretation – Restriction requires prohibition

Northglenn 11

(City of Northglenn Zoning Ordinance, “Rules of Construction – Definitions”, http://www.northglenn.org/municode/ch11/content\_11-5.html)

Section 11-5-3. Restrictions. As used in this Chapter 11 of the Municipal Code, the term "restriction" shall mean a prohibitive regulation. Any use, activity, operation, building, structure or thing which is the subject of a restriction is prohibited, and no such use, activity, operation, building, structure or thing shall be authorized by any permit or license.

####  “In the area” means all of the activities

United Nations 13

(United Nations Law of the Sea Treaty, http://www.un.org/depts/los/convention\_agreements/texts/unclos/part1.htm)

PART I¶ INTRODUCTION¶ Article 1

Use of terms and scope¶ 1. For the purposes of this Convention:¶ (1) "Area" means the seabed and ocean floor and subsoil thereof, beyond the limits of national jurisdiction;¶ (2) "Authority" means the International Seabed Authority;¶ (3) "activities in the Area" means all activities of exploration for, and exploitation of, the resources of the Area;

#### Violation: affirmative restricts, doesn’t prohibit

#### B. Standards:

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

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

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

### 2nd Off

#### Plan: The President of the United States should issue an executive order to adopt the presumption that cyberattacks will be carried out under the covert action statute.  The President of the United States should issue a declaratory policy stating that the United States will not authorize the preemptive use of large-scale cyber-attacks, except in direct support of authorized United States military operations. The President of the United States should adhere to these mandates.

#### Making the covert action regime the presumptive framework for cyberattacks restricts presidential authority, facilitates agency cooperation and oversight, and ensures constitutional legitimacy of future attacks

Brecher 12

(Aaron, – J.D. candidate @ University of Michigan and#34;NOTE: Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperationsand#34; 111 Mich. L. Rev. 423 (December)) 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.

#### Declaratory policy solves.

Singer and Wright 13

director of the 21st Century Defense Initiative @ Brookings and fellow @ Managing Global Order project.
Peter W. and Thomas, and#34;Obama, own your secret warsand#34; ~<http://www.nydailynews.com/opinion/obama-secret-wars-article-1.1265620~~>February 17

Irony pervades [President Obama](http://www.nydailynews.com/topics/Barack%2BObama)’s place in foreign policy today. He won the Nobel Peace Prize for his efforts to roll back the nuclear bomb, the signature weapon of the 20th century, but he has also broken new ground in the use of revolutionary military technologies — from the armed drone to cyber weaponry — that may well become the signature weapons of the 21st century.

As the controversy continues about secret drone strikes and leaked legal documents, Obama promised in his State of the Union address last week to work with Congress to make the drone program, now shrouded in secret, more transparent.¶ But the problem is that a tipping point has already been reached, and it’s not just a matter of playing nice with Congress. A veil of official semi-silence surrounds these new technologies, the policy that guides them and their growing use in what can only be described as not-so-covert operations. When crucial information does come out, it’s most often through leaks to the press.¶ 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.

### 3rd Off

#### Squo use of OCO’s has created a deterrent effect.

Limnell ‘13

[Jarno Limnéll, Director of Cyber Security in Stonesoft Corporation, “Offensive Cyber Capabilities are

Needed Because of Deterrence,” National Defense University Department of Leadership and Military Pedagogy, Series 2, Article Collection 10, 2013, <http://www.doria.fi/bitstream/handle/10024/88689/The%20Fog%20of%20Cyber%20Defence%20NDU%202013.pdf?sequence=1> // wyo-ch]

The nation states are “forced” to conduct cyber attacks in real situations and against real targets. This will mean attacks against terrorist or activist groups, industrial plants, or even against other states. After conducting attacks, the nation states will claim the responsibility in order to increase their cyber deterrence. As an example, in May 2012 the US Secretary of State Hillary Clinton announced that the agency’s specialists attacked sites related to Al Qaeda on which the organisation tried to recruit new members.10 This was a strong political message of intent to use cyber weapons. It was a glimpse into the future of cyberwarfare – and it served to build credible deterrence.

#### 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.

#### Unrestrained use deters cyber war – legal norms increase risk of conflict by reducing fear.

Crosston 12 (Dr. Matthew Crosston is the Miller Endowed Chair for Industrial and International Security and founder and director of the International Security and Intelligence Studies (ISIS) program at Bellevue University. He has authored two books, several book chapters, and nearly a dozen peer-reviewed articles on counterterrorism, corruption, democratization, radical Islam, and cyber deterrence, “Virtual Patriots and a New American Cyber Strategy” Winter 2012, Strategic Studies Quarterly, p. 100-118)

These proposed behavioral rules about jus in cyber bello are paradoxical: with so many constraints on allowable action, the underlying motivational framework of fear—so essential in the original Cold War in moderating behavior—becomes nonexistent. Indeed, if the above parameters were observed, then a state could arguably be more motivated to attack. Remove the civilian population and domestic infrastructure from cyber attack, and you have sanitized cyber war to a point where there is no fear of engagement. A Cyber Cold War would be multilateral rather than bilateral: it would involve many nations, with different interests and not allied by treaty. Furthermore, the parties would include major non-governmental players such as private compa nies or even individuals or groups of individual hackers, perhaps with political interests. It is unlikely, in the more capitalistic and constitutionally free countries, which national governments can easily rein in these potential corporate and indi vidual cyber attackers. 20 The problem with this formulation is that it envisions a so-called cyber cold war beholden to apparently voluntary parameters of constraint. The parameters elaborated, however, do not honor but corrupt the true deterring force that existed in the Cold War. If an overt strategy of credible cyber debilitation were allowed to openly develop, then most of the problems mentioned above would be inconsequential to the proper functioning of the virtual global commons—multilateral or bilateral, individuals or groups, national governments or private corporations, clearly defined adversaries or anonymous, nonattributable attacks. A system that does not rely on arbitrary good behavior and instead proactively establishes overt cyber-weaponization strategies alongside continued covert capabili ties creates an environment where the futility of first-strike efficacy and perceived retaliatory devastation reigns in behavior globally. The United States tends to be obsessive about keeping its technological capabilities classified. This is partially explained by the need to maintain effective surprise in retaliation to an attack rather than striving to prevent an attack initially. Yet, it is also explained by the US attempt to be the leading voice for liberally idealistic global cyber norms. This was confirmed in 2008 when former intelligence official Suzanne Spaulding testified before the House Cybersecurity Subcommittee. My concern is that (the Department of Defense) has been so vocal about the development and deployment of [classified] cyber-warfare capabilities that it will be very difficult for that department to develop and sustain the trust necessary to undertake essential collaboration on defensive cybersecurity efforts with the private sector and with international stakeholders. . . . There is significant risk that these vital partners will suspect that the collaboration is really aimed at strengthening our offensive arsenal (emphasis added). 21 There are two problems with the above quote. On the one hand, policymakers continue to focus on apparent voluntary trust in a domain that is not typified by such behavior. On the other hand, the DoD remains stead fast in its worship of clandestine capability and thus loses the preemptive deterrence of overt strategy which can compel cooperation as opposed to just hoping for it. These are not small problems, as trust and collaboration between dangerous actors work when there is an element of consequence to poor action. An overt strategy of offensive cyber capability—revealing some cards while not revealing all, with no nod to ethical considerations that demand targeting constraints and a focus purely on the efficacy of preemptive deterrence—arguably has a chance to shine a light of consequence into the shadowy anarchy of cyber. This is how the United States, as men tioned at the beginning of this article, could be inspired by the essence of Chinese cyber strategy, but it must ultimately elevate to a higher capability and competence. Further hindering this evolution, the academic community has re mained too enamored with trying to connect ethical theories into the cyber domain to create a liberal, idealistic governing code. Many scholars have acknowledged that these theories, whether utilitarianism, Kantian theory, or natural rights theory, have cast relatively little new light into the cyber domain. 22 Despite such sincere if misguided efforts, the best possibility for preemptive cyber deterrence might be old-school strategic realism and not new-school ethical liberalism. As awkward as it may be to admit publicly, the Chinese might have something for the United States to truly consider. A fusion of Sun Tzu’s pragmatism with Machiavelli’s overt strategic amorality carries the potential to deter negative cyber action before it ever begins. As Sun Tzu as serted, the highest realization of warfare is to attack the enemy’s plans; next is to attack its alliances; next to attack the army; and the lowest is to attack its fortified cities. Machiavelli made it clear that if an injury has to be done to a man, it should be so severe that his vengeance need not be feared. This overt, amoral offensive fusion has one purpose: not to logistically conduct war but to strategically avoid it. At the present time there is no current discussion of US cyber strategy broaching these subjects, and subsequently, the zero-sum cyber game remains unchanged.

