# 1NC

## Off

### 1

#### TOPICALITY

#### A. Restrictions are prohibitions on action --- excludes conditions

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

3. The ordinary definition of the term "restrictions" also does not include the reporting and monitoring or supervising terms and conditions that are included in the 2001 Stipulation.

Black's Law Dictionary, 'fifth edition,(1979) defines "restriction" as;

A limitation often imposed in a deed or lease respecting the use to which the property may be put. The term "restrict' is also cross referenced with the term "restrain." Restrain is defined as; To limit, confine, abridge, narrow down, restrict, obstruct, impede, hinder, stay, destroy. To prohibit from action; to put compulsion on; to restrict; to hold or press back. To keep in check; to hold back from acting, proceeding, or advancing, either by physical or moral force, or by interposing obstacle, to repress or suppress, to curb.

In contrast, the terms "supervise" and "supervisor" are defined as; To have general oversight over, to superintend or to inspect. See Supervisor. A surveyor or overseer. . . In a broad sense, one having authority over others, to superintend and direct. The term "supervisor" means an individual having authority, in the interest of the employer, to hire, transfer, suspend, layoff, recall, promote, discharge, assign, reward, or discipline other employees, or responsibility to direct them, or to adjust their grievances, or effectively to recommend such action, if in connection with the foregoing the exercise of such authority is not of a merely routine or clerical nature, but required the use of independent judgment.

Comparing the above definitions, it is clear that the definition of "restriction" is very different from the definition of "supervision"-very few of the same words are used to explain or define the different terms. In his 2001 stipulation, Mr. Kincheloe essentially agreed to some supervision conditions, but he did not agree to restrict his license.

#### B. Voting Issue---Precision—restrictions must be a distinct term for debate to occur

Heinze-Senior Lecturer Law, University of London-3

(Senior Lecturer in Law, University of London, Queen Mary. He has held fellowships from the Fulbright Foundation and the French and German governments. He teaches Legal Theory, Constitutional Law, Human Rights and Public International Law. JD Harvard) 2003 “The Logic of Liberal Rights A study in the formal analysis of legal discourse” http://mey.homelinux.org/companions/Eric%20Heinze/The%20Logic%20of%20Liberal%20Rights\_%20A%20Study%20in%20%20%28839%29/The%20Logic%20of%20Liberal%20Rights\_%20A%20Study%20in%20%20-%20Eric%20Heinze.pdf

Variety of ‘restrictions’

The term ‘restriction’, defined so broadly, embraces any number of familiar concepts: ‘deprivation’, ‘denial’, ‘encroachment’, ‘incursion’, ‘infringement’, ‘interference’, ‘limitation’, ‘regulation’. Those terms commonly comport differences in meaning or nuance, and are not all interchangeable in standard legal usage. For example, a ‘deprivation’ may be distinguished from a ‘limitation’ or ‘regulation’ in order to denote a full denial of a right (e.g. where private property is wholly appropriated by the state 16 Agents without compensation) as opposed to a partial constraint (e.g. where discrete restrictions are imposed on the use of property which nonetheless remains profitably usable). Similarly, distinctions between acts and omissions can leave the blanket term ‘restriction’ sounding inapposite when applied to an omission: if a state is accused of not doing enough to give effect to a right, we would not colloquially refer to such inaction as a ‘restriction’. Moreover, in a case of extreme abuse, such as extrajudicial killing or torture, it might sound banal to speak merely of a ‘restriction’ on the corresponding right. However, the term ‘restriction’ will be used to include all of those circumstances, in so far as they all comport a purpose or effect of extinguishing or diminishing the right-seeker’s enjoyment of an asserted right. (The only significant distinction which will be drawn will be between that concept of ‘restriction’ and the concept of ‘breach’ or ‘violation’. The terms ‘breach’ or ‘violation’ will be used to denote a judicial determination about the legality of the restriction.6) Such an axiom may seem unwelcome, in so far as it obliterates subtleties which one would have thought to be useful in law. It must be stressed that we are seeking to eliminate that variety of terms not for all purposes, but only for the very narrow purposes of a formal model, for which any distinctions among them are irrelevant.

### 2

#### COUNTERPLAN

#### The President of the United States should give a prompt and full account to Congress of every significant use of cyber weapons, begin an interagency process of doctrine-formation for the offensive use of cyber weapons, and publish the results.

#### The executive branch of the United States should publish non-classified descriptions of the doctrine that governs cyber attacks.

#### CP clears up any legal confusion by causing agency buy in

**Young, Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence, 2010**

(Mark, “National Cyber Doctrine: The Missing Link in the Application of American Cyber Power”, <http://jnslp.com/wp-content/uploads/2010/08/12_Young.pdf>, ldg)

