### 1NC T

#### Interpretation- “war powers authority of the President” refers to authority given to the President by Congress- this means there has to be an explicit authorization for the thing they restrict

Bejesky 2012 (Robert, M.A. Political Science (Michigan), M.A. Applied Economics (Michigan), LL.M. International Law (Georgetown). The author has taught international law courses for Cooley Law School and the Department of Political Science at the University of Michigan, American government and constitutional law courses for Alma College, and business law courses at Central Michigan University and the University of Miami, WAR POWERS PURSUANT TO FALSE PERCEPTIONS AND ASYMMETRIC INFORMATION IN THE "ZONE OF TWILIGHT,” St. Mary's Law Journal, 44 St. Mary's L. J. 1, lexis)

V. CONCLUSION¶ The roles of war powers delegated to Congress and the Executive within the text of the United States Constitution are quite clear when Framer intent and historical records are considered. Congress authorizes the use of force; the President is Commander in Chief of the United States Military when using force within the confines of Congress's authorization. n560 Congress has authorized the use of military force in all but one major confrontation the United States has engaged in (the Korean War), which includes declaring war five times and authorizing large-scale military force four times. n561 Presidents largely adhere to the War Powers Resolution of 1973, which requires the President provide information to Congress and affirms Congress's right to authorize the use of force. n562¶ The Constitution states Congress funds, legislates over, and otherwise provides for the military and that the President is caretaker of the military during peacetime. n563 Once Congress authorizes the President to deploy military force, Congress cannot interfere with the President's execution of orders; however, Congress has limited, conditioned, and parameterized the use of force. n564 Presidents respected those restrictions at Jackson's lowest [\*94] ebb. Professors Barron and Lederman emphasized that there was no prior "sustained practice of [Presidents] actually disregarding statutes" until the last Bush Administration. n565¶ Due to drastic global changes since the Framers adopted the United States Constitution, it is possible for the Executive Branch and advocates of Executive powers to be immoderately risk-averse and propel presidential power. The President's informational advantages with the expansion of the administrative state and control over the national security apparatus, the reinterpretation of the use of force in the post-UN world and disparate levels of force, judicial hesitation to accept certiorari on use of force questions after the Vietnam War, and the President's advice from legal counsel are the primary variables that lead to confrontation within the zone of twilight. n566 Other considerations that should abate risk aversion since the Constitution's adoption include: today's elevated cooperation, UN restrictions on the use of force, United States hegemony, NATO as a global defense pact, and the role of the UN Security Council to prevent the use of force.¶ Advocates should be respected for their creativity in sponsoring a dominant executive position and so-called inherent presidential authority in war powers premised on originalism. n567 However, biased advisory memos classified under national security that contain faulty premises should not be regarded as legitimate opinions leading to precedent that expands presidential powers. It is toilsome to conceive that the text of the Constitution is so manipulable and that Supreme Court cases, legislation, [\*95] academics, and logic have been in discord about the scope of the Executive's war powers for nearly two centuries.

#### Centuries of legal practice support our interpretation

Dycus 2010 (Stephen, Professor, Vermont Law School, Congress’s Role in Cyber Warfare, JOURNAL OF NATIONAL SECURITY LAW & POLICY Vol. 4:155, http://jnslp.com/wp-content/uploads/2010/08/11\_Dycus.pdf)

Before an attack can be launched, of course, Congress must have¶ supplied the President with personnel and weapons.13 Moreover, Congress¶ may regulate the President’s actions as Commander in Chief, except when¶ the nation comes under sudden attack or the President exercises her tactical¶ powers (and perhaps even then). In the Supreme Court’s 1800 decision in¶ Bas v. Tingy, Justice Paterson, one of the Framers, echoed the other Justices¶ in declaring that “[a]s far as congress authorized and tolerated the war on¶ our part, so far may we proceed in hostile operations.”14 Four years later, in¶ Little v. Barreme, the Court reiterated that the President must not exceed¶ limits set forth in Congress’s authorization of hostilities.15 Since then, no¶ court has ruled otherwise.16

#### “Offensive cyber operations” are *sustained campaigns,* meant to *degrade the capabilities of an organized adversary*

Belk and Noyes 2012 (Robert, Naval aviator and Politico-Military Fellow, studying international and global affairs at the Harvard Kennedy School; Matthew, studies international security policy and is a senior associate with the cybersecurity practice at Good Harbor Consulting; this paper was a project completing their Master’s in Public Policy, On the Use of Offensive Cyber Capabilities, http://www.dtic.mil/dtic/tr/fulltext/u2/a561817.pdf)

Some, but not all, cyber actions are directed towards accomplishing¶ strategic objectives; these actions are cyber operations. We follow the JP 1-2¶ definition of objective as “The clearly defined, decisive, and attainable goal toward¶ which every operation is directed.” Cyber operations pose a much graver security¶ dilemma than mere actions, because they indicate a sustained and dedicated¶ campaign and the presence of an organized adversary. Thus, policy for engaging¶ in, or responding to, cyber operations must be different than engaging in or¶ responding to mere cyber actions.¶ Determining that a particular observed cyber action is part of a cyber¶ operation can be difficult, but can still be achieved through examining the¶ characteristics of various cyber actions to determine whether they are a part of a¶ sustained campaign or not. Identifying a cyber operation is simpler than divining¶ intent, because it only requires determining that there exists a goal and a¶ dedicated campaign to achieve it. It does not require determining what that goal¶ is or who is attempting to achieve it. Advanced Persistent Threats (APTs)29 are¶ one common example of observed actors engaging in cyber operations. Their¶ activities are typically identified as operations before the precise intent of the¶ operation is determined. The objective of an operation can be offensive, defensive, or informational¶ in nature. Offensive objectives are those seeking to coerce rival action, impose¶ harm, or degrade rival capabilities. Defensive objectives are those seeking to¶ secure one’s own systems, and preserve freedom of operation. Informational¶ objectives seek either to access or to expose information that is not generally, or¶ publically, available. There exists some overlap between these three categories.¶ For example, one may degrade rival capabilities as part of a counter-attack,¶ giving an operation both an offensive and defensive characteristic. However,¶ these categories are still useful for characterizing external cyber operations based¶ on the nature of the objectives sought.