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

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

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

**An unchecked North Korea causes global catastrophe (Green highlighting)**

**Hayes and Green, 10**

[\*Victoria University AND Executive Director of the Nautilus Institute (Peter and Michael, “-“The Path Not Taken, the Way Still Open: Denuclearizing the Korean Peninsula and Northeast Asia”, 1/5, http://www.nautilus.org/fora/security/10001HayesHamalGreen.pdf) uwyo//amp]

**The consequences of failing to address the proliferation threat posed by the North Korea developments, and related political and economic issues, are serious, not only for the Northeast Asian region but for the whole international community. At worst, there is the possibility of nuclear attack1, whether by intention, miscalculation, or merely accident, leading to the resumption of Korean War hostilities.** On the Korean Peninsula itself, **key population centres are well within short or medium range missiles.** **The whole of Japan is likely to come within North Korean missile range**. Pyongyang has a population of over 2 million, Seoul (close to the North Korean border) 11 million, and Tokyo over 20 million. **Even a limited nuclear exchange would result in a holocaust of unprecedented proportions. But the catastrophe within the region would not be the only outcome. New research indicates that even a limited nuclear war in the region would rearrange our global climate far more quickly than global warming.** Westberg draws attention to new studies modelling the effects of even a limited nuclear exchange involving approximately 100 Hiroshima-sized 15 kt bombs2 (by comparison it should be noted that the United States currently deploys warheads in the range 100 to 477 kt, that is, individual warheads equivalent in yield to a range of 6 to 32 Hiroshimas).The studies indicate that **the soot from the fires produced would lead to a decrease in global temperature by 1.25 degrees Celsius for a period of 6-8 years**.3 In Westberg’s view: **That is not global winter, but the nuclear darkness will cause a deeper drop in temperature than at any time during the last 1000 years.** The temperature over the continents would decrease substantially more than the global average. **A decrease in rainfall over the continents would also follow…The period of nuclear darkness will cause much greater decrease in grain production than 5% and it will continue for many years...hundreds of millions of people will die from hunger…To make matters even worse, such amounts of smoke injected into the stratosphere would cause a huge reduction in the Earth’s protective ozone.4** These, of course, are not the only consequences. **Reactors might also be targeted, causing further mayhem and downwind radiation effects, superimposed on a smoking, radiating ruin left by nuclear next-use.** Millions of refugees would flee the affected regions. **The direct impacts, and the follow-on impacts on the global economy via ecological and food insecurity, could make the present global financial crisis pale by comparison. How the great powers, especially the nuclear weapons states respond to such a crisis, and in particular, whether nuclear weapons are used in response to nuclear first-use, could make or break the global non proliferation and disarmament regimes. There could be many unanticipated impacts on regional and global security relationships5, with subsequent nuclear breakout and geopolitical turbulence, including possible loss-of-control over fissile material or warheads in the chaos of nuclear war, and aftermath chain-reaction affects involving other potential proliferant states.** The Korean nuclear proliferation issue is not just a regional threat but a global one that warrants priority consideration from the international community.

### 4th Off

#### Executive war power primacy now—the plan flips that

Posner 13

[Eric Posner, 9/3/13, Obama Is Only Making His War Powers Mightier, www.slate.com/articles/news\_and\_politics/view\_from\_chicago/2013/09/obama\_going\_to\_congress\_on\_syria\_he\_s\_actually\_strengthening\_the\_war\_powers.html]

President Obama’s surprise announcement that he will ask Congress for approval of a military attack on Syria is being hailed as a vindication of the rule of law and a revival of the central role of Congress in war-making, even by critics. But all of this is wrong. Far from breaking new legal ground, President **Obama has reaffirmed the primacy of the executive** in matters of war and peace. **The war powers of the presidency remain as mighty as ever**.¶ It would have been different if the president had announced that **only Congress can authorize** the use of military force, as dictated by the Constitution, which gives Congress alone the power to declare war. **That would have been** worthy of notice, **a reversal of the ascendance of executive power over Congress**. **But the president said no such thing**. He said: “I believe I have the authority to carry out this military action without specific congressional authorization.” Secretary of State John Kerry confirmed that the president “has the right to do that”—launch a military strike—“no matter what Congress does.”¶ Thus, the president believes that the law gives him the option to seek a congressional yes or to act on his own. He does not believe that he is bound to do the first. He has merely stated the law as countless other presidents and their lawyers have described it before him.¶ The president’s announcement should be understood as a political move, not a legal one. His motive is both self-serving and easy to understand, and it has been all but acknowledged by the administration. If Congress now approves the war, it must share blame with the president if what happens next in Syria goes badly. If Congress rejects the war, it must share blame with the president if Bashar al-Assad gases more Syrian children. The big problem for Obama arises if Congress says no and he decides he must go ahead anyway, and then the war goes badly. He won’t have broken the law as he understands it, but he will look bad. He would be the first president ever to ask Congress for the power to make war and then to go to war after Congress said no. (In the past, presidents who expected dissent did not ask Congress for permission.)¶ People who celebrate the president for humbly begging Congress for approval also apparently don’t realize that his understanding of the law—that it gives him the option to go to Congress—maximizes executive power vis-à-vis Congress. If the president were required to act alone, without Congress, then he would have to take the blame for failing to use force when he should and using force when he shouldn’t. If he were required to obtain congressional authorization, then Congress would be able to block him. But if he can have it either way, he can force Congress to share responsibility when he wants to and avoid it when he knows that it will stand in his way.¶