Whether directed by the Cyber Command or by other government agencies, the employment of U.S. power in the cyber domain requires a rapid paradigm shift uncharacteristic of the DoD. To accelerate this shift, the national security community needs a new doctrine to provide the fundamental principles by which executive branch departments and agencies can ensure the freedom of U.S. action in cyberspace. The DoD controls most of the expertise in computer network operations and is well positioned to lead the national security community in establishing U.S. cyber policies and doctrines. It cannot do this alone, however. This article argues that a national cyber doctrine is necessary. It is the link between strategy and the execution of the missions of the national security sector. Doctrine may traditionally be a military notion, but agencies are acknowledging the wisdom of establishing guiding principles. A national cyber doctrine can be a vehicle used to define the roles of departments and agencies for the entire U.S. government. In contrast to a presidential executive order or a National Security Council directive, a doctrine is developed in an openly collaborative fashion. Author David Kilcullen’s observations regarding counterinsurgency collaboration are also applicable to the development of a national cyber doctrine: “To be effective, we must marshal not only all agencies of the [U.S. government], but also all agencies of a host nation, multiple foreign allies and coalition partners, international institutions, nongovernment organizations . . . international and local media, religious and community groups, and charities and businesses.”5 The DoD has developed an extensive collection of doctrines that guide military operations, but there is no doctrine to guide applications of national cyberpower. Cyber Command’s missions are being formulated without an adequate doctrine to define the strategic context, establish the fundamentals of cyberpower, or debate issues concerning computer network operations. The Secretary of Defense memorandum ordering the establishment of the Cyber Command mandates the synchronization of cyberwar effects “across the global security environment as well as providing support to civil authorities and international partners.”6 Coordination of interagency cyber operations and cooperation with civil and foreign partners are the types of activities for which doctrine is well suited. Other DoD doctrines govern similar activities in the sea, air, land, and space domains.7 While the DoD has no authority to enforce military doctrines outside of the Department, sound principles developed with the full participation of interagency partners will be followed due to their utility and effectiveness, not because of coercion. As has been observed, “You cannot command what you do not control.”8 Therefore the doctrine should foster a unified effort across the entire U.S. national security community. Its success will depend “on a shared diagnosis of the problem, platforms for collaboration, information sharing and deconfliction.”9 The current U.S. counterinsurgency doctrine provides a model of how an inclusive doctrine can gain acceptance throughout the national security community. The development of the counterinsurgency doctrine was directed by then Lieutenant General David Petraeus after his return from his second tour of duty in Iraq in 2004. Petraeus brought together traditional and nontraditional partners to devise fundamental principles by which to address an extremely difficult set of combat circumstances. Some “military officers questioned the utility of the representatives from nongovernment organizations (NGOs) and the media, but they proved to be the most insightful of commentators.”10 The application of cyberpower is just as complicated as counterinsurgency operations, and in many ways it is more complicated. The success of the counterinsurgency doctrine, produced by a group of collaborators that included those typically excluded from the development of military doctrine, shows the wisdom of an inclusive approach. By creating a diverse community of interest to draft cyber doctrine, the national security community can more adequately address long-standing questions about U.S. activities in cyberspace: How should the government act to protect privacy while undertaking robust efforts to prevent cyber attacks? How will the Cyber Command support the strategic goal of defending the U.S. economy? What are the likely consequences of and who will be responsible for responding to a successful cyber attack that results in loss of life or destruction of property? Doctrines are developed by a process that can answer these policy questions, even if only on a temporary basis. The Chairman of the Joint Chiefs of Staff has developed specific procedures for the initiation, development, approval, and maintenance of joint doctrine projects. The process requires active involvement by all principal users of joint doctrine. The process also includes a means to work towards consensus among doctrine developers as well as a method for resolving key issues or divergent views.1 In the same way that the drafting of the Army Counterinsurgency Field Manual assembled “journalists, human rights advocates, academics, and practitioners of counterinsurgency”12 – an unusual group to develop an Army doctrine – the development of a national cyber doctrine can encourage horizontal integration of the commercial, government, academic, and civil liberties sectors to enhance the rigor of national security decision making in the cyber domain. It will focus the application of U.S. cyberpower. “Cyberpower” is defined here as “the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power.”13 With the dearth of nonmilitary cyber capacity, the Cyber Command will become the default organization to confront threats affecting the diverse networks on which U.S. defense and the global market rely. Although the command is currently restricted to operations on DoD networks, it is easily foreseeable that the command may be called upon to take action on other networks in times of crisis. With the establishment of the Cyber Command and the prioritization of cybersecurity,14 national strategy must be effectively communicated and implemented. A doctrine should be in effect before a national crisis occurs so that appropriate constitutional management of U.S. power is maintained. “When strategy is freed from effective political control, it becomes mindless and heedless. . . .”15 What was true of nuclear weapons during the Cold War is also true of network attack in the cyber age. Modern technology that created the bombs that were dropped on Hiroshima and Nagasaki and the more sophisticated ones that have in the years since 1945 aroused visions of conflict between the superpowers that would end in mutual annihilation, is now, in its restless energy, creating new kinds of weapons that may in time make nuclear war obsolete and recreate the conditions in which the principles of classical strategy were formulated.16 Historians Gordon Craig and Felix Gilbert were arguing that point in reference to precision-guided munitions, but cyber war might have a similar potential to make deterrence with nuclear weapons and classic strategic thought obsolete. Nuclear deterrence during the Cold War contemplated an automated response to attack by the Soviet Union, and similar automated responses to cyber attack are now being debated. Computer network attacks happen at the speed of light, so future threats require an equally rapid and perhaps automatic response. Portals can be programmed to disconnect automatically from the network when known hostile signatures are detected. The nature of network attacks makes a well reviewed cyber doctrine particularly important, since national security leaders will have little time to consult with the National Security Council or the Commander in Chief when faced with an attack that could devastate the national economy, corrupt the flow of commerce, or disrupt military supply chains. Due to technical challenges, counterstrikes remain a time-consuming proposition. Disruption of a cyber attack is more easily achieved but may not be accomplished in time to protect critical data or national security systems. The risks in removing human judgment from the network operations decision cycle are significant. For example, in 1988, the automated Aegis computer system on board the U.S.S. Vincennes registered Iran Air flight 655 as a hostile Iranian F-14 fighter aircraft. Though the hard data were telling the human crew that the plane wasn’t a fighter jet, they trusted the computer more. Aegis was in semi-automatic mode, giving it the least amount of autonomy, but not one of the 18 sailors and officers in the command crew challenged the computer’s wisdom. They authorized it to fire.17 This semi-automatic response killed 290 passengers. Although there are problems associated with attributing the source of cyber attacks, cyber weapons may already be under development. “One can argue plausibly that the autonomy of the political leadership begins to shrink from the moment that it authorizes the expenditure of national resources on this or that kind of weapons research or the production of this or that kind of bomber, missile, or submarine.”18 Some claim that large amounts have already been spent on the research and development of cyber weapons. The current doctrine is inadequate to the task levied on the Cyber Command. Only through a deliberate development process will the risks of applying U.S. cyberpower against cyber threats be mitigated. This process will ensure that the autonomy of U.S. political leadership and the values expressed in the use of U.S. force or influence are maintained.

### 3

#### Trade Promotion Authority

#### Text: The President of the United States should substantially increase lobbying and persuasion efforts, using available political resources, on behalf of Congressional enactment of Trade Promotion Authority.

#### Obama applying PC is key to TPA and TPP---key to US leadership in Asia

**Barfield, AEI resident scholar, 3-4-14**

(Claude, “Domestic politics slow down Obama’s ‘fast track’ plan to free trade”, <http://www.eastasiaforum.org/2014/03/04/domestic-politics-slow-down-obamas-fast-track-plan-to-free-trade/>, ldg)

Symbolically, however, it is the TPP negotiations and the drive to conclude these negotiations expeditiously that stands as the focal point of the pivot. A successful TPP and the resulting benefits to US businesses and workers will form the economic anchor to persuade Congress and the public that Asia’s security and economic well-being is inextricably linked to US security and prosperity. There are now 12 Asia Pacific nations negotiating the TPP, with another, South Korea, standing in the wings. The membership (adding South Korea) represents over 40 per cent of world GDP and more than a third of total world trade. Substantively, the TPP aims to create a ‘gold standard’ agreement: meaning that it will set the standard for a 21st century trade regime, including rules for services and investment, intellectual property, health and safety, state-owned enterprises, regulatory transparency and due process, labour and the environment. The key tradeoffs will include balancing the 21st century demands of the US and others against the more traditional 20th century priorities of developing TPP nations in areas like textiles, clothes, shoes, sugar, cotton and dairy products. The TPP has reached endgame negotiations, where all twelve nations are expected to finally put their bottom line positions on the table. And it is here at this crucial juncture that US domestic politics have crashed the party with as yet incalculable consequences. In his State of the Union address, President Obama called upon Congress to give him so-called trade-promotion authority (expedited rules for Congress to ratify FTAs) in order to conclude the TPP and move forward on parallel negotiations with Europe. Within 24 hours of Obama’s plea, the Democratic majority leader Harry Reid defied the president by signalling opposition to granting trade-promotion authority and warning the administration not to send up such a bill. In the ‘all politics is local’ tradition, Reid’s eye is focused narrowly on holding the Senate in the midterm elections and retaining key support from union and environmental groups who strongly oppose the TPP. This leaves the ball squarely in Obama’s court: he must quickly decide whether to tackle Reid head on and mobilise other Democratic senators against their own majority leader — or attempt to get an ironclad agreement from Reid to allow a vote on TPP in a lame duck session after the election. He must also forge an alliance with congressional Republicans who — whatever Reid decides — will provide the majority of votes for TPP in both houses of Congress. Other TPP nations will be closely monitoring the administration’s decisions and Congress’ in coming weeks — as a guide to their own negotiating positions. The outcome of this debate and political battle will have far-reaching consequences. The failure of the US to continue to lead in a successful conclusion of the TPP would likely destroy the possibility of a broader US-led and anchored Trans-Pacific regional economic structure. In its place, the Chinese are already assiduously pushing for a narrower East Asian architecture that does not include the US. And well beyond the economic consequences, future US diplomatic and security leadership and alliances in Asia will be severely jeopardised as US regional allies come to doubt its ability to overcome local forces in order to pursue vital national interests.