#### Violation- they restrict an activity not authorized by Congress and they advocate different OCO

#### Reasons to vote-

#### Limits- There are literally an infinite number of theoretical detentions to make or places to introduce armed forces- our interpretation forces them to revoke things that actually happen- only way to place a predictable limit on the object of the aff’s restriction

#### Bidirectionality- they move the topic toward theoretical Presidential ASSERTIONS of authority rather than ACTUAL authority- allows the aff to do things like “restrict” to the actual authority to prevent legal challenges to it

#### Ground- they fundamentally change the nature of the lit base- they let the aff use Presidentialists like John Yoo to say basically whatever they want- we force the topic to be about the AUMF and a few other pieces of legislation- gives a more cohesive, legal focus to the topic and ensures the neg can defend all of the tactics the aff can ban

### 1NC Exec Restraint CP

#### CP Text: The President of the United States should issue an executive order prohibiting the use of offensive cyber operations about which Congress has not been notified.

### 1NC Cyber Deterrence DA

#### The US has established Cyber Deterrence

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

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

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

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

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

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

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

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

#### Nuclear war

Harrell 2/20/09 (Eben, pg. http://www.time.com/time/world/article/0,8599,1880702,00.html)

But to marvel at the bizarre coincidence of the collision, or to breathe a sigh of relief that nuclear safety was not breached, is to miss the point. The seemingly impossible collision of two subs in a large ocean should remind us of the fallacy by which we assume nuclear weapons will never be used. Because the threat of global nuclear war is not zero, even a small chance of war each year, multiplied over a number of years, adds up to the likelihood that the weapons will be used. Like those two subs stalking through the Atlantic, the odds will begin to align. Mathematically, they are destined to. This is not a mere logic game. If there is a single "big idea" to have emerged in the first decade of the new millennium — from [the September 11 attacks](http://www.time.com/time/magazine/article/0,9171,1000761,00.html" \t "_new) to the [financial crash](http://www.time.com/time/business/article/0,8599,1846450,00.html" \t "_new) — it is the notion of the ["black swan,"](http://www.time.com/time/business/article/0,8599,1853531,00.html" \t "_new) the danger posed by difficult to predict, high-impact events. The short history of nuclear weapons is already scattered with unplanned and seemingly improbable incidents that suggest we feel more secure than we should. In 1995, a communication failure with the Russian Embassy led the Russian military to believe that a weather rocket launched off the coast of Norway was an incoming submarine-launched ballistic missile. In the 1980s, malfunctioning U.S. missile defense systems relayed information to U.S. officials of a massive incoming first strike — twice. As recently as 2007, a U.S. Air Force plane flew across the American heartland while unknowingly carrying several live warheads on board. At the time, all of these events were described as freak occurrences. The truth is they were freak occurrences. But they happened.([Read the Top 10 underreported stories of 2008.](http://www.time.com/time/specials/2008/top10/article/0,30583,1855948_1861760,00.html" \t "_new)) A day after the latest nuclear accident became public, an analyst from the Federation of American Scientists, a nonproliferation think tank, released U.S. Naval intelligence documents obtained through the Freedom of Information Act that showed that the Russian Navy undertook more underwater ballistic missile submarine patrols in 2008 than it has in a decade. The Russian subs are joined in the word's oceans by nuclear-armed vessels from France, Britain, and China. Under the plains of the American West, and in similar silos in Russia, Air Force missile operators keep constant vigil, launch keys at the ready. Nuclear missiles have no self-destruct button; once launched, they cannot be called back. Twenty years after the end of the cold war, humanity still lives within 30 minutes of its own destruction. The price we pay for maintaining nuclear weapons is the gamble that the highly improbable will not lead to the unthinkable. The question to ask after this latest nervy episode: is it worth it?

### 1NC ADV 1

#### Defense fails cyber offense is key

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

Even if we would like to think so, success in the cyber domain is not only a question of defence – at least, not for the nation states. Defence capabilities have to be as preventive as possible in order to reduce the effectiveness of the adversary ́s – whoever it may be – cyber attack. However, despite the best defensive efforts, intrusions will occur. Therefore, one also has to be resilient in the cyber domain, that is, one has to have the ability to withstand attacks and failures, as well as to mitigate harm more than in other domains. The creation of cyber defence capabilities and resilience are pretty easy for the public to accept. Yet, these acts are not enough. Deterrence is also needed, that is, the capabilities and policies to convince the others not to launch a cyber attack against one. Deterrence will only be effective if one can build and demonstrate offensive cyber capabilities. To put this in a clear manner: offensive cyber capabilities are an essential element for the nation-states to succeed in their current and future international and security policies.3 Defence, resilience and offense all contribute to the country’s overall ability to protect herself – one needs them all.