#### Congressional restraints spill over to destabilize all presidential war powers.

Heder ’10

(Adam, J.D., magna cum laude , J. Reuben Clark Law School, Brigham Young University, “THE POWER TO END WAR: THE EXTENT AND LIMITS OF CONGRESSIONAL POWER,” St. Mary’s Law Journal Vol. 41 No. 3, <http://www.stmaryslawjournal.org/pdfs/Hederreadytogo.pdf>)

This constitutional silence invokes Justice Rehnquist’s oftquoted language from the landmark “political question” case, Goldwater v. Carter . 121 In Goldwater , a group of senators challenged President Carter’s termination, without Senate approval, of the United States ’ Mutual Defense Treaty with Taiwan. 122 A plurality of the Court held, 123 in an opinion authored by Justice Rehnquist, that this was a nonjusticiable political question. 124 He wrote: “In light of the absence of any constitutional provision governing the termination of a treaty, . . . the instant case in my view also ‘must surely be controlled by political standards.’” 125 Notably, Justice Rehnquist relied on the fact that there was no constitutional provision on point. Likewise, there is **no constitutional provision** on whether Congress has the legislative power to **limit, end, or otherwise redefine the scope of a war**. Though Justice Powell argues in Goldwater that the Treaty Clause and Article VI of the Constitution “add support to the view that the text of the Constitution does not unquestionably commit the power to terminate treaties to the President alone,” 126 **the same cannot be said about Congress’s legislative authority** to terminate or **limit a war** in a way that goes beyond its explicitly enumerated powers. There are no such similar provisions that would suggest Congress may decline to exercise its appropriation power but nonetheless legally order the President to cease all military operations. Thus, the case for deference to the political branches on this issue is even greater than it was in the Goldwater context. Finally, the Constitution does not imply any additional powers for Congress to end, limit, or redefine a war. The textual and historical evidence suggests the Framers purposefully **declined to grant Congress such powers**. And as this Article argues, granting Congress this power would be **inconsistent with the general war powers structure of the Constitution.** Such a reading of the Constitution would **unnecessarily empower Congress** and **tilt the scales heavily in its favor**. More over, it **would strip the President of his Commander in Chief authority** to direct the movement of troops at a time **when the Executive’s expertise is needed.** 127 And fears that the President will grow too powerful are unfounded, given the reasons noted above. 128 In short, the Constitution does not impliedly afford Congress any authority to prematurely terminate a war above what it explicitly grants. 129 Declaring these issues nonjusticiable political questions would be the most practical means of balancing the textual and historical demands, the structural demands, and the practical demands that complex modern warfare brings . Adjudicating these matters would only lead the courts to engage in impermissible line drawing — lines that would both confus e the issue and add layers to the text of the Constitution in an area where the Framers themselves declined to give such guidance.

#### That goes nuclear

Li ‘9

[Zheyao, J.D. candidate, Georgetown University Law Center, 2009; B.A., political science and history, Yale University, 2006. This paper is the culmination of work begun in the "Constitutional Interpretation in the Legislative and Executive Branches" seminar, led by Judge Brett Kavanaugh, “War Powers for the Fourth Generation: Constitutional Interpretation in the Age of Asymmetric Warfare,” 7 Geo. J.L. & Pub. Pol'y 373 2009 WAR POWERS IN THE FOURTH GENERATION OF WARFARE