#### The plan expends capital on a separate war powers issue–it’s immediate and forces a trade-off

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

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

#### Leadership key to prevent Asian war

**Goh, University of Oxford International Relations lecturer, 2008**

(Evelyn, International Relations of the Asia-Pacific, "Hierarchy and the role of the United States in the East Asian security order," irap.oxfordjournals.org/content/8/3/353.full, ldg)

The centrality of these mutual processes of assurance and deference means that the stability of a hierarchical order is fundamentally related to a collective sense of certainty about the leadership and order of the hierarchy. This certainty is rooted in a combination of material calculations – smaller states' assurance that the expected costs of the dominant state conquering them would be higher than the benefits – and ideational convictions – the sense of legitimacy, derived from shared values and norms that accompanies the super-ordinate state's authority in the social order. The empirical analysis in the next section shows that regional stability in East Asia in the post-Second World War years can be correlated to the degree of collective certainty about the US-led regional hierarchy. East Asian stability and instability has been determined by U.S. assurances, self-confidence, and commitment to maintaining its primary position in the regional hierarchy; **the perceptions** and confidence **of regional states about US commitment**; and the reactions of subordinate states in the region to the varied challengers to the regional hierarchical order. 3 Hierarchy and the United States in East Asia after 1945 The U.S.' involvement has had a profound impact on [the] history of East Asia's development. America maintained an ‘open-door’ to China, twice transformed Japan, and spilt blood to hold the line against aggression and communism. The U.S. constructed and maintained the post-World War II international order that allowed East Asia to flourish. America's victory in the Cold War and its technology driving the new economy are continued influences. In the strategic sense, therefore, the U.S. is very much a part of East Asia. It has been, and still is, a **positive force for stability and prosperity**.5 The United States has been indisputably the preponderant power in East Asia since 1945. Throughout much of post-war Asia, it has largely been acknowledged as the central, or dominant, state with no local territorial ambitions. Washington's key allies which institutionalize this benign view through their defense treaties, but unallied countries such as those in Southeast Asia, and, more recently India, also see it as an honest broker and offshore balancer (Goh, 2000; Layne, 1997). The communist countries in the region, which have experienced containment, subversion, and invasion by US forces, have good reason to disagree. But even China has accepted the idea of the United States as a stabilizing force in the region since the 1970s.6 Certainly, this is less controversial a claim than that of other scholars who have argued for such a dominant position for China (Acharya, 2003/04). The United States has also been intimately involved in key regional conflicts in East Asia after 1945. It intervened crucially on the side of the Allied powers to win the war, and was a core player in the peace settlement for the Pacific theatre, especially in the occupation and rehabilitation of Japan. During the Cold War, Washington intervened in hot wars and led in containing communism, and after the Cold War, it has been critical in managing the main regional conflicts on the Korean Peninsula and across the Taiwan Straits.7 Indirectly, it has provided a regional security umbrella, which may have dampened or limited the regional effects of other bilateral or domestic conflicts, such as the South China Sea territorial disputes.8 The United States has also earned it dominant position at the top of the East Asian hierarchy because of its critical economic role, in providing vital market access to Japan and the other Asian ‘tiger’ economies for their remarkable development, and in continuing to provide significant investments to the region. Its socio-economic and political model has become even more attractive in the region after the dissolution of the Soviet model at end of the Cold War. In every way, the United States is the preponderant power and gatekeeper of the great power club. Furthermore, the US-led hierarchy in East Asia since 1945 reflects our expectations of regional strategic behavioral in such an order. First, the centrality of acquiescence by subordinate states is clear: most of the main Asian states, with the partial exception of China, are either US allies or are cultivating closer security relations with Washington. As discussed below, even China today is not challenging but accommodating the interests of United States in the region. Second, the East Asian security order has been most unstable when the United States' commitment to the region and thus its position at the top of the hierarchy was uncertain and/or challenged. The following analysis traces the East Asian security order through three periods after the Second World War. In the 1945–70 period, the United States consolidated its post-war dominance in the region and established a hierarchy of non-Communist bulwark states, and regional order was stable in spite of Communist challenges. After 1970, as China and the Soviet Union exerted more regional influence in the wake of the post-Vietnam American drawdown, the US preponderance was challenged and the regional hierarchical order destabilized as subordinate powers jostled for position and adopted a range of balancing and insurance policies. After the end of the Cold War, Asia's security order has been evolving again, with smaller states trying to bolster the US preponderance while facilitating the reconstituting of a hierarchical order that includes China, Japan, and India. The East Asian hierarchy is notable for its enduring layered nature. Within this US-dominated order, Japan has traditionally held the second-highest rank because of its alliance and strategic affinity with the United States, but after 1972, China entered the top ranks of this hierarchy and increasingly laid claims to the second position. During the Cold War, a looser Soviet-led hierarchical system did exist alongside the US-led hierarchy, but this disintegrated after 1972 and disappeared after 1989. In the post-Cold War period, the main challenge appears to be how to contain the incipient competition for the primary position in this hierarchy between the United States and China, but also how to manage potential contests over hierarchical rank between Japan, India, and China. 3.1 Consolidating U.S. preponderance, 1945–1970 After the Second World War, the United States emerged as the world's greatest power: the size of its economy was three times that of Russia and more than five times that of Britain after the war; it held two-thirds of the world's gold reserves and three-quarters of its invested capital, and more than half the world's manufacturing capacity (Leffler, 1992). This status quo preponderance was, however, perceived to have been threatened by the USSR's ascension to superpower status, especially in terms of rising Soviet military influence in Eastern Europe and Northeast Asia. While post-war American efforts to rally against Soviet geopolitical aspirations were concentrated in Europe and the Northern Tier, it was the Korean War that marked the beginning of the use of military force to counter communist expansion on a global scale.9 The American decision to cross the 38th parallel was an attempt to secure preponderant power in East Asia, and establish a global containment posture against Moscow. China's entry into the Korean War launched its own quest to become a great power, and was, in American eyes, a corollary to Soviet expansionist aims to establish international communist domination and push back the US power from key geostrategic strong points on the Eurasian continent. The Korean War decisively opened up Asia as an enduring theatre of the Cold War, in which future American policy calculations would have to take into account China as well as the Soviet Union. Because of its dominant power, the United States was able to throw a security cordon around China to contain Washington's growing fear of Asian revolution influenced by Chinese communists. This entailed primarily recognition and a commitment to the defense of the Republic of China on Taiwan, and an early end to the occupation of Japan, a peace and security treaty granting American forces’ extensive base rights in the post-Occupation period, and American sponsorship of Japanese re-development. Washington also signed security pacts with the Philippines, New Zealand, and Australia, and entered into defensive treaties with the Republic of Korea (1953) and Taiwan (1954). The Southeast Asia Treaty Organization was also created (in late 1954) and was comprised of non-communist states within and outside the Asian region. Moreover, the United States placed restrictions on European and Japanese economic relations with China (Schaller, 1985). In these ways, the US strategy in the 1950s constituted the regional order at a time of post-war weakness of established East Asian states and decolonization of new states. The US resources, actions, and relationships helped establish a hierarchy with the United States firmly at the top. Its role in ending the Pacific war had already guaranteed it a vital role in post-war regional reconstruction, but by entering the Korean War, Washington further established security priorities in Northeast Asia, identified the other important major states in the region, and which it would make friends and enemies of in the unfolding global ideological contest. Thus, Japan, South Korea, and Taiwan were incorporated into the US-led hierarchy by virtue of their strategic importance, and were extended hierarchical assurance by means of US security guarantees and economic aid and access for reconstruction and development. In return, these states deferred to US preponderance and leadership by their strategic