#### No Solvency- Cant distinguish between cyber D# and O#

Andru E. Wall, ’11 (Senior Associate with Alston & Bird LLP; former senior legal advisor for U.S. Special Operations Command Central (2007 to 2009). “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action”, Harvard National Security Journal / Vol. 3)

This distinction between merely altering computer code without asserting control or degrading function and actually assuming control or degrading functions is consistent with international law, which does not generally consider intelligence activities to be acts of war. Its weakness, however, is definitional reliance upon the intent of the sponsor. Distinguishing cyber attack from exploitation based on the intent of the sponsor is analogous to the challenge of distinguishing between warning shots and an initiation of armed conflict: intent is clear to the person pulling the trigger, but much less so to those on the receiving end. The salient point is this: during the initial period after you discover someone is or was inside your network, you may not know whether the other person is initiating an attack or merely attempting to exploit your network. The other party knows why he is inside your network, but you do not. If you know your network is being attacked, a broad range of responses may be justified in self-defense; however, if your network is merely being exploited (an intelligence activity) your range of responses are arguably more limited. Thus, this distinction helps define the legal authority to carry out an operation, but does little to define appropriate defensive responses. Which is why intelligence is the key to successful cyberwarfare. Cyber exploitation plays a critical supporting role in cyber attack. Knowing where an adversary’s cyber systems are vulnerable will likely require computer network exploitation “to understand the target, get access to the right attack vantage point, and collect BDA [battle damage assessment].”118 In the words of one expert on cyber attack, “those who prepare and conduct operational cyberwar will have to inject the intelligence operative’s inclinations into the military ethos”—inclinations that include discrete effects, patience, an intuitive understanding of the adversary’s culture, a “healthy wariness of deception, indirection, and concealment . . . [and] a willingness to abandon attack plans to keep intelligence instruments in place.”119

#### No other country would follow the international norm - Lack of oversight and attribution problems

Tom Gjelten, 12- ’10 (Antioch University New England, “Shadow Wars: Debating Cyber 'Disarmament'”, World Affairs http://www.worldaffairsjournal.org/article/shadow-wars-debating-cyber-disarmament)

But what constitutes an “armed attack” in cyberspace? There are no soldiers crossing borders or shots fired. International law pertaining to the actual conduct of military operations is also unclear. Among the key principles under the Geneva Conventions is that the damage inflicted in a military attack should be “proportional” to the objective and that civilian targets should be avoided. But the application of those principles to cyber war is problematic. A targeting officer can use algorithms to predict the damage that will be caused by a bomb, based on its size, the angle of its approach, and the strength of the target, but an attack on a computer network can have unpredictable second- and third-order effects. The geographic spread of infections from the Stuxnet computer worm suggests that even a cyber weapon with extraordinary targeting capability cannot be easily controlled once it is let loose. Under the Bush administration, little progress was made in the cyber war discussions at the U.N. and elsewhere. Many conservatives had a longstanding aversion to arms control in general, having concluded from experiences with the Soviets during the Cold War that the U.S. military would generally adhere to treaty and legal commitments while its adversaries would not. Among those who question the value of discussing cyber war from a legal or arms control perspective is Stewart Baker, a former general counsel at the National Security Agency and an assistant secretary for policy at the Department of Homeland Security under President George W. Bush. “It is a near certainty that the United States will scrupulously obey whatever is written down,” Baker says, “and it is almost as certain that no one else will.” The U.S. disadvantage would be compounded by the fact that, by most analyses, no other military has such an advanced offensive capability for cyber war. Under a comprehensive cyber arms limitation agreement, the United States would presumably have to accept deep constraints on its use of cyber weapons and techniques. Critics also point to the so-called “attribution problem.” In conventional warfare, an aggressor can quickly be identified, and the responsibility for war crimes or treaty violations can be determined, but an attack on a computer network can be almost impossible to attribute. The use of hijacked “zombie” computers means the geographic origin of an attack may be unclear, as will be the identity of the perpetrator. “Since no one is going to get caught,” says Baker, “to say [a cyber attack] is a violation of the law of war is simply to make the law of war irrelevant.”

### 1NC ADV 2

#### CP text: The President of the United States should issue an executive order requiring the initiation of an Offensive Cyber operation against China.

#### The US must strike before china, attack is imminent

Avery Goldstein, 2013 (David M. Knott Professor of Global Politics and International Relations, Director of the Center for the Study of Contemporary China, and Associate Director of the Christopher H. Browne Cen- ter for International Politics at the University of Pennsylvania. , “First Things First, The Pressing Danger of Crisis Instability in U.S.-China Relations”, International Security, Vol. 37, No. 4 (Spring 2013), pp. 49–89)

Fourth, developments in technology since the third quarter of the twentieth century have dramatically improved the offensive conventional military capabilities available to states.46 In the European theater during the Cold War, the strategic advantage that would derive from a conventional first strike, especially during a Soviet-American crisis in which both sides were mobilized, was far from clear. Put another away, the weapons available did not clearly confer a decisive edge to either offense or defense.47 By contrast, in the early twentyarst century, although the United States enjoys a huge advantage over China in conventional military power, both sides possess capabilities that are much more effective, indeed perhaps only effective, if used to attack before the other side has either attacked or adopted countermeasures.¶ In particular, to the extent the effectiveness of the most advanced conventional weapons is tied to sophisticated command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) networks that can be degraded through kinetic strikes or electronic and cyberwarfare, their distinctive usefulness for striking the adversary, or for signaling resolve and warning of escalation, may evaporate once the ability to conadently track and target is damaged. If, as is generally believed, emerging cyber- and space-warfare capabilities favor the attacker over the defender, once peacetime restraint based on mutual vulnerability gives way to the search for advantage in a crisis, neither side can be confident about the durability of its C4ISR.48 The weaker Chinese side will have especially powerful incentives to use its most sophisticated capabilities before the integrity of elements essential to command and control over them is compromised. This may induce pressures to initiate the use of force that are as great as those induced by more traditional concerns about losing the weapons themselves.49 The stronger U.S. side, too, will face incentives to act first, though its considerations would be different