1. The Emergence of Non-State Actors]

Even as the quantity of nation-states in the world has increased dramatically since the end of World War II, the **institution** of the nation-state has been in decline over the past few decades. Much of this decline is the direct result of the waning of major interstate war, which primarily resulted from the introduction of nuclear weapons.122 The proliferation of nuclear weapons, and their immense capacity for absolute destruction, has ensured that **conventional wars** remain limited in scope and duration. Hence, "both the size of the armed forces and the quantity of weapons at their disposal has declined quite sharply" since 1945.123 At the same time, concurrent with the decline of the nation-state in the second half of the twentieth century, non-state actors have increasingly been willing and able to use force to advance their causes. In contrast to nation-states, who adhere to the Clausewitzian distinction between the ends of policy and the means of war to achieve those ends, non-state actors do not necessarily fight as a mere means of advancing any coherent policy. Rather, they see their fight **as a life-and-death struggle**, wherein the ordinary terminology of war as an instrument of policy breaks down because of this blending of means and ends.124 It is the existential nature of this struggle and the disappearance of the Clausewitzian distinction between war and policy that has given rise to a new generation of warfare. The concept of fourth-generational warfare was first articulated in an influential article in the Marine Corps Gazette in 1989, which has proven highly prescient. In describing what they saw as the modem trend toward a new phase of warfighting, the authors argued that: In broad terms, fourth generation warfare seems likely to be widely dispersed and largely undefined; the distinction between war and peace will be blurred to the vanishing point. It will be nonlinear, possibly to the point of having no definable battlefields or fronts. The distinction between "civilian" and "military" may disappear. Actions will occur concurrently throughout all participants' depth, including their society as a cultural, not just a physical, entity. Major military facilities, such as airfields, fixed communications sites, and large headquarters will become rarities because of their vulnerability; the same may be true of civilian equivalents, such as seats of government, power plants, and industrial sites (including knowledge as well as manufacturing industries). 125 It is precisely this blurring of peace and war and the demise of traditionally definable battlefields that provides the impetus for the formulation of a new theory of war powers. As evidenced by Part M, supra, the constitutional allocation of war powers, and the Framers' commitment of the war power to two co-equal branches, **was not designed** to cope with the current international system, one that is characterized by the persistent machinations of international terrorist organizations, the rise of multilateral alliances, the emergence of **rogue states**, and the potentially wide proliferation of easily deployable **w**eapons of **m**ass **d**estruction, **nuclear and otherwise.** B. The Framers' World vs. Today's World The Framers crafted the Constitution, and the people ratified it, in a time when everyone understood that the state controlled both the raising of armies and their use. Today, however, the threat of terrorism is bringing an end to the era of the nation-state's legal monopoly on violence, and the kind of war that existed before-based on a clear division between government, armed forces, and the people-is on the decline. 126 As states are caught between their decreasing ability to fight each other due to the existence of nuclear weapons and the increasing threat from non-state actors, it is clear that the Westphalian system of nation-states that informed the Framers' allocation of war powers is no longer the order of the day. 127 As seen in Part III, supra, the rise of the modem nation-state occurred as a result of its military effectiveness and ability to defend its citizens. If nation-states such as the United States are unable to adapt to the changing circumstances of fourth-generational warfare-that is, if they are unable to adequately defend against low-intensity conflict conducted by non-state actors-"**then clearly [the modem state] does not have a future in front of it**.' 128 The challenge in formulating a new theory of war powers for fourthgenerational warfare that remains legally justifiable lies in the difficulty of adapting to changed circumstances while remaining faithful to the constitutional text and the original meaning. 29 To that end, it is crucial to remember that the Framers crafted the Constitution in the context of the Westphalian system of nation-states. The three centuries following the Peace of Westphalia of 1648 witnessed an international system characterized by wars, which, "through the efforts of governments, assumed a more regular, interconnected character."' 130 That period saw the rise of an independent military class and the stabilization of military institutions. Consequently, "warfare became more regular, better organized, and more attuned to the purpose of war-that is, to its political objective."' 1 3' **That era is now over**. Today, the stability of the long-existing Westphalian international order has been greatly eroded in recent years with the advent of international terrorist organizations, which care nothing for the traditional norms of the laws of war. This new global environment exposes the limitations inherent in the interpretational methods of originalism and textualism and necessitates the adoption of a new method of constitutional interpretation. While one must always be aware of the text of the Constitution and the original understanding of that text, that very awareness identifies the extent to which fourth-generational warfare epitomizes a phenomenon unforeseen by the Framers, a problem the constitutional resolution of which must rely on the good judgment of the present generation. 13 Now, to adapt the constitutional warmarking scheme to the new international order characterized by fourth-generational warfare, one must understand the threat it is being adapted to confront. C. The Jihadist Threat The erosion of the Westphalian and Clausewitzian model of warfare and the blurring of the distinction between the means of warfare and the ends of policy, which is one characteristic of fourth-generational warfare, apply to al-Qaeda and other adherents of jihadist ideology who view the United States as an enemy. An excellent analysis of jihadist ideology and its implications for the rest of the world are presented by Professor Mary Habeck. 133 Professor Habeck identifies the centrality of the Qur'an, specifically a particular reading of the Qur'an and hadith (traditions about the life of Muhammad), to the jihadist terrorists. 134 The jihadis believe that the scope of the Qur'an is universal, and "that their interpretation of Islam is also intended for the entire world, which must be brought to recognize this fact peacefully if possible and through violence if not."' 135 Along these lines, the jihadis view the United States and her allies as among the greatest enemies of Islam: they believe "that every element of modern Western liberalism is flawed, wrong, and evil" because the basis of liberalism is secularism. 136 The jihadis emphasize the superiority of Islam to all other religions, and they believe that "God does not want differing belief systems to coexist."' 37 For this reason, jihadist groups such as al-Qaeda "recognize that the West will not submit without a fight and believe in fact that the Christians, Jews, and liberals have united against Islam in a war that will end in the complete destruction of the unbelievers.' 138 Thus, the adherents of this jihadist ideology, be it al-Qaeda or other groups, will continue to target the United States until she is destroyed. Their ideology demands it. 139 To effectively combat terrorist groups such as al-Qaeda, it is necessary to understand not only how they think, but also how they operate. Al-Qaeda is a transnational organization capable of simultaneously managing multiple operations all over the world."14 It is both centralized and decentralized: al-Qaeda is centralized in the sense that Osama bin Laden is the unquestioned leader, but it is decentralized in that its operations are carried out locally, by distinct cells."4 AI-Qaeda benefits immensely from this arrangement because it can exercise direct control over high-probability operations, while maintaining a distance from low-probability attacks, only taking the credit for those that succeed. The local terrorist cells benefit by gaining access to al-Qaeda's "worldwide network of assets, people, and expertise."' 42 Post-September 11 events have highlighted al-Qaeda's resilience. Even as the United States and her allies fought back, inflicting heavy casualties on al-Qaeda in Afghanistan and destroying dozens of cells worldwide, "al-Qaeda's networked nature allowed it to absorb the damage and remain a threat." 14 3 This is a far cry from earlier generations of warfare, where the decimation of the enemy's military forces would generally bring an end to the conflict. D. The Need for Rapid Reaction and Expanded Presidential War Power By now it should be clear just how different this conflict against the extremist terrorists is from the type of warfare that occupied the minds of the Framers at the time of the Founding. Rather than maintaining the geographical and political isolation desired by the Framers for the new country, today's United States is an international power targeted by individuals and groups that will not rest until seeing her demise. The Global War on Terrorism is not truly a war within the Framers' eighteenth-century conception of the term, and the normal constitutional provisions regulating the division of war powers between Congress and the President do not apply. Instead, this "war" **is a struggle for survival** and dominance against forces that threaten to destroy the United States and her allies, and the fourth-generational nature of the conflict, highlighted by an indiscernible distinction between wartime and peacetime, necessitates an evolution of America's traditional constitutional warmaking scheme. As first illustrated by the military strategist Colonel John Boyd, constitutional decision-making in the realm of war powers in the fourth generation should consider the implications of the OODA Loop: Observe, Orient, Decide, and Act. 44 In the era of fourth-generational warfare, **quick reactions**, proceeding through the OODA Loop rapidly, and disrupting the enemy's OODA loop are the keys to victory. "In order to win," Colonel Boyd suggested, "we should operate at a **faster tempo** or rhythm than our adversaries." 145 In the words of Professor Creveld, "[b]oth organizationally and in terms of the equipment at their disposal, the armed forces of the world will have to adjust themselves to this situation by changing their doctrine, doing away with much of their heavy equipment and becoming more like police."1 46 Unfortunately, the existing constitutional understanding, which diffuses war power between two branches of government, necessarily (by the Framers' design) slows down decision- making. In circumstances where war is undesirable (which is, admittedly, most of the time, especially against other nation-states), the deliberativeness of the existing decision-making process is a positive attribute. In America's current situation, however, in the midst of the conflict with al-Qaeda and other international terrorist organizations, the existing process of constitutional decision-making in warfare may prove a **fatal hindrance** to achieving the initiative **necessary** for victory. As a **slow-acting**, deliberative **body**, Congress does not have the ability to adequately deal with **fast-emerging situations** in fourth-generational warfare. Thus, in order to combat transnational threats such as al-Qaeda, the executive branch **must** have the ability to operate by taking offensive military action even without congressional authorization, because **only the executive branch** is capable of the swift decision-making and action necessary to prevail in fourth-generational conflicts against fourthgenerational opponents.

### 5th Off

#### Iran sanctions package stopped in senate by Obama—stalling sanctions key to keep Iran at the table and maintain cooperation with allies to reach a compromise.

Reuters 10/2

Reuters, “Iran sanctions hit delay in US Senate ahead of Geneva talks,” 10/2/13, Jerusalem Post

WASHINGTON - Under pressure not to squeeze Iran too hard, the US Senate is unlikely to impose a fresh round of sanctions on the Islamic Republic until after Tehran holds nuclear talks with world powers later this month, lawmakers and congressional aides said. The Senate Banking Committee had been due in September to look at a new package of sanctions passed in July by the House of Representatives, but now it will not do so for at least a few more weeks, an aide said. That could create a better atmosphere at talks between Iran and six major nations in Geneva on October 15-16, the first such encounter since President Barack Obama and new Iranian President Hassan Rouhani held a historic phone call last week. While the sanctions issue has been slowed by congressional wrangling over the US government shutdown, lawmakers acknowledged that the idea had come up of deliberately delaying new sanctions to improve the mood at the Geneva talks. "There's been some discussion about whether it's best right now, while the negotiations are occurring, just to keep the existing ones in place," Senator Bob Corker, the senior Republican on the Senate Foreign Relations Committee and a member of the Banking Committee, told Reuters. He stressed that Congress generally remains deeply suspicious of Iran and supportive of tougher sanctions. Catherine Ashton, the European Union's foreign policy chief, made clear on Monday she would prefer US lawmakers and others not to impose additional sanctions before the nuclear talks. "I would like to get to Geneva with the best possible atmosphere to really have these negotiations," she said. Congressional aides familiar with the issue said some Obama administration officials have been quietly pressing for Congress to hold off. "We will continue to consult with Congress on all Iran-related legislation as we have long before last week. Iran has an imperative to improve its economy, because every single economic indicator is negative for them," said State Department spokeswoman Jen Psaki. The House passed a new package of sanctions by a vote of 400 to 20 at the end of July. That bill seeks to cut Iran's oil exports by another 1 million barrels per day over a year to near zero, to try to reduce the flow of funds to the nuclear program. SQUEEZING IRAN Sanctions on Iran's oil sales, shipping and insurance businesses have led to losses of billions of dollars in revenue each month as well as crippling inflation and high unemployment. The Senate bill will likely be less tough than the House's measure in targeting Iran's oil exports, which already have been halved by existing European and US sanctions. The Obama administration has noted that it has concerns about the House legislation. Administration officials declined to elaborate, but analysts and congressional aides said the White House fears that if sanctions are too hard on Iran's customers they may stop cooperating with the United States. Existing sanctions - which push countries including China, India and Japan to reduce their imports of Iranian oil by threatening to cut off their banks from the US financial system - may have already gone as far as they can without antagonizing these countries. "It's hard to get Iran's main customers in Asia to cut their (oil) purchases too much more, so seeking to cut oil exports even further could be counterproductive and the sanctions coalition could unravel," said Jeffrey Schott, an expert in sanctions at the Peterson Institute for International Economics. An eventual sanctions package from the Senate could include new measures to pressure Iran's natural gas exports and other businesses.