dependence and clientalism, and by gradually evolving into bastions of capitalist democracies. In contrast, the opening of the East Asian front of the Cold War in Korea created as challengers to US preponderance and hierarchy the Soviet Union, China, North Korea, and later the Indo-Chinese states. This communist bloc was a competing regional hierarchy of sorts, but one that was less defined because of the lack of clarity about rank ordering within the region, and thus continually subject to internal conflict and external disruption.10 Yet, American dominance in East Asia was sustained in this period: even though there were many conflicts, the regional order was relatively stable because US commitment to sustaining its hierarchical preponderance was clear. This was seen especially in the offshore islands crises in the late 1950s, during which Chinese claims over islands near Taiwan met with little or no Soviet support, and the main incentive for Chinese restraint was the asymmetrical nuclear capability possessed by the United States (Chang, 1990). In the 1960s, the United States continued its policy of active containment in East Asia in the form of growing intervention in the Vietnam conflict, culminating in air strikes and a land invasion in 1965. The application of this grand strategy to preserve the US regional and global preponderance to Vietnam in the 1960s, however, revealed new constraints of American power in terms of the limits of US public tolerance for protracted and destructive warfare in a distant land against an ideological enemy. 3.2 Hierarchical uncertainty and regional instability, 1970–90 The unwinnable war in Vietnam led to a transition period in East Asia marked by grave uncertainty about the global balance of power between the United States and USSR, and about the stability of the regional hierarchy. In his 1969 Guam Doctrine, Richard Nixon declared a scaling-down of US global aspirations. The United States was now a Pacific power with reservations; it had no intention of becoming directly involved again in any regional conflict in Asia, although it would support allies and friends with military assistance and diplomatic backing. Washington's unsuccessful and draining war in Vietnam had already undermined regional confidence in its continued willingness to shoulder the costs of regional primacy, and the Guam Doctrine was interpreted by Asian states as signaling the potential abandonment of American regional leadership all together. This acute uncertainty about the US position at the top of the regional hierarchy led to instability and war, as regional states engaged in self-help and balance of power politics more actively than at any time since the end of the Second World War. The first significant change was that China became a much more prominent actor by being co-opted into the high levels of the US-led hierarchy. The bipolar superpower conflict underwent dramatic changes in the 1970s: the pre-existing Sino-Soviet strategic enmity intensified into a border war in 1969, and in response to the Nixon administration's overtures, China ‘defected’ from its alliance with the Soviet Union to a rapprochement and normalization with the US. The United States, meanwhile, sought a parallel détente with the Soviet Union. A strategic triangle thus emerged, with the United States as the pivotal player enjoying relatively good relations with the other two (Kissinger, 1977; Nixon, 1978). With the congruence between ideology and strategic affinity broken, the Cold War assumed an explicit realpolitik hue, focusing on state interests and capabilities. Within Asia though, the power competition developed along the Sino-Soviet fault-line, with the United States and China on the same side. The Sino-American rapprochement did not encourage Soviet conciliation, and instead heightened Soviet insecurity. Thus, one of the immediate Soviet reactions after the rapprochement was to encourage India to facilitate the breakup of Pakistan, a staunch ally of China. This forced the American ‘tilt toward Pakistan’ in 1971 in order to prevent India from destroying the Pakistani army and endangering China (Goh, 2004, pp.185–192). The Sino-Japanese rapprochement and Treaty of Peace and Friendship in 1978 further exacerbated the Soviet sense of isolation and encirclement. Moscow now saw itself as confronted in East Asia by an alliance of the most populous, most economically successful, and most powerful states, without the buffer of a friendly China to make up for the traditionally loose Soviet Far Eastern commitment (Solomon, 1982). This in turn contributed to more aggressive Soviet policy, such as the invasion of Afghanistan and the decision to support Vietnam (Yahuda, 1996). The Soviets granted Vietnam membership in COMECON and signed a formal friendship treaty with that Southeast Asian country in late 1978, which provided support for the Vietnamese invasion of Cambodia. China, in turn, was emboldened by its normalized relationship with the United States to attack Vietnam to ‘teach it a lesson’ for the Cambodian infringement (Ross, 1993). Thus, by 1979, strategic enmities in East Asia followed the Sino-Soviet divide, which was reinforced by the breakdown of the Soviet-American détente. Without the direct intervention of the United States, this pattern of conflict remained localized, centered on Indochina and regional powers. Hanoi and Moscow had taken advantage of the declining US commitment to the region to push Vietnam's bid for hegemony in Indochina; and upon its cooption into the regional hierarchy, China had taken punitive military action against Vietnam to try to uphold the regional status quo. The destabilizing effects of uncertainty about continued US dominance in the regional hierarchy was further evinced in Southeast Asia by the formation of the ASEAN in 1967. This collection of small, non-communist states saw their existing policy of bandwagoning with the United States as unsustainable, and chose to band together in a diplomatic community to help ensure their autonomy and security (Leifer, 1989). The stalemate that materialized over the ensuing decade featured internationally isolated Vietnam depending upon the Soviet Union to sustain its dominant position in Cambodia while being confronted in the margins by resistance forces backed by China, the United States, and ASEAN countries. It is possible to argue that for the Asian region as a whole, the late 1970s and 1980s saw a relatively stable pro-Western power equilibrium: apart from Vietnam, Laos, and Cambodia, almost all the other countries in the region, including China, were tied into a Western alliance system in one way or another (Zagoria, 1982). Yet, the United States receded as the central state in the regional order during this time. In South Asia, as a result of the 1971 war and Pakistani fragmentation, a strengthened India moved closer to the USSR by signing a bilateral Friendship Treaty. In East Asia, China (as a US partner) and Vietnam (with Soviet backing) became the key protagonists on the regional stage, while ASEAN also developed a greater role with its international diplomatic activism. During this unstable period, the regional hierarchy was in flux as the United States withdrew from its dominant position; China was gradually but uncertainly incorporated into the regional hierarchy and was the main protagonist in the conflict with communist Vietnam and the Soviet Union; while Indochina and ASEAN developed their own dynamics outside of the shifting regional great power hierarchy. 3.3 Reconstituting hierarchical order after 1990 The end of the Cold War brought about the most significant transition in the global and Asian regional orders. Globally, the United States remained the only superpower with resources that outstripped those of any other single state. In Asia, China's position continued to strengthen, as concerns grew about the further decline of American strategic interest in the region. The 1990s are notable as a decade in which regional actors become most prominent in actively trying to reconstitute the regional hierarchy, to maneuver the United States firmly back into a position of regional primacy. This activism on the part of both important potential challengers and strategically less powerful regional states is a strong indication of the mutually constructed, consensual nature of the preferred hierarchical order. The post-Cold War uncertainty about American commitment to Asia particularly affected Japan and Southeast Asia. Both reacted by trying to retain the dominant US military presence and its important economic and political influence in the region. The Japan–United States alliance could have been undermined after more than a decade of trade conflicts and bilateral tension over charges that it was free-riding on the US security guarantee, and by the deepening uncertainty surrounding the US commitment to East Asia in the early 1990s. Instead, the US policy-makers decided to strengthen their strategic ties as Tokyo likewise chose to enhance its alliance with Washington. Japan's decision reflected a fear of abandonment by the United States and a desire to continue to bind the US to the bilateral security guarantee and to its dominant position in the region. At the most pragmatic level, given the domestic political difficulties involved in constitutional amendment and in the face of security threats from North Korea and China, Japan needed to maintain its special relationship with the United States. The April 1996 Japan–United States Joint Declaration on Security and September 1997 Revised Guidelines for Japan–U.S. Defense Cooperation allowed for the expansion of security cooperation, especially in supplies and services to ‘situations in areas surrounding Japan that will have an important influence on Japan's peace and security’ (see guidelines available at http://www.mofa.go.jp/region/n-america/us/security/guideline2.html). This extended the Japanese Self-Defense Forces' mandate beyond defending the home islands against direct attack, to more generally enhancing regional stability. More recently, after the 9/11 terrorist attacks, the Japanese Diet passed an emergency law in October 2001 that allowed the Japanese military to provide logistical support for United