#### We have passed the point of no return- China has no incentive to halt Cyber attacks

* China has too much to gain
* Diplomatic outreach has failed
* PLA is in control of offensive capabilities

Gordon G. Chang, 6-6-13 (JD Cornell law and Author of many books about China, “Cyber Détente with China”, World Affairs)

The ultimate goal is to arrive at understandings with the Chinese. As a “senior American official involved in the negotiations” told the paper, “We need to get some norms and rules.”¶ Actually, we have long passed that stage. What we need to do at this point is stop Chinese cyber intrusions, cyber attacks, and cyber espionage, all part of what many suspect to be the most extensive cyber campaign conducted by one country against another¶ Administration officials, according to the Times, say they do not expect the talks will result in an immediate and significant reduction in Chinese attacks. And as Stanford University’s Tim Junio told the AP, “China benefits too much by stealing intellectual property from the US, so it’s really hard to imagine anyone convincing them to slow down.”¶ So what is the purpose of further talks? It’s not as if the Obama administration has not already broached the subject with Beijing. The president and various officials had numerous conversations with the Chinese during the first term, but the attacks increased dramatically in the middle of last year. This year, Treasury Secretary Jack Lew, Secretary of State John Kerry, and Joint Chiefs Chairman Martin Dempsey have all trooped to Beijing to discuss the issue with no apparent result. Despite the persistent effort to establish a cooperative relationship, the People’s Liberation Army reportedly ramped up its cyber attacks sometime around the beginning of April.

#### China first strike is inevitable: Non-Cyber based pentagon strategic choices make miscalc likely

David C. Gompert, 8-2-13 (is an adjunct senior fellow and Terrence K. Kelly is the director of the Strategy, Doctrine, and Resources Program at the Arroyo Center at the nonprofit, nonpartisan RAND Corporation.; he served as President Obama's principal deputy director of national intelligence., “Escalation Cause: How the Pentagon's New Strategy Could Trigger War with China”, RanD)

Air-Sea Battle increases the odds that a crisis will turn violent. Already, the Chinese People's Liberation Army (PLA) leans toward early strikes on U.S. forces if hostilities have begun or appear imminent (this inclination is a first premise of the Air-Sea Battle concept). Given that, to be most effective, Air-Sea Battle would need to take down Chinese targeting and strike capabilities before they could cause significant damage to U.S. forces and bases. It follows, and the Chinese fear, that such U.S. capabilities are best used early and first — if not preemptively, then in preparation for further U.S. offensive action. After all, such U.S. strikes have been used to initiate conflict twice in Iraq. This perception will, in turn, increase the incentive for the PLA to attack preemptively, before Air-Sea Battle has degraded its ability to neutralize the U.S. strike threat. It could give the Chinese cause to launch large-scale preemptive cyber- and anti-satellite attacks on our Air-Sea Battle assets. Indeed, they might feel a need, out of self-defense, to launch such attacks even if they had not planned to start a war. It is a dangerous situation when both sides put a premium on early action.

#### The CP solves and prevents nuclear escalation

DOD DSC, Department of defense Defense science board, 1-’13 (“Resilient Military Systems and the Advanced Cyber Threat”, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf)

To provide a non-nuclear but cyber survivable escalation ladder between conventional conflict and the nuclear threshold – that is to increase stability and build a new sub- nuclear red line in this emerging era of a cyber peer competitor delivering a catastrophic attack. Despite the past decade of policy deliberations on new conventional global strike capabilities as part of a deterrence strategy, the situation today is such that the ultimate U.S. deterrent, including response against a catastrophic full spectrum cyber attack, is the nuclear triad– intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs), and nuclear-capable heavy bombers. The nuclear command and control (NC2) of the nuclear forces is comprised of systems, communication paths, and procedures associated with National Security Presidential Directive (NSPD)-28, which provides guidance to the Military Departments on the nature of redundant survivable communication paths to each nuclear delivery platform. Importantly, the definition of “survivability” in the traditional context of Nuclear C2 and forces usually referred to their credible ability to withstand a massive nuclear strike, with all of its attendant effects (including Electromagnetic Pulse (EMP)), and then provide a counter value retaliatory response. The Task Force expands the definition of survivability to include credible capability to withstand a Type V-VI cyber attack.