#### OCO causes contentious debates in congress

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. ¶

#### Plan causes Obama to fighting to defend his war power- this saps Obama’s capital, trading off with rest of 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.

#### Agreement on Iranian proliferation solves regional tension, Iranian prolif, and war now – new congressional sanctions crush the fragile momentum

NIAC, nonpartisan, nonprofit organization dedicated to advancing the interests of the Iranian-American community, “NIAC Applauds US-Iran Diplomatic Progress, Warns Congress Against Sabotaging a Deal,” 10/16/2013. http://www.niacouncil.org/site/News2?page=NewsArticle&id=9893

Washington, DC - The National Iranian American Council released the following statement after the conclusion of diplomatic negotiations between the P5+1 and Iran in Geneva:¶ ¶ The National Iranian American Council (NIAC) applauds the U.S. and Iran for engaging in substantive, productive negotiations in Geneva over the past two days. Both Iran and the U.S. and other members of the P5+1 have declared their commitment to reaching a solution that introduces verifiable limits on Iran’s nuclear program and ends the nuclear standoff. Such an agreement is possible and achievable if each side remains committed to the diplomatic track and halts escalatory measures that have prevented diplomatic progress in the past.¶ ¶ Ahead of new negotiations that are scheduled for November 7 and 8, it is critical that the U.S. Congress not interfere. New sanctions legislation would sabotage this promising but fragile process. The Senate must not complicate the talks by tying the hands of the President or undermining confidence that the U.S. can reciprocate in these negotiations. A verifiable agreement to reduce tensions, ensure Iran never develops nuclear weapons, and prevent war is possible if Congress gives diplomacy a chance to succeed. The consideration of new sanctions would undermine a deal. ¶ ¶ The new, positive atmosphere surrounding talks is due, in large part, to a shift in tone and approach from each party. The P5+1, critically, showed flexibility by agreeing to discuss the endgame with Iran, departing from their previous focus on short-term confidence building measures. Each side must continue to focus on a pragmatic approach towards a shared vision for the endgame in order to overcome the deep, long-held mistrust that has fueled escalatory policies. ¶ ¶ Further credit should be given to the injection of political capital into the negotiating process. Direct talks between Kerry and Zarif on the sidelines of the UN General Assembly, and the historic phone call between Presidents Obama and Rouhani, have helped to break the taboo of diplomatic contact between the U.S. and Iran. NIAC supports further bilateral discussions between the United States and Iran to continue progress on the nuclear issue, and to address other issues of concern at the earliest possible opportunity, including human rights and regional security.¶ ¶ However, in Congress, Rep. Trent Franks (R-AZ) introduced a war authorization along with 14 other Republicans. In the Senate, the Banking Committee is set to consider new sanctions that passed the House just days before the inauguration of Iran’s new President. If either measure passes, it would reinforce Iranian fears that the United States is really interested in regime change and is unwilling or unable to deliver sanctions relief that is required by any deal. It is time for those in Congress who are serious about preventing war and finding a diplomatic solution to the nuclear standoff to stand up against efforts to sabotage talks and box the U.S. into a military confrontation.

#### Deal prevents global nuclear war

Edelman, distinguished fellow – Center for Strategic and Budgetary Assessments, ‘11

(Eric S, “The Dangers of a Nuclear Iran,” *Foreign Affairs*, January/February)

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

### 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.

### Arms Race

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

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

- Defenses solve---benefits of offense are overstated

- Too difficult to execute/mistakes in code are inevitable

- AT: Infrastructure attacks

- Military networks are air-gapped/difficult to access

- Overwhelming consensus goes neg

Gray 13

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

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

#### 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. 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.

#### Prolif inev, but no cyber arms race – their impacts are fear mongering which ignore deployment difficulties

Economist 13

(“Digital doomsters: How scared should we be?” 6-29-13, http://www.economist.com/news/books-and-arts/21580123-how-scared-should-we-be-digital-doomsters,)

Yet businesses seeking to increase their sales, and officials and politicians who want more money and power, love tales of doom and gloom. Trade is booming for what some have dubbed the “cyber-industrial complex”. State agencies demand more power to fend off a dreadful attack by a foreign enemy—a kind of “digital Pearl Harbour”. Companies peddle security advice and software, often with a hefty price tag. The difficulty for the citizen and taxpayer is to decide: are people being too paranoid, or too complacent? Two new books provide some useful perspective. “A Fierce Domain” is a collection of essays edited by Jason Healey, a former cyber-policy chief in the Obama White House. His main point is that this is not a new problem: the first big cyber-attack dates back to 1986, when a bunch of German hackers in Hanover, working for the KGB, sneaked into American military networks. Named “Cuckoo’s Egg”, it was caught only because a sharp-eyed official noted a tiny 75-cent billing error, revealing unauthorised use of a computer network. Many more attacks have followed: Moonlight Maze, Solar Sunrise, Titan Rain and Byzantine Hades. None is a household name, though from the gripping accounts in Mr Healey’s book many readers will feel they all should be. One especially damaging operation involved the theft of top-secret material from the most classified NATO networks. The attackers had used infected memory sticks, which were left lying around in car parks near sensitive buildings. Careless or thrifty officials picked them up, and some used them to copy material between classified computer networks and those connected to the internet. A clever bit of software then copied, encrypted, compressed and dispatched the material—probably, spooks think, to Moscow. Mr Healey’s main message is to urge policymakers to be less secretive and more humble. Too many past attacks remain classified. Officials continue to burble the same warnings and assurances as they did 20 years ago; the public is left in the dark. Thomas Rid is a German-born academic, now at King’s College London. He is one of Britain’s leading authorities on, and sceptics about, cyber-warfare. His provocatively titled book attacks the hype and mystique about sabotage, espionage, subversion and other mischief on the internet. He agrees that these present urgent security problems. But he dislikes talk of “warfare” and the militarisation of the debate about dangers in cyberspace. Computer code can do lots of things, but it is not a weapon of war. He criticises the American air force for using a “lobbying gimmick” with talk of “cyber” as a fifth domain of warfare, after land, sea, air and space. However much the military brass may hype up the threat, states are in fact highly unlikely to use cyber-weapons against each other, Mr Rid argues. They are expensive to acquire, unreliable and fiddly. That does not mean they are useless. Malicious code, “malware”, can do shocking damage, destroying machines, starting fires, spewing pollution or jamming communications. Cleverer weapons could be more dangerous still, such as malicious code that adapts to its environment, rewriting itself to evade pursuers. They will be used, but as part of sabotage or terrorism rather than all-out war, he argues.