States and others in anti-terrorist missions, paving the way for Japan to provide support functions in campaigns in Afghanistan and Iraq.11 These were decisions calculated to buttress the Japanese alliance with the United States, to assure the continuity of the US commitment to national and regional security in spite of changing strategic circumstances (Katzenstein and Okawara, 2004). This intensification of the United States–Japan alliance critically helps to underwrite the United States' position as the dominant state in the regional hierarchy in two ways: it enhances U.S. power projection both in the region and in the world; and it is a powerful symbol of the acquiescence and subordination of the main potential challenger for regional hegemony to the US domination (Nau, 2003, pp. 224–230). Thus, Japan's continued hierarchical deference to the United States vitally underpins its super-ordinate position in the region. Owing to their peripheral location and relative lack of strategic importance to the United States, most Southeast Asian states were even more concerned about a potential American withdrawal after the Cold War in the face of a rising China. Much has been written about Southeast Asian policies of engagement with China to mediate the China threat (Ba, 2003; Shambaugh, 2004/5; Goh, 2007). At the same time, however, they have tried selectively to harness the superior US force in the region to deter the potential aggression from China. Two Southeast Asian states – the Philippines and Thailand – are formal allies of the United States, but neither plays host to American bases. Instead, they and a number of non-allied countries, including Singapore, Malaysia, and Indonesia – provide military facilities and access to the US naval and air forces. They also participate in bilateral and multilateral joint exercises with the US forces, and some countries have preferential military supply relations with the Americans (Goh, 2007/08, pp. 113–157). They further demonstrate hierarchical deference and support by additionally tying themselves more closely to the United States in the short- to medium-term fight against terrorism, to help anchor the United States in the region as a counterweight against China (Goh, 2005b; Khong, 2004). Rather than encouraging the United States to target its forces directly against China, though, the goal is to further buttress American military superiority in the region, or to demonstrate the ability to harness it in ways required to act as a general deterrence to Chinese (or other) aggression.12 At the same time, they also seek to strengthen their individual military capabilities by attracting the US military aid and training, trade, and economic assistance. Southeast Asian strategies go beyond simple bandwagoning with the dominant power, though, because they pay great attention also to engaging China and other regional powers. For instance, ASEAN's efforts at developing closer economic relations, generating more sustained political/security dialogue, and establishing military exchanges and relationships, are aimed not only at China, but also at the United States, as well as other major regional players such as Japan, South Korea, and India. By enmeshing the United States, China, and other large powers into regional institutions and norms, Southeast Asian states want to involve them actively in the region by means of good political relationships, deep and preferential economic exchanges, and some degree of defense dialogue and exchange. Southeast Asian policy-makers believe that this creates greater long-term stability in the region (Acharya, 2002). The aim is not to produce a multipolar balance of power in the conventional sense, because the major powers involved here are not all equally formidable. Rather, many Southeast Asian countries prefer to retain the United States as the preponderant superpower, with China as the regional great power, and India and Japan as second-tier regional powers (Goh, 2007/08). This strategic vision reflects a surprising degree of activism on the part of subordinate states not only in helping to sustain hierarchical leadership, but also to innovate so as to buttress regional order. The key innovation here is to try to facilitate the further integration of China into the regional hierarchy, to lend more direction and substance to this process which began in the 1970s. The most important element though is how to integrate China at a level below that of the United States, that is, as the second ranked but still subordinate power. For the last 50 years, the East Asian hierarchy was US-dominated, with the rank order of states within the hierarchy dependent chiefly on alliance or other defense relations with the United States, while communist challengers were excluded from the hierarchy altogether. Now, China has to be integrated on the basis of its economic, political, and military strength, and perhaps more importantly, its right to be a leading power, as perceived by states the region. This model of regional order coincides most closely with Kang's model, though with two significant differences: the United States, not China, is the primary state; and the hierarchical order is constituted by layers of major powers, rather than just the one. 4 Hierarchy and the East Asian security order Currently, the regional hierarchy in East Asia is still dominated by the United States. Since the 1970s, China has increasingly claimed the position of second-ranked great power, a claim that is today legitimized by the hierarchical deference shown by smaller subordinate powers such as South Korea and Southeast Asia. Japan and South Korea can, by virtue of their alliance with the United States, be seen to occupy positions in a third layer of regional major powers, while India is ranked next on the strength of its new strategic relationship with Washington. North Korea sits outside the hierarchic order but affects it due to its military prowess and nuclear weapons capability. Apart from making greater sense of recent history, conceiving of the US' role in East Asia as the dominant state in the regional hierarchy helps to clarify three critical puzzles in the contemporary international and East Asian security landscape. First, it contributes to explaining the lack of sustained challenges to American global preponderance after the end of the Cold War. Three of the key potential global challengers to US unipolarity originate in Asia (China, India, and Japan), and their support for or acquiescence to, US dominance have helped to stabilize its global leadership. Through its dominance of the Asian regional hierarchy, the United States has been able to neutralize the potential threats to its position from Japan via an alliance, from India by gradually identifying and pursuing mutual commercial and strategic interests, and from China by encircling and deterring it with allied and friendly states that support American preponderance. Secondly, recognizing US hierarchical preponderance further explains contemporary under-balancing in Asia, both against a rising China, and against incumbent American power. I have argued that one defining characteristic of a hierarchical system is voluntary subordination of lesser states to the dominant state, and that this goes beyond rationalistic bandwagoning because it is manifested in a social contract that comprises the related processes of hierarchical assurance and hierarchical deference. Critically, successful and sustainable hierarchical assurance and deference helps to explain why Japan is not yet a ‘normal’ country. Japan has experienced significant impetus to revise and expand the remit of its security forces in the last 15 years. Yet, these pressures continue to be insufficient to prompt a wholesale revision of its constitution and its remilitarization. The reason is that the United States extends its security umbrella over Japan through their alliance, which has led Tokyo not only to perceive no threat from US dominance, but has in fact helped to forge a security community between them (Nau, 2003). Adjustments in burden sharing in this alliance since the 1990s have arisen not from greater independent Japanese strategic activism, but rather from periods of strategic uncertainty and crises for Japan when it appeared that American hierarchical assurance, along with US' position at the top of the regional hierarchy, was in question. Thus, the Japanese priority in taking on more responsibility for regional security has been to improve its ability to facilitate the US' central position, rather than to challenge it.13 In the face of the security threats from North Korea and China, Tokyo's continued reliance on the security pact with the United States is rational. While there remains debate about Japan's re-militarization and the growing clout of nationalist ‘hawks’ in Tokyo, for regional and domestic political reasons, a sustained ‘normalization’ process cannot take place outside of the restraining framework of the United States–Japan alliance (Samuels, 2007; Pyle, 2007). Abandoning the alliance will entail Japan making a conscience choice not only to remove itself from the US-led hierarchy, but also to challenge the United States dominance directly. The United States–ROK alliance may be understood in a similar way, although South Korea faces different sets of constraints because of its strategic priorities related to North Korea. As J.J. Suh argues, in spite of diminishing North Korean capabilities, which render the US security umbrella less critical, the alliance endures because of mutual identification – in South Korea, the image of the US as ‘the only conceivable protector against aggression from the North,’ and in the United States, an image of itself as protector of an allied nation now vulnerable to an ‘evil’ state suspected of transferring weapons of mass destruction to terrorist networks (Suh, 2004). Kang, in contrast, emphasizes how South Korea has become less enthusiastic about its ties with the United States – as indicated by domestic protests and the rejection of TMD – and points out that Seoul is not arming against a potential land invasion from China but rather maritime threats (Kang, 2003, pp.79–80). These observations are valid, but they can be explained by