#### Chinese cyber offensive capabilities destroy Hegemony and cause china to attack Taiwan

Magnus Hjortdal, ’11 (researcher associated with CHINA-SEC, Centre for Military Studies at the University of Copenhagen. He holds an M.Sc. in Political Science from the University of Copenhagen and is owner of MH International Relations, which advises private and public institutions. Former Research Fellow at the Royal Danish Defense College “China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence”, Journal of strategic security)

Virtually all digital and electronic military systems can be attacked via cyberspace. Therefore, it is essential for a state to develop capabilities in this area if it wishes to challenge the present American hegemony. The interesting question then is whether China is developing capabilities in cyberspace in order to deter the United States.16 China's military strategists describe cyber capabilities as a powerful asymmetric opportunity in a deterrence strategy.19 Analysts consider that an "important theme in Chinese writings on computer-network operations (CNO) is the use of computer-network attack (CNA) as the spear- point of deterrence."20 CNA increases the enemy's costs to become too great to engage in warfare in the first place, which Chinese analysts judge to be essential for deterrence.21 This could, for example, leave China with the potential ability to deter the United States from intervening in a scenario concerning Taiwan. CNO is viewed as a focal point for the People's Liberation Army, but it is not clear how the actual capacity functions or precisely what conditions it works under.22¶ If a state with superpower potential (here China) is to create an opportunity to ascend militarily and politically in the international system, it would require an asymmetric deterrence capability such as that described here.23¶ It is said that the "most significant computer network attack is characterized as a pre-emption weapon to be used under the rubric of the rising Chinese strategy of [...] gaining mastery before the enemy has struck."24 Therefore, China, like other states seeking a similar capacity, has recruited massively within the hacker milieu inside China.25 Increasing resources in the PLA are being allocated to develop assets in relation to cyberspace.26 The improvements are visible: The PLA has established "information warfare" capabilities,27 with a special focus on cyber war- fare that, according to their doctrine, can be used in peacetime.28 Strategists from the PLA advocate the use of virus and hacker attacks that can paralyze and surprise its enemies.29

#### Heg solves great power war and dampens all global violence

Brooks et al 13

Stephen G. Brooks is Associate Professor of Government at Dartmouth College, John Ikenberry is the Albert G. Milbank Professor of Politics and International Affairs at Princeton University in the Department of Politics and the Woodrow Wilson School of Public and International Affairs. He is also a Global Eminence Scholar at Kyung Hee University, William C. Wohlforth is the Daniel Webster Professor in the Department of Government at Dartmouth College, International Security, Winter 2012/2013, "Don’t Come Home, America", MIT Press Journals