#### 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.¶

#### Cyber prolif does not increase the use of cyberweapons or risk of war

Liff 12

(research fellow @ University of Tokyo’s Institute of Social Science and political science PhD candidate @ Princeton, Adam P., "Cyberwar: A New ’Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War" Journal of Strategic Studies Volume 35, Issue 3, 2012) KH
Although the proliferation of cyberwarfare capabilities may have the net effect of increasing the frequency of war, much of the public debate on cyberwarfare is excessively pessimistic. Cyberwarfare appears to be a tool for states to pursue political (strategic) and/or military (tactical) objectives at relatively low cost only under very limited circumstances. Although Stuxnet manifests cyberwarfare's potential to become a useful *brute force* measure, no examples of irrefutably effective *coercive* CNA exist. Cyberattacks against Estonia in 2007 were an example of ‘hacktivism’, not war.[64](http://www.tandfonline.com.libproxy.uwyo.edu/doi/full/10.1080/01402390.2012.663252#FN0064)Although the 2008 cyber exchange between Georgia and Russia better fits the bill, the attacks had no measurable impact on bargaining or the war's outcome. Thus, CNA's most ‘game-changing’ aspect may be its usefulness as a brute force weapon, which will probably have at most a marginal effect on the frequency of war. Inshort, although gradual proliferation of cyberwarfare capabilities may be inevitable, the widespread use of CNA is probably not.

(\*CNA = computer network attacks)

#### Defensive measures overwhelm

Rid 12

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

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

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

Kaminski 13

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

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

### Alliances

#### China-Taiwan war unlikely – economic ties and improving relations

Weede, Former Professor of Sociology at the University of Bonn, 2010

(Erich, retired in 2004, current member of the Mont Pelerin Society, “The Capitalist Peace and the Rise of China: Establishing Global Harmony by Economic Interdependence”, International Interactions 36:2, 206-213, 5/18/10, accessed 6/20/11) JDB

From an international trade perspective, all of East Asia has recently become a Chinese sphere of influence. China is the most important destination of Japanese, South Korean, and Taiwanese exports—ahead of the United States. Although Taiwanese politicians around the turn of the millennium rejected the idea of reunification on the Mainland’s terms, and although some of them were attracted to the idea of declaring the legal independence of Taiwan, economic and social ties across the Taiwan Strait grew vigorously at the same time. Taiwanese companies employ millions of people on the mainland. About a million people from Taiwan live on the Chinese mainland. Mainland China has been the preferred destination of Taiwan’s foreign investment. Since the lateral escalation of a military conflict between the People’s Republic of China and Taiwan constitutes the most plausible scenario whereby the U.S. and China might get into a war, economic interdependence between China and Taiwan contributes to the preservation of peace. Recently, political relations between the People’s Republic of China and the Republic of China on Taiwan have improved fast. Given the record of Sino-Japanese wars in the past and the power of these neighboring states, the extent of Sino-Japanese economic cooperation provides another reason for optimism. The capitalist peace stands a chance to apply between China and its neighbors and competitors.

**China is de-escalating South China Sea tensions – promoting peaceful negotiations now**

**Ponnudurai ‘12 –** Parameswaran Ponnudurai, September 26th, 2012, "China Seeks To Mend Fences In Sea Dispute – Analysis" www.eurasiareview.com/26092012-china-seeks-to-mend-fences-in-sea-dispute-analysis/

As Beijingflexes its muscles over its territorial dispute with Japan in the East China Sea, it **is mending fences with Southeast Asian nations** after a spate of tensions in the contested South China Sea.¶ Following much prodding and diplomacy, **China appears to be showing some flexibility in its approach towards drawing up a code of conduct with the Southeast Asian nations** aimed at avoiding clashes over competing territorial claims in the vast sea, diplomats in the region told RFA.¶ Although they are skeptical of any early breakthrough for a legally binding document between China and the Association of Southeast Asian Nations (ASEAN) to guide behavior in the sea, there is optimism that negotiations will occur on a sustained basis.¶“We see some flexibility to discuss the COC with ASEAN,” one Southeast Asian diplomat said, referring to the elusive Code of Conduct or COC which ASEAN—comprising Brunei, Burma, Cambodia, Indonesia, Laos, Malaysia, the Philippines, Singapore, Thailand and Vietnam—has been striving to devise with Beijing for a decade.¶**In an initial display of seriousness that it is prepared to come to the table, China sent its senior officials to Cambodia last week to informally discuss with their counterparts from ASEAN the prospects for drawing up a code**, officials said.¶This is the first meeting between the two sides specifically on the maritime dispute since ASEAN plunged into a crisis two months ago when foreign ministers of the 10-member bloc failed to issue their customary joint statement at the conclusion of their annual meeting hosted by Cambodia, China’s top ally in Southeast Asia.¶ Some ASEAN diplomats had charged that Cambodia had been influenced by China not to incorporate in the statement the views of ASEAN member states the Philippines and Vietnam, which had tiffs earlier this year with Beijing over islands and reefs in the South China Sea, causing an impasse at the meeting.¶ China claims to South China Sea¶ China claims to South China Sea¶ The ASEAN-China Senior Officials’ Informal Consultations on the Code of Conduct (COC) in the South China Sea, as last week’s meeting in Phnom Penh was officially called, was among a series of discussions in preparation for the ASEAN summit and the East Asia Summit in November.¶ “**Compared to two months ago, when there was complete reluctance to come to the table, China appears willing to sit down and talk,” said one Southeast Asian official, who was briefed on the talks but spoke on condition of anonymity**.¶ “Indirectly, they may be feeling the heat from the mounting criticism over what happened at the meeting in July which was a big blow to ASEAN,” the official said.¶ “But China has also asked the ASEAN states to do their part by reducing tensions and not conducting border incursions and creating a conducive environment for any future talks. **They don’t want us to bring in third parties [the United States] over the conflict and want us to stick to the 2002 declaration**,” the diplomat said.¶ Under a 2002 agreement for managing their overlapping territorial claims, ASEAN and China adopted a Declaration on the Conduct of Parties in the South China Sea, called DOC as a first step towards a binding code of conduct.¶ But in a reflection of the sensitivity over the issue, it was only last year—after 10 years—that they agreed on a set of guidelines to implement the declaration that was aimed at laying the groundwork for discussions on the regional code of conduct.¶ Ray of hope¶ The new ray of hope for achieving a COC comes after extensive diplomacy, including U.S. Secretary of State Hillary Clinton’s trip to Southeast Asia and China, with a meeting with Chinese President Hu Jintao.¶Chinese leaders told Clinton—who has often emphasized that freedom of navigation in the South China Sea is a U.S. “national interest”—that they want to pursue the COC, U.S. Ambassador to China Gary Locke told a forum in Washington last week, saying the talks between the two sides were “very good.”¶“I’ve also heard from many prominent Chinese academics that **China would like somehow to return to the status quo**, that **they would like to lower the temperature**,” Locke said.¶ Chinese Foreign Minister Yang Yechi had also visited Indonesia as well as Malaysia and Brunei, giving reassurances that diplomacy was still on track.¶ Cambodian Prime Minister Hun Sen, embarrassed by the failure by his country as 2012 ASEAN chairman to forge an agreement on the foreign ministers’ joint statement, also made a trip to China this month, meeting Prime Minister Wen Jiabao.¶ Hun Sen won assurances from Wen that Beijing will “closely work” to make the upcoming East Asia Summit which Cambodia will host a success,” Chinese media reported.¶ Southeast Asian diplomats said a key objective is to get an initial ASEAN-China accord on the COC before the November East Asia Summit, to be attended by leaders of ASEAN as well as China, Japan, South Korea, India, Australia, New Zealand, Russia and the United States.¶**Key elements of the COC have been agreed upon by ASEAN member states whose foreign ministers will meet to consider a full draft document on the sidelines of the U.N. General Assembly in New York this coming week**, the diplomats said.¶ “We are now in the process of spelling out the draft [of the code] and we hope to be able to share it with my ASEAN foreign minister colleagues when I meet them in New York,” Indonesian Foreign Minister Marty Natalegawa said, according to the Jakarta Globe newspaper.¶ “The development of the South China Sea [issues] reminds us how we desperately need the code of conduct, [so] I’m trying to use the momentum,” Marty said, as Indonesia asserts a leadership role in ASEAN to deal with the South China Sea issue, Asia’s biggest potential military flashpoint.¶ Cambodia or Thailand, which is the ASEAN coordinator for China issues, could host another round of informal talks between senior officials from ASEAN and China on the COC before the East Asia Summit.¶ “Both sides might also issue a joint statement to commemorate the 10th anniversary of the DOC at Summit,” an official involved in the planning of the summit told RFA, referring to the declaration adopted in 2002 in Cambodia to set the stage for the regional code of conduct.¶**Beijing has maintained all this while that it wants to resolve the South China Sea territorial conflicts on a bilateral basis with ASEAN members Brunei, Malaysia, the Philippines and Vietnam, which have competing claims with China**.