hierarchical deference toward the United States, rather than China. The ROK's military orientation reflects its identification with and dependence on the United States and its adoption of US' strategic aims. In spite of its primary concern with the North Korean threat, Seoul's formal strategic orientation is toward maritime threats, in line with Washington's regional strategy. Furthermore, recent South Korean Defense White Papers habitually cited a remilitarized Japan as a key threat. The best means of coping with such a threat would be continued reliance on the US security umbrella and on Washington's ability to restrain Japanese remilitarization (Eberstadt et al., 2007). Thus, while the United States–ROK bilateral relationship is not always easy, its durability is based on South Korea's fundamental acceptance of the United States as the region's primary state and reliance on it to defend and keep regional order. It also does not rule out Seoul and other US allies conducting business and engaging diplomatically with China. India has increasingly adopted a similar strategy vis-à-vis China in recent years. Given its history of territorial and political disputes with China and its contemporary economic resurgence, India is seen as the key potential power balancer to a growing China. Yet, India has sought to negotiate settlements about border disputes with China, and has moved significantly toward developing closer strategic relations with the United States. Apart from invigorated defense cooperation in the form of military exchange programs and joint exercises, the key breakthrough was the agreement signed in July 2005 which facilitates renewed bilateral civilian nuclear cooperation (Mohan, 2007). Once again, this is a key regional power that could have balanced more directly and independently against China, but has rather chosen to align itself or bandwagon with the primary power, the United States, partly because of significant bilateral gains, but fundamentally in order to support the latter's regional order-managing function. Recognizing a regional hierarchy and seeing that the lower layers of this hierarchy have become more active since the mid-1970s also allows us to understand why there has been no outright balancing of China by regional states since the 1990s. On the one hand, the US position at the top of the hierarchy has been revived since the mid-1990s, meaning that deterrence against potential Chinese aggression is reliable and in place.14 On the other hand, the aim of regional states is to try to consolidate China's inclusion in the regional hierarchy at the level below that of the United States, not to keep it down or to exclude it. East Asian states recognize that they cannot, without great cost to themselves, contain Chinese growth. But they hope to socialize China by enmeshing it in peaceful regional norms and economic and security institutions. They also know that they can also help to ensure that the capabilities gap between China and the United States remains wide enough to deter a power transition. Because this strategy requires persuading China about the appropriateness of its position in the hierarchy and of the legitimacy of the US position, all East Asian states engage significantly with China, with the small Southeast Asian states refusing openly to ‘choose sides’ between the United States and China. Yet, hierarchical deference continues to explain why regional institutions such as the ASEAN Regional Forum, ASEAN + 3, and East Asian Summit have made limited progress. While the United State has made room for regional multilateral institutions after the end of the Cold War, its hierarchical preponderance also constitutes the regional order to the extent that it cannot comfortably be excluded from any substantive strategic developments. On the part of some lesser states (particularly Japan and Singapore), hierarchical deference is manifested in inclusionary impulses (or at least impulses not to exclude the United States or US proxies) in regional institutions, such as the East Asia Summit in December 2005. Disagreement on this issue with others, including China and Malaysia, has stymied potential progress in these regional institutions (Malik, 2006). Finally, conceiving of a US-led East Asian hierarchy amplifies our understanding of how and why the United States–China relationship is now the key to regional order. The vital nature of the Sino-American relationship stems from these two states' structural positions. As discussed earlier, China is the primary second-tier power in the regional hierarchy. However, as Chinese power grows and Chinese activism spreads beyond Asia, the United States is less and less able to see China as merely a regional power – witness the growing concerns about Chinese investment and aid in certain African countries. This causes a disjuncture between US global interests and US regional interests. Regional attempts to engage and socialize China are aimed at mediating its intentions. This process, however, cannot stem Chinese growth, which forms the material basis of US threat perceptions. Apprehensions about the growth of China's power culminates in US fears about the region being ‘lost’ to China, echoing Cold War concerns that transcribed regional defeats into systemic setbacks.15 On the other hand, the US security strategy post-Cold War and post-9/11 have regional manifestations that disadvantage China. The strengthening of US alliances with Japan and Australia; and the deployment of US troops to Central, South, and Southeast Asia all cause China to fear a consolidation of US global hegemony that will first threaten Chinese national security in the regional context and then stymie China's global reach. Thus, the key determinants of the East Asian security order relate to two core questions: (i) Can the US be persuaded that China can act as a reliable ‘regional stakeholder’ that will help to buttress regional stability and US global security aims;16 and (ii) can China be convinced that the United States has neither territorial ambitions in Asia nor the desire to encircle China, but will help to promote Chinese development and stability as part of its global security strategy? (Wang, 2005). But, these questions cannot be asked in the abstract, outside the context of negotiation about their relative positions in the regional and global hierarchies. One urgent question for further investigation is how the process of assurance and deference operate at the topmost levels of a hierarchy? When we have two great powers of unequal strength but contesting claims and a closing capabilities gap in the same regional hierarchy, how much scope for negotiation is there, before a reversion to balancing dynamics? This is the main structural dilemma: as long as the United States does not give up its primary position in the Asian regional hierarchy, China is very unlikely to act in a way that will provide comforting answers to the two questions. Yet, the East Asian regional order has been and still is constituted by US hegemony, and to change that could be **extremely disruptive** and may lead to regional actors acting in **highly destabilizing ways**. Rapid Japanese remilitarization, armed conflict across the Taiwan Straits, Indian nuclear brinksmanship directed toward Pakistan, or a highly destabilized Korean peninsula are all illustrative of potential regional disruptions. 5 Conclusion To construct a coherent account of East Asia's evolving security order, I have suggested that the United States is the **central force** in constituting regional stability and order. The major patterns of equilibrium and turbulence in the region since 1945 can be explained by the relative stability of the US position at the top of the regional hierarchy, with periods of greatest insecurity being correlated with greatest uncertainty over the American commitment to managing regional order. Furthermore, relationships of hierarchical assurance and hierarchical deference explain the unusual character of regional order in the post-Cold War era. However, the greatest contemporary challenge to East Asian order is the potential conflict between China and the United States over rank ordering in the regional hierarchy, a contest made more potent because of the inter-twining of regional and global security concerns. Ultimately, though, investigating such questions of positionality requires conceptual lenses that go beyond basic material factors because it entails social and normative questions. How can China be brought more into a leadership position, while being persuaded to buy into shared strategic interests and constrain its own in ways that its vision of regional and global security may eventually be reconciled with that of the United States and other regional players? How can Washington be persuaded that its central position in the hierarchy must be ultimately shared in ways yet to be determined? The future of the East Asian security order is tightly bound up with the durability of the United States' global leadership and regional domination. At the regional level, the main scenarios of disruption are an outright Chinese challenge to US leadership, or the defection of key US allies, particularly Japan. Recent history suggests, and the preceding analysis has shown, that challenges to or defections from US leadership will come at junctures where it appears that the US commitment to the region is in doubt, which in turn destabilizes the hierarchical order. At the global level, American geopolitical over-extension will be the key cause of change. This is the one factor that could lead to both greater regional and global turbulence, if only by the attendant strategic uncertainly triggering off regional challenges or defections. However, it is notoriously difficult to gauge thresholds of over-extension. More positively, East Asia is a region that has adjusted to previous periods of uncertainty about US primacy. Arguably, the regional consensus over the United States as primary state in a system of benign hierarchy could accommodate a shifting of the strategic burden to US allies like Japan and Australia as a means of systemic preservation. The alternatives that could surface as a result of not doing so would appear to be much worse.