Assessing the Security Benefits of Deep Engagement Even if deep engagement’s costs are far less than retrenchment advocates claim, they are not worth bearing unless they yield greater benefits. We focus here on the strategy’s major security benefits; in the next section, we take up the wider payoffs of the United States’ security role for its interests in other realms, notably the global economy—an interaction relatively unexplored by international relations scholars. A core premise of deep engagement is that it prevents the emergence of a far more dangerous global security environment. For one thing, as noted above, the United States’ overseas presence gives it the leverage to restrain partners from taking provocative action. Perhaps more important, its core alliance commitments also deter states with aspirations to regional hegemony from contemplating expansion and make its partners more secure, reducing their incentive to adopt solutions to their security problems that threaten others and thus stoke security dilemmas. The contention that engaged U.S. power dampens the baleful effects of anarchy is consistent with influential variants of realist theory. Indeed, arguably the scariest portrayal of the war-prone world that would emerge absent the “American Pacifier” is provided in the works of John Mearsheimer, who forecasts dangerous multipolar regions replete with security competition, arms races, nuclear proliferation and associated preventive war temptations, regional rivalries, and even runs at regional hegemony and full-scale great power war.72 How do retrenchment advocates, the bulk of whom are realists, discount this benefit? Their arguments are complicated, but two capture most of the variation: (1) U.S. security guarantees are not necessary to prevent dangerous rivalries and conflict in Eurasia; or (2) prevention of rivalry and conflict in Eurasia is not a U.S. interest. Each response is connected to a different theory or set of theories, which makes sense given that the whole debate hinges on a complex future counterfactual (what would happen to Eurasia’s security setting if the United States truly disengaged?). Although a certain answer is impossible, each of these responses is nonetheless a weaker argument for retrenchment than advocates acknowledge. The first response flows from defensive realism as well as other international relations theories that discount the conflict-generating potential of anarchy under contemporary conditions.73 Defensive realists maintain that the high expected costs of territorial conquest, defense dominance, and an array of policies and practices that can be used credibly to signal benign intent, mean that Eurasia’s major states could manage regional multipolarity peacefully without the American pacifier. Retrenchment would be a bet on this scholarship, particularly in regions where the kinds of stabilizers that nonrealist theories point to—such as democratic governance or dense institutional linkages—are either absent or weakly present. There are three other major bodies of scholarship, however, that might give decisionmakers pause before making this bet. First is regional expertise. Needless to say, there is no consensus on the net security effects of U.S. withdrawal. Regarding each region, there are optimists and pessimists. Few experts expect a return of intense great power competition in a post-American Europe, but many doubt European governments will pay the political costs of increased EU defense cooperation and the budgetary costs of increasing military outlays.74 The result might be a Europe that is incapable of securing itself from various threats that could be destabilizing within the region and beyond (e.g., a regional conflict akin to the 1990s Balkan wars), lacks capacity for global security missions in which U.S. leaders might want European participation, and is vulnerable to the influence of outside rising powers. What about the other parts of Eurasia where the United States has a substantial military presence? Regarding the Middle East, the balance begins to swing toward pessimists concerned that states currently backed by Washington— notably Israel, Egypt, and Saudi Arabia—might take actions upon U.S. retrenchment that would intensify security dilemmas. And concerning East Asia, pessimism regarding the region’s prospects without the American pacifier is pronounced. Arguably the principal concern expressed by area experts is that Japan and South Korea are likely to obtain a nuclear capacity and increase their military commitments, which could stoke a destabilizing reaction from China. It is notable that during the Cold War, both South Korea and Taiwan moved to obtain a nuclear weapons capacity and were only constrained from doing so by a still-engaged United States.75 The second body of scholarship casting doubt on the bet on defensive realism’s sanguine portrayal is all of the research that undermines its conception of state preferences. Defensive realism’s optimism about what would happen if the United States retrenched is very much dependent on its particular—and highly restrictive—assumption about state preferences; once we relax this assumption, then much of its basis for optimism vanishes. Specifically, the prediction of post-American tranquility throughout Eurasia rests on the assumption that security is the only relevant state preference, with security defined narrowly in terms of protection from violent external attacks on the homeland. Under that assumption, the security problem is largely solved as soon as offense and defense are clearly distinguishable, and offense is extremely expensive relative to defense. Burgeoning research across the social and other sciences, however, undermines that core assumption: states have preferences not only for security but also for prestige, status, and other aims, and they engage in trade-offs among the various objectives.76 In addition, they define security not just in terms of territorial protection but in view of many and varied milieu goals. It follows that even states that are relatively secure may nevertheless engage in highly competitive behavior. Empirical studies show that this is indeed sometimes the case.77 In sum, a bet on a benign postretrenchment Eurasia is a bet that leaders of major countries will never allow these nonsecurity preferences to influence their strategic choices. To the degree that these bodies of scholarly knowledge have predictive leverage, U.S. retrenchment would result in a significant deterioration in the security environment in at least some of the world’s key regions. We have already mentioned the third, even more alarming body of scholarship. Offensive realism predicts that the withdrawal of the American pacifier will yield either a competitive regional multipolarity complete with associated insecurity, arms racing, crisis instability, nuclear proliferation, and the like, or bids for regional hegemony, which may be beyond the capacity of local great powers to contain (and which in any case would generate intensely competitive behavior, possibly including regional great power war). Hence it is unsurprising that retrenchment advocates are prone to focus on the second argument noted above: that avoiding wars and security dilemmas in the world’s core regions is not a U.S. national interest. Few doubt that the United States could survive the return of insecurity and conflict among Eurasian powers, but at what cost? Much of the work in this area has focused on the economic externalities of a renewed threat of insecurity and war, which we discuss below. Focusing on the pure security ramifications, there are two main reasons why decisionmakers may be rationally reluctant to run the retrenchment experiment. First, overall higher levels of conflict make the world a more dangerous place. Were Eurasia to return to higher levels of interstate military competition, one would see overall higher levels of military spending and innovation and a higher likelihood of competitive regional proxy wars and arming of client states—all of which would be concerning, in part because it would promote a faster diffusion of military power away from the United States. Greater regional insecurity could well feed proliferation cascades, as states such as Egypt, Japan, South Korea, Taiwan, and Saudi Arabia all might choose to create nuclear forces.78 It is unlikely that proliferation decisions by any of these actors would be the end of the game: they would likely generate pressure locally for more proliferation. Following Kenneth Waltz, many retrenchment advocates are proliferation optimists, assuming that nuclear deterrence solves the security problem.79 Usually carried out in dyadic terms, the debate over the stability of proliferation changes as the numbers go up. Proliferation optimism rests on assumptions of rationality and narrow security preferences. In social science, however, such assumptions are inevitably probabilistic. Optimists assume that most states are led by rational leaders, most will overcome organizational problems and resist the temptation to preempt before feared neighbors nuclearize, and most pursue only security and are risk averse. Confidence in such probabilistic assumptions declines if the world were to move from nine to twenty, thirty, or forty nuclear states. In addition, many of the other dangers noted by analysts who are concerned about the destabilizing effects of nuclear proliferation—including the risk of accidents and the prospects that some new nuclear powers will not have truly survivable forces—seem prone to go up as the number of nuclear powers grows.80 Moreover, the risk of “unforeseen crisis dynamics” that could spin out of control is also higher as the number of nuclear powers increases. Finally, add to these concerns the enhanced danger of nuclear leakage, and a world with overall higher levels of security competition becomes yet more worrisome. The argument that maintaining Eurasian peace is not a U.S. interest faces a second problem. On widely accepted realist assumptions, acknowledging that U.S. engagement preserves peace dramatically narrows the difference between retrenchment and deep engagement. For many supporters of retrenchment, the optimal strategy for a power such as the United States, which has attained regional hegemony and is separated from other great powers by oceans, is offshore balancing: stay over the horizon and “pass the buck” to local powers to do the dangerous work of counterbalancing any local rising power. The United States should commit to onshore balancing only when local balancing is likely to fail and a great power appears to be a credible contender for regional hegemony, as in the cases of Germany, Japan, and the Soviet Union in the midtwentieth century. The problem is that China’s rise puts the possibility of its attaining regional hegemony on the table, at least in the medium to long term. As Mearsheimer notes, “The United States will have to play a key role in countering China, because its Asian neighbors are not strong enough to do it by themselves.”81 Therefore, unless China’s rise stalls, “the United States is likely to act toward China similar to the way it behaved toward the Soviet Union during the Cold War.”82 It follows that the United States should take no action that would compromise its capacity to move to onshore balancing in the future. It will need to maintain key alliance relationships in Asia as well as the formidably expensive military capacity to intervene there. The implication is to get out of Iraq and Afghanistan, reduce the presence in Europe, and pivot to Asia— just what the United States is doing.83 In sum, the argument that U.S. security commitments are unnecessary for peace is countered by a lot of scholarship, including highly influential realist scholarship. In addition, the argument that Eurasian peace is unnecessary for U.S. security is weakened by the potential for a large number of nasty security consequences as well as the need to retain a latent onshore balancing capacity that dramatically reduces the savings retrenchment might bring. Moreover, switching between offshore and onshore balancing could well be difficult. Bringing together the thrust of many of the arguments discussed so far underlines the degree to which the case for retrenchment misses the underlying logic of the deep engagement strategy. By supplying reassurance, deterrence, and active management, the United States lowers security competition in the world’s key regions, thereby preventing the emergence of a hothouse atmosphere for growing new military capabilities. Alliance ties dissuade partners from ramping up and also provide leverage to prevent military transfers to potential rivals. On top of all this, the United States’ formidable military machine may deter entry by potential rivals. Current great power military expenditures as a percentage of GDP are at historical lows, and thus far other major powers have shied away from seeking to match top-end U.S. military capabilities. In addition, they have so far been careful to avoid attracting the “focused enmity” of the United States.84 All of the world’s most modern militaries are U.S. allies (America’s alliance system of more than sixty countries now accounts for some 80 percent of global military spending), and the gap between the U.S. military capability and that of potential rivals is by many measures growing rather than shrinking.85 In the end, therefore, deep engagement reduces security competition and does so in a way that slows the diffusion of power away from the United States. This in turn makes it easier to sustain the policy over the long term.