**[2] Zero chance of war in the SCS – blue highlighting**

Gupta 11 [Rukmani Gupta, Associate Fellow at the Institute for Defence Studies and Analyses, “South China Sea Conflict? No Way,” <http://the-diplomat.com/2011/10/23/south-china-sea-conflict-no-way/2/>]

Despite what opinion pieces in the Global Times may say, there’s reason to suspect that China doesn’t want to escalate conflict in the region. Although commentary from the United States has suggested that China considers the South China Sea a ‘core interest,’ no official Chinese writing canbe found to corroborate this. In addition, China’s caution can also be seen as a reflection on Chinese military capabilities, which aren’t seen as strong enough to win a war over the South China Sea. In fact, the China National Defence News, published by the Chinese People’s Liberation Army’s General Political Department, has likened the use of force by China in the South China Sea to shooting one’s own foot. Not only would the use of force bring ASEAN together on the issue, it could conceivably involve the United States and Japan, derail China’s plans for continued economic growth and undo China’s diplomacy. Chinese declarations on the South China Sea can therefore be seen as attempts to exaggerate claims so as to secure a better negotiating stance.

#### Restrictions gut US military ability to respond to Chinese threats which means 1ac restrictions trigger their China impact.

Bucci, Rosenzweig, and Inserra ‘2013

[Steven P. Bucci Ph.D, director of the Allison Center for Foreign Policy Studies at The Heritage Foundation, served America for three decades as an Army Special Forces officer and top Pentagon official; Paul Rosenzweig, visiting fellow for the Heritage Foundation, helped craft policy and strategy inside the Department of Homeland Security; Research Assistant, National Security and Cyber Security <http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace> //wyo-sf]

Failure to take responsible action, however, leaves the U.S. vulnerable to a variety of threats. Nation-states such as Russia, China, and Iran are more than willing to steal or destroy U.S. digital property to further their power or prestige. Non-state actors such as Hamas and Hezbollah have also shown the capability to employ cyber methodologies and criminal organizations from around the world, and have acted as hired guns as well as on their own, using cyber tools as their weapon of choice.[1] Cyber espionage is rampant, with U.S. companies estimated to be losing a staggering $250 billion every year in intellectual property.[2] The latent nature of this threat leads many people to forgo investment in security because it has not yet harmed their organization or because they mistakenly believe that they have nothing a cyber adversary would want. More important, they misunderstand that their own cyber insecurity has collateral effects on others—effects for which they are responsible. There is, therefore, a role for the federal government to encourage actions that will improve the overall cybersecurity posture of the U.S. That role, however, is not to set mandatory regulations. As the U.S. Government Accountability Office (GAO) has found, such an approach would be more like an anchor holding back U.S. entities while not providing additional security.[3]

#### No nuclear escalation and outside powers will stay out

Roger **Cliff,** Ph.D. in international relations, Princeton, M.A. in history (Chinese studies), University of California, San Diego, Assistant for Strategy Development, Office of the Secretary of Defense, and David A. **Shlapak**, Ph.D., senior international policy analyst, RAND Project Air Force Report, 200**7**

This situation would occur if China attempted to use force to achieve unification, the United States intervened, and China’s efforts were defeated, but Beijing refused to accept Taiwan’s independence.10 Analysis at RAND has found that a conflict between the United States and China over Taiwan would likely be confined to the use of conventional weapons, even though both the United States and China possess nuclear weapons, and that it would not likely escalate into a broader war between the United States and China. That is, the war would be contained in the area around Taiwan; the main combatants would probably be limited to the United States, China, and Japan; and active hostilities would probably end after a relatively short time. Nonetheless, such a war would probably result in a bitter relationship between the United States and China, comparable in some ways to that between the United States and the Soviet Union during the Cold War. China might well accelerate the buildup of its military capabilities with an eye toward waging a second, this time successful, campaign to claim Taiwan. This military competition would likely also be accompanied by a broader deterioration in Sino-U.S. relations, with mutual trade and investment falling dramatically or even ceasing, and each country demanding that its allies not cooperate with its rival. Countries in Asia might find themselves under pressure to choose between good relations with the United States and good relations with China. Nonetheless, even under these circumstances, the relationship between the United States and China after an inconclusive war over Taiwan would have important differences from the one between the United States and the Soviet Union during the Cold War. Unlike the Soviet Union, China is closely integrated into the world economy. With the exception of Japan, most countries in Asia would likely regard the importance of maintaining good relations with Beijing as outweighing any concerns about China having used force against Taiwan. They would resist U.S. pressure to choose between Washington and Beijing, preferring to maintain good relations with both. This logic would apply even more strongly to countries outside the region, which would be even less concerned about China’s use of force.