## WPR Advantage

### 1NC

#### WPR wrecks the political will for successful operations

**Newton, Vanderbilt law professor, 2012**

(Michael, “Inadvertent Implications of the War Powers Resolution”, Fall, <http://law.case.edu/journals/JIL/Documents/45CaseWResJIntlL1&2.10.Article.Newton.pdf>, ldg)

The corollary to this modern reality, and the second of three inadvertent implications of the Resolution, is that our enemies now focus on American political will as the Achilles heel of our vast capabilities. Prior to the War Powers Resolution, President Eisenhower understood that it was necessary to “seek the cooperation of the Congress. Only with that can we give the reassurance needed to deter aggression.”62 President Clinton understood the importance of clear communication with the Congress and the American people in order to sustain the political legitimacy that is a vital element of modern military operations. Justifying his bombing of targets in Sudan, he argued that the “risks from inaction, to America and the world, would be far greater than action, for that would embolden our enemies, leaving their ability and their willingness to strike us intact.” 63 In his letter to Congress “consistent with the War Powers Resolution,” the president reported that the strikes “were a necessary and proportionate response to the imminent threat of further terrorist attacks against U.S. personnel and facilities” and “were intended to prevent and deter additional attacks by a clearly identified terrorist threat.” 64 The following day, in a radio address to the nation, the president explained his decision to take military action, stating, “Our goals were to disrupt bin Laden’s terrorist network and destroy elements of its infrastructure in Afghanistan and Sudan. And our goal was to destroy, in Sudan, the factory with which bin Laden’s network is associated, which was producing an ingredient essential for nerve gas.” 65 Citing “compelling evidence that the bin Laden network was poised to strike at us again” and was seeking to acquire chemical weapons, the president declared that we simply could not ignore the threat posed, and hence ordered the strikes.66 Similarly, President Clinton understood that intervention in Bosnia could not be successful absent some national consensus, which had been slow to form during the long Bosnian civil war.67 Secretary of State George Schultz provided perhaps the most poignant and pointed example of this truism in his testimony to Congress regarding the deployment of US Marines into Lebanon to separate the warring factions in 1982. On September 21, 1983, he testified before the Senate Foreign Relations Committee and provided a chilling premonition of the bombing that would come only one month later and kill 241 Americans, which was the bloodiest day in the Marine Corps since the battle of Iwo Jima.68 Seeking to bolster legislative support and to better explain the strategic objectives, he explained that: It is not the mission of our marines or of the [Multinational Force in Lebanon] as a whole to maintain the military balance in Lebanon by themselves. Nevertheless, their presence remains one crucial pillar of the structure of stability. They are an important deterrent, a symbol of the international backing behind the legitimate Government of Lebanon, and an important weight in the scales. To remove the marines would put both the Government and what we are trying to achieve in jeopardy. This is why our domestic controversy over the war powers has been so disturbing. Uncertainty about the American commitment can only weaken our effectiveness. Doubts about our staying power can only cause political aggressors to discount our presence or to intensify their attacks in hopes of hastening our departure. An accommodation between the President and Congress to resolve this dispute will help dispel those doubts about our staying power and strengthen our political hand.69 Following the spectacularly successful terrorist attack on the Marine barracks in Beirut, President Reagan withdrew the Marines. Osama bin Laden later cited this as an example of American weakness that could not withstand the jihadist fury he sought.70 The legal battles over the scope and effect of the War Powers Resolution have highlighted the focus on national political will as the fulcrum of successful military operations by requiring assurances that military operations are limited in nature, duration, and scope, and therefore well within the president’s constitutional authority as Commander-in-Chief and chief executive. President Obama’s report to Congress in the context of the Libya operations in 2011 cited precedent from air strikes in Bosnia that took just over two weeks and involved more than 2,300 US sorties and the deployment of US forces in Somalia in 1992 and Haiti in 1993.71 The White House released a memorandum from the OLC, similar to previous interventions, explaining how the authorization to use such force was constitutional on the basis that “‘war’ within the meaning of the [Constitution’s] Declaration of War Clause” does not encompass all military engagements, but only those that are “prolonged and substantial . . . typically involving exposure of U.S. military personnel to significant risk over a substantial period.” 72 President Obama consistently maintained that the US role in Libya was limited, unlikely to expose any US persons to attack (especially given the role of missiles and drones and the utter inability of Qaddafi’s forces to strike back with conventional means), and likely to end expeditiously.73 By that logic, it did not require authorization from Congress. The administration ultimately adopted a legal analysis that the US military’s activities fell short of “hostilities,” and thus, the president needed no permission from Congress to continue the mission after the expiration of the sixty-day reporting window specified in the War Powers Resolution.74 The president’s reasoning rested on previous OLC opinions that what counts as war depends on “a factspecific assessment of the ‘anticipated nature, scope, and duration’ of the planned military operations.” 75 Present justifications for bypassing the War Powers Resolution hinge on interpretations that it requires “prolonged and substantial military engagements, typically involving exposure of U.S. military personnel to significant risk over a substantial period.” 76 The OLC engaged in similar reasoning in the Bosnia intervention in 1995, explaining that in deciding whether the proposed deployment into Bosnia amounted to a “‘war’ in the constitutional sense, considerable weight was given to the consensual nature and protective purposes of the operation.” 77 That deployment was similarly intended to be a limited mission but that mission, in contrast to the present one, was in support of an agreement that the warring parties had reached and it was at the invitation of the parties that led to the belief that little or no resistance to the deployment would occur. Though some scholars argued that the Libya OLC Memorandum defended its reasoning for why the operation did not amount to “war,” it did not address whether the administration believed that it will have to stop operations upon expiration of the sixty-ninety-day clock under the War Powers Resolution.78 The deadline passed with little fanfare. The memorandum also relied upon quite distinguishable precedent to serve as a guiding point in this intervention. Professor Goldsmith argued the opinion broke “new ground . . . in its extension of the ‘no war’ precedents beyond the Bosnia and Haiti situations—which involved consensual peacekeeping-like introductions of ground troops but no significant uses of force—to cover two weeks of non-consensual aerial bombardments.” 79 Thus, even as it incentivizes short term, limited deployments, the War Powers Resolution embeds an inevitable constitutional collision between the coordinate branches. Our enemies can rely upon constitutional carping from Congress, and in fact can adapt tactics and statements that seek to undermine political will in the US Congress and among the American people from the first days of an operation. The Resolution helps to ensure that such debates over the national political will take center stage sooner rather than later, and an asymmetric enemy can in theory erode our political will even before it solidifies

### A2: Group Think

#### Groupthink theory is wrong

**Hempell, User Experience Consulting Senior Information Architect, 2004**

(Anthony, “Groupthink: An introduction to Janis' theory of concurrence-seeking tendencies in group work”, 3-3, http://www.anthonyhempell.com/papers/groupthink/)