#### China is preparing for a cyber Spacewar- It ensures they beat the United States

Bill Gertz, 7-30-’13 (lectured on defense, national security, and media issues at the Defense Department’s National Security Leadership Program, Johns Hopkins University School of Advanced International Studies, the FBI National Academy, the National Defense University, and the CIA , media fellow at the Hoover Institution on War, Revolution and Peace at Stanford University, editor of the Washington Free Beacon. Prior to joining the Beacon he was a national security reporter, editor, and columnist for 27 years at the Washington Times. Bill is the author of six books, four of which were national bestsellers. ,“China’s Military Preparing for ‘People’s War’ in Cyberspace, Space” , The Washington Free Bacon, <http://freebeacon.com/china-military-preparing-for-peoples-war-in-cyberspace-space/>)

Translated report reveals high-tech plans for cyber attacks, anti-satellite strikes”, ¶ China’s military is preparing for war in cyberspace involving space attacks on satellites and the use of both military and civilian personnel for a digital “people’s war,” according to an internal Chinese defense report.¶ “As cyber technology continues to develop, cyber warfare has quietly begun,” the report concludes, noting that the ability to wage cyber war in space is vital for China’s military modernization.¶ According to the report, strategic warfare in the past was built on nuclear weapons. “But strategic warfare in the information age is cyber warfare,” the report said.¶ “With the reliance of information warfare on space, cyberspace will surely become a hot spot in the struggle for cyberspace control,” the report said.¶ The new details of Chinese plans for cyber and space warfare were revealed in a report “Study on Space Cyber Warfare” by four engineers working at a Chinese defense research center in Shanghai.¶ The report presents a rare inside look of one of Beijing’s most secret military programs: Cyber warfare plans against the United States in a future conflict.¶ “Cyber warfare is not limited to military personnel. All personnel with special knowledge and skills on information system may participate in the execution of cyber warfare. Cyber warfare may truly be called a people’s warfare,” the report says.¶ People’s War was first developed by China’s Communist founder Mao Zedong as a Marxist-Leninist insurgency and guerrilla warfare concept. The article provides evidence that Chinese military theorists are adapting Mao’s peasant uprising stratagem for a future conflict with the United States.¶ A defense official said the report was recently circulated in military and intelligence circles. Its publication came as a surprise to many in the Pentagon because in the past, U.S. translations of Chinese military documents on similar warfighting capabilities were not translated under a directive from policy officials seeking to prevent disclosure of Chinese military writings the officials feared could upset U.S.-China relations.¶ A Chinese government spokesman could not be reached for comment. However, Chinese spokesmen in the past have denied reports that China engages in cyber attacks.¶ The study links China’s space warfare development programs with its extensive cyber warfare capabilities. Both programs are considered “trump card” weapons that would allow a weaker China to defeat a militarily stronger United States in a conflict.¶ “Cyber warfare is an act of war that utilizes space technology; it combines space technology and cyber technology and maintains and seizes the control of cyberspace,” the study says.¶ Because cyberspace relies on satellites, “space will surely be the main battlefield of cyber warfare,” the report said.¶ Satellites and space vehicles are considered the “outer nodes” of cyber space and “are clear targets for attack and may be approached directly,” the report said, adding that ground-based cyberspace nodes are more concealed and thus more difficult to attack.¶ Additionally, satellites have limited defenses and anti-jamming capabilities, leaving them very vulnerable to attack.¶ The report reveals that China’s military, which controls the country’s rapidly growing space program, is preparing to conduct space-based cyber warfare—“cyber reconnaissance, jamming, and attack”—from space vehicles.¶ Space-based cyber warfare will include three categories: space cyber attack, space cyber defense, and space cyber support. The space cyber support involves reconnaissance, targeting, and intelligence gathering.¶ “A space cyber-attack is carried out using space technology and methods of hard kill and soft kill,” the report said. “It ensures its own control at will while at the same time uses cyberspace to disable, weaken, disrupt, and destroy the enemy’s cyber actions or cyber installations.”