#### Coalition building doesn’t solve-can’t shape policies

Blechman, 2005 (Barry M, founder and president of DFI International Inc., a research and consulting company in Washington, DC (frequent consultant to the US Government),Winter 2004/ “Soft Power: The Means to Success in World Politics,” Political Science Quarterly, Vol. 119, Iss 4; pg. 680-681, proquest)

Soft Power: The Means to Success in World Politics by Joseph S. Nye. New York, Public Affairs, 2004. 208 pp. $25.00.

Joseph Nye has done his usual masterful job in this elegant monograph, describing the many sources of influence in international relations and reminding readers that excessive reliance on military or economic instruments of policy can often trigger backlashes that harm the nation's interests in the longer term. Nye points out that rather than either coercing others to share our objectives or buying their agreement with economic incentives, it is better for the United States to get what it wants because others share our goals. Soft power, he says, is more than influence or persuasion, "it is also the ability to attract, and attraction often leads to acquiescence" (p. 6). Much of the book is devoted to descriptions of the sources of soft power in the United States and other countries, including the nation's values and the styles of individual behavior expressed in the dominant culture and transmitted through both commercial activities (Hollywood movies, for example) and personal contacts, and the nation's policies, particularly when they reflect values that are widely shared around the world. Thus, Nye argues, the United States won the Cold War in part because of the attractiveness of the American form of government and economy, and because American values, or American soft power, eventually came to dominate global perceptions of the two superpowers and induced others to want to share in our vision of the world. Although Nye makes a persuasive case, in the end, the book is unsatisfying because of inherent limitations in the concept of soft power. It is a form of power, yes, but not an instrument of power that can be deployed in specific situations or even one that can be shaped in a meaningful way by the government. Soft power exists, and may be influenced by governmental choices**, but it is more an existential factor in the policy environment than something policy makers can utilize to their advantag**e**. A nation's "attractiveness" § Marked 16:39 § to others is not a factor that can be exploited in any coherent way**. Indeed, the chapter "Wielding Soft Power" is devoted solely to public diplomacy-the various means available to the government to communicate the nation's policies and values. But in our interdependent and interactive world, government-inspired communications of all types are only a tiny fraction of the information received by people around the world about the United States. Even if the United States spent a more reasonable amount on its public diplomacy than it does now, as Nye rightfully suggests, it's diplomacy would still be dwarfed by the private sources of information in the United States and abroad, and by the huge volume of interactions among citizens of all nations that take place independent of government actions or inactions

#### Aggression won’t escalate

**Sieg 9/23** (Linda, – writer for Reuters “Japan, China military conflict seen unlikely despite strain”, <http://www.reuters.com/article/2012/09/23/us-china-japan-confrontation-idUSBRE88M0F220120923>)

¶ (Reuters) - Hawkish Chinese commentators have urged Beijing to prepare for military conflict with Japan as tensions mount over disputed islands in the East China Sea, but most experts say chances the Asian rivals will decide to go to war are slim.¶ A bigger risk is the possibility that an unintended maritime clash results in deaths and boosts pressure for retaliation, but even then Tokyo and Beijing are expected to seek to manage the row before it becomes a full-blown military confrontation.¶ "That's the real risk - a maritime incident leading to a loss of life. If a Japanese or Chinese were killed, there would be a huge outpouring of nationalist sentiment," said Linda Jakobson, director of the East Asia Program at the Lowy Institute for International Policy in Sydney.¶ "But I still cannot seriously imagine it would lead to an attack on the other country. I do think rational minds would prevail," she said, adding economic retaliation was more likely.¶ A feud over the lonely islets in the East China Sea flared this month after Japan's government bought three of the islands from a private owner, triggering violent protests in China and threatening business between Asia's two biggest economies.¶ Adding to the tensions, China sent more than 10 government patrol vessels to waters near the islands, known as the Diaoyu in China and the Senkaku in Japan, while Japan beefed up its Coast Guard patrols. Chinese media said 1,000 fishing boats have set sail for the area, although none has been sighted close by.¶ Despite the diplomatic standoff § Marked 16:38 § and rising nationalist sentiment in China especially, experts agree neither Beijing nor Tokyo would intentionally escalate to a military confrontation what is already the worst crisis in bilateral ties in decades.¶ U.S. PRESSURE¶ "The chances of a military conflict are very, very slim because neither side wants to go down that path," said former People's Liberation Army officer, Xu Guangyu, now a senior consultant at a government-run think tank in Beijing.¶ Pressure from the United States, which repeated last week that the disputed isles were covered by a 1960 treaty obliging Washington to come to Japan's aid if it were attacked, is also working to restrain both sides, security experts said.¶ "I very seriously do not think any of the involved parties - Japan, China and including the United States because of its defense treaty (with Japan) - want to see a military conflict over this dispute," said the Lowy Institute's Jakobson.¶ "They don't want to risk it, they don't seek it and they do not intend to let it happen."¶ Still, the possibility of a clash at sea remains.¶ While the presence of the Chinese surveillance ships - none of which is a naval vessel - and Japan Coast Guard ships in the area might appear to set the stage for trouble, military experts said each side would try to steer clear of the other.¶ "The bad news is that China sent ships to the area. The good news is that they are official ships controlled by the government," said Narushige Michishita at the National Graduate Institute for Policy Studies in Tokyo.¶ "This is good news because they are not likely to engage in aggressive action because that would really exacerbate the situation and turn it into a major crisis," said Michishita.¶ The Chinese ships, he said, had another mission besides asserting China's claims to the islands and nearby waters.¶ "My guess is that some (Chinese) official patrol boats are there to watch out for fishing boats ... to stop them from making problems," Michishita said.¶ FISHING BOATS WILD CARD¶ Military specialists say the Chinese patrol vessels are well disciplined as are the Japan Coast Guard ships, while the two sides have grown accustomed to communicating.¶ "Both sides are ready, but both sides are very well under control," said a former senior Japanese military official.¶ What worries observers most is the risk that a boat carrying Chinese fishermen slips through or activists try to land, sparking clashes with Japan's Coast Guard that result in deaths - news of which would spread like wildfire on the Internet.¶ In 1996, a Hong Kong activist drowned in the nearby waters. ¶ Diplomatic and economic relations chilled sharply in 2010 after Japan arrested a Chinese trawler captain whose boat collided with a Japan Coast Guard vessel. This time, tensions are already high and China is contending with a tricky once-in-a-decade leadership change while Japan's ruling party faces a probable drubbing in an election expected in months.¶ "Two rational governments of major countries would not intentionally decide to enter into a major war with each other over a few uninhabited rocks," said Denny Roy, an Asia security expert at the East-West Center in Hawaii.¶ "But unfortunately, you can arrive at war in ways other than that - through unintended escalation, in which both countries start out at a much lower level, but each of them think that they must respond to perceived provocation by the other side, both very strongly pushed into it by domestic pressure. That seems to be where we are now and it is difficult to see how countries can get out of that negative spiral."¶ Others, however, were more confident that an unplanned clash could be kept from escalating into military conflict.¶ "That's not really a major possibility, because there are still broad channels of communication between the two sides, and they would help prevent that happening. Both sides could still talk to each other," said former senior PLA officer Xu.¶ "Even before anything happened, you would also have the U.N Secretary General and others stepping in to ensure that the situation does not get out of control."