**Extinction**

**Mitchell, et al 01** -Associate Professor of Communication and Director of Debate at the University of Pittsburgh

(Dr. Gordon, ISIS Briefing on Ballistic Missile Defence, “Missile Defence: Trans-Atlantic Diplomacy at a Crossroads”, No. 6 July, <http://www.isisuk.demon.co.uk/0811/isis/uk/bmd/no6.html>)

A buildup of space weapons might begin with noble intentions of 'peace through strength' deterrence, but this rationale glosses over the tendency that '… the presence of space weapons…will result in the increased likelihood of their use'.33 This drift toward usage is strengthened by a strategic fact elucidated by Frank Barnaby: when it comes to arming the heavens, 'anti-ballistic missiles and anti-satellite warfare technologies go hand-in-hand'.34 The interlocking nature of offense and defense in military space technology stems from the inherent 'dual capability' of spaceborne weapon components. As Marc Vidricaire, Delegation of Canada to the UN Conference on Disarmament, explains: 'If you want to intercept something in space, you could use the same capability to target something on land'. 35 To the extent that ballistic missile interceptors based in space can knock out enemy missiles in mid-flight, such interceptors can also be used as orbiting 'Death Stars', capable of sending munitions hurtling through the Earth's atmosphere. The dizzying speed of space warfare would introduce intense 'use or lose' pressure into strategic calculations, with the spectre of split-second attacks creating incentives to rig orbiting Death Stars with automated 'hair trigger' devices. In theory, this automation would enhance survivability of vulnerable space weapon platforms. However, by taking the decision to commit violence out of human hands and endowing computers with authority to make war, military planners could sow insidious seeds of accidental conflict. Yale sociologist Charles Perrow has analyzed 'complexly interactive, tightly coupled' industrial systems such as space weapons, which have many sophisticated components that all depend on each other's flawless performance. According to Perrow, this interlocking complexity makes it impossible to foresee all the different ways such systems could fail. As Perrow explains, '[t]he odd term "normal accident" is meant to signal that, given the system characteristics, multiple and unexpected interactions of failures are inevitable'.36Deployment of space weapons with pre-delegated authority to fire death rays or unleash killer projectiles would likely make war itself inevitable, given the susceptibility of such systems to 'normal accidents'. It is chilling to contemplate the possible effects of a space war. According to retired Lt. Col. Robert M. Bowman, 'even a tiny projectile reentering from space strikes the earth with such high velocity that it can do enormous damage — even more than would be done by a nuclear weapon of the same size!'. 37 In the same Star Wars technology touted as a quintessential tool of peace, defence analyst David Langford sees one of the most destabilizing offensive weapons ever conceived: 'One imagines dead cities of microwave-grilled people'.38 Given this unique potential for destruction, it is not hard to imagine that any nation subjected to space weapon attack would retaliate with maximum force, including use of nuclear, biological, and/or chemical weapons. An accidental war sparked by a computer glitch in space could plunge the world into the most destructive military conflict ever seen.

#### 2. We have passed the point of no return- China has no incentive to halt Cyber attacks

* China has too much to gain
* Diplomatic outreach has failed
* PLA is in control of offensive capabilities

Gordon G. Chang, 6-6-13 (JD Cornell law and Author of many books about China, “Cyber Détente with China”, World Affairs)

The ultimate goal is to arrive at understandings with the Chinese. As a “senior American official involved in the negotiations” told the paper, “We need to get some norms and rules.”¶ Actually, we have long passed that stage. What we need to do at this point is stop Chinese cyber intrusions, cyber attacks, and cyber espionage, all part of what many suspect to be the most extensive cyber campaign conducted by one country against another¶ Administration officials, according to the Times, say they do not expect the talks will result in an immediate and significant reduction in Chinese attacks. And as Stanford University’s Tim Junio told the AP, “China benefits too much by stealing intellectual property from the US, so it’s really hard to imagine anyone convincing them to slow down.”¶ So what is the purpose of further talks? It’s not as if the Obama administration has not already broached the subject with Beijing. The president and various officials had numerous conversations with the Chinese during the first term, but the attacks increased dramatically in the middle of last year. This year, Treasury Secretary Jack Lew, Secretary of State John Kerry, and Joint Chiefs Chairman Martin Dempsey have all trooped to Beijing to discuss the issue with no apparent result. Despite the persistent effort to establish a cooperative relationship, the People’s Liberation Army reportedly ramped up its cyber attacks sometime around the beginning of April.

#### 3. Dialogue fails- US and China views on cyber capabilities are too far apart to overcome

Diane Bartz and Paul Eckert, 7-14-11 (“U.S. and China face vast divide on cyber issues”, Reuters)

For two years, academic experts from the United States and China have quietly held talks on cyber-security, straining to establish rules of the road in a realm that has proven a persistent irritant between the world's two largest economies.¶ The informal discussions have yielded modest progress in areas such as cooperation to combat Internet fraud, where both Beijing and Washington have an incentive to work together, according to participants.¶ But mostly, the talks appear to have exposed a wide gap between the United States and China over almost everything virtual: policing computer networks, moderating cyber warfare, even controlling information.¶ China's contrasting view of cyber security was made clear as soon as the United States began discussing the need to protect computer networks, James Mulvenon, a China expert at the Defense Group Inc, told a recent Washington conference.¶ China wanted to talk about censorship. "The Chinese came back immediately and said no, no, no, we want to talk about information security, which is both protecting the network and policing the content on the network," Mulvenon said.¶ "Right from the outset, we were talking past one another," he added.