In the thirty years since Janis first proposed the groupthink model, there is still little agreement as to the validity of the model in assessing decision-making behaviour (Park, 2000). Janis' theory is often criticized because it does not present a framework that is suitable for empirical testing; instead, the evidence for groupthink comes from largely qualitative, historical or archival methods (Sunstein, 2003). Some critics go so far as to say that Janis's work relies on "anecdote, casual observation, and intuitive appeal rather than rigorous research" (Esser, 1998, cited in Sunstein, 2003, p.142). While some studies have shown support for the groupthink model, the support tends to be mixed or conditional (Esser, 1998); some studies have revealed that a closed leadership style and external threats (in particular, time pressure) promote groupthink and defective decision making (Neck & Moorhead, 1995, cited by Choi & Kim, 1999); the effect of group cohesiveness is still inconclusive (Mullen, Anthony, Salas & Driskel, 1994, cited by Choi & Kim, 1999). Janis's model tends to be supported by studies that employ a qualitative case-study approach as opposed to experimental research, which tends to either partially support or not support Janis's thesis (Park, 2000). The lack of success in experimental validation of groupthink may be due to difficulties in operationalizing and conceptualizing it as a testable variable (Hogg & Hains, 1998; Park, 2000). Some researchers have criticized Janis for categorically denouncing groupthink as a negative phenomenon (Longley & Pruitt, 1980, cited in Choi & Kim, 1999). Sniezek (1992) argues that there are instances where concurrence-seeking may promote group performance. When used to explain behaviour in a practical setting, groupthink has been frames as a detrimental group process; the result of this has been that many corporate training programs have created strategies for avoiding groupthink in the workplace (Quinn, Faerman, Thompson & McGrath, 1990, cited in Choi & Kim, 1999). Another criticism of groupthink is that Janis overestimates the link between the decision-making process and the outcome (McCauley, 1989; Tetlock, Peterson, McGuire, Chang & Feld, 1992; cited in Choi & Kim, 1999). Tetlock et al argue that there are many other factors between the decision process and the outcome. The outcome of any decision-making process, they argue, will only have a certain probability of success due to various environmental factors (such as luck). A large-scale study researching decision-making in seven major American corporations concluded that decision-making worked best when following a sound information processing method; however these groups also showed signs of groupthink, in that they had strong leadership which attempted to persuade others in the group that they were right (Peterson et al, 1998, cited in Sunstein, 2003). Esser (1998) found that groupthink characteristics were correlated with failures; however cohesiveness did not appear to be a factor: groups consisting of strangers, friends, or various levels of previous experience together did not appear to effect decision-making ability. Janis' claims of insulation of groups and groups led by autocratic leaders did show that these attributes were indicative of groupthink symptoms. Moorhead & Montanari conducted a study where they concluded that groupthink symptoms had no significant effect on group performance, and that "the relationship between groupthink-induced decision defects and outcomes were not as strong as Janis suggests" (Moorhead & Montanari, 1986, p. 399; cited by Choi & Kim, 1999).

### Heg

#### Legitimacy is resilient

**Brooks et al., Dartmouth government professor, 2009**

(Stephen, “Reshaping the world order: how Washington should reform international institutions”, Foreign Affairs, Marhc/April, ebsco, ldg)

FOR ANALYSTS such as Zbigniew Brzezinski and Henry Kissinger, the key reason for skepticism about the United States' ability to spearhead global institutional change is not a lack of power but a lack of legitimacy. Other states may simply refuse to follow a leader whose legitimacy has been squandered under the Bush administration; in this view, the legitimacy to lead is a fixed resource that can be obtained only under special circumstances. The political scientist G.John Ikenberry argues in After Victory that states have been well positioned to reshape the institutional order only after emerging victorious from some titanic struggle, such as the French Revolution, the Napoleonic Wars, or World War I or II. For the neoconservative Robert Kagan, the legitimacy to lead came naturally to the United States during the Cold War, when it was providing the signal service of balancing the Soviet Union. The implication is that today, in the absence of such salient sources of legitimacy, the wellsprings of support for U.S. leadership have dried up for good. But this view is mistaken. For one thing, it overstates how accepted U.S. leadership was during the Cold War: anyone who recalls the Euromissile crisis of the 1980s, for example, will recognize that mass opposition to U.S. policy (in that case, over stationing intermediaterange nuclear missiles in Europe) is not a recent phenomenon. For another, it understates how dynamic and malleable legitimacy is. Legitimacy is based on the belief that an action, an actor, or a political order is proper, acceptable, or natural. An action - such as the Vietnam War or the invasion of Iraq - may come to be seen as illegitimate without sparking an irreversible crisis of legitimacy for the actor or the order. When the actor concerned has disproportionately more material resources than other states, the sources of its legitimacy can be refreshed repeatedly. After all, this is hardly the first time Americans have worried about a crisis of legitimacy. Tides of skepticism concerning U.S. leadership arguably rose as high or higher after the fall of Saigon in 1975 and during Ronald Reagan's first term, when he called the Soviet Union an "evil empire." Even George W. Bush, a globally unpopular U.S. president with deeply controversial policies,oversaw a marked improvement in relations with France, Germany, and India in recent years - even before the elections of Chancellor Angela Merkel in Germany and President Nicolas Sarkozy in France. Of course, the ability of the United States to weather such crises of legitimacy in the past hardly guarantees that it can lead the system in the future. But there are reasons for optimism. Some of the apparent damage to U.S. legitimacy might merely be the result of the Bush administration's approach to diplomacy and international institutions. Key underlying conditions remain particularly favorable for sustaining and even enhancing U.S. legitimacy in the years ahead. The United States continues to have a far larger share of the human and material resources for shaping global perceptions than any other state, as well as the unrivaled wherewithal to produce public goods that reinforce the benefits of its global role. No other state has any claim to leadership commensurate with Washington's. And largely because of the power position the United States still occupies, there is no prospect of a counterbalancing coalition emerging anytime soon to challenge it. In the end, the legitimacy of a system's leader hinges on whether the system's members see the leader as acceptable or at least preferable to realistic alternatives. Legitimacy is not necessarily about normative approval: one may dislike the United States but think its leadership is natural under the circumstances or the best that can be expected. Moreover, history provides abundant evidence that past leading states - such as Spain, France, and the United Kingdom - were able to revise the international institutions of their day without the special circumstances Ikenberry and Kagan cite. Spainfashioned both normative and positive laws to legitimize its conquest of indigenous Americans in the early seventeenth century; France instituted modern concepts of state borders to meet its needs as Europe's preeminent land power in the eighteenth century; and the United Kingdom fostered rules on piracy, neutral shipping, and colonialism to suit its interests as a developing maritime empire in the nineteenth century. As Wilhelm Grewe documents in his magisterial The Epochs of International Law, these states accomplished such feats partly through the unsubtle use of power: bribes, coercion, and the allure oflucrative long-term cooperation. Less obvious but often more important, the bargaining hands of the leading states were often strengthened by the general perception that they could pursue their interests in even less palatable ways - notably, through the naked use of force. Invariably, too, leading states have had the power to set the international agenda, indirectly affecting the development of new rules by defining the problems they were developed to address. Given its naval primacy and global trading interests, the United Kingdom was able to propel the slave trade to the forefront of the world's agenda for several decades after it had itself abolished slavery at home, in 1833. The bottom line is that the UnitedStates today has the necessary legitimacy to shepherd reform of the international system.

#### Doesn’t solve “better wars”

**Nzelibe et al., Northwestern law professor, 2006**

(Jide, “Rational War and Constitutional Design,” Yale Law Journal, Vol. 115, SSRN)

But before accepting this attractive vision, we should ask whether the Congress first system produces these results. In other words, has requiring congressional ex ante approval for foreign wars produced less war, better decision making, or greater consensus? Students of American foreign policy generally acknowledge that comprehensive empirical studies of American wars are impractical, due to the small number of armed conflicts. Instead, they tend to focus on case studies. A cursory review of previous American wars does not suggest that congressional participation in war necessarily produces better decision making. We can certainly identify wars, such as the Mexican-American War or the Spanish-American War, in which a declaration of war did not result from extensive deliberation nor necessarily result in good policy.14 Both wars benefited the United States by expanding the nation’s territory and enhanced its presence on the world stage,15 but it seems that these are not the wars that supporters of Congress’s Declare War power would want the nation to enter – i.e., offensive wars of conquest. Nor is it clear that congressional participation has resulted in greater consensus and better decision making. Congress approved the Vietnam War, in the Tonkin Gulf resolution, and the Iraq war, both of which have produced sharp division in American domestic politics and proven to be mistakes. The other side of the coin here usually goes little noticed, but is just as important for evaluating the substantive performance of the Congress-first system. To a significant extent, much of the war powers literature focuses on situations in which the United States might erroneously enter a war where the costs outweigh the expected benefits. Statisticians usually label such errors of commission as Type I errors. Scholars rarely, if ever, ask whether requiring congressional ex ante approval for foreign wars could increase Type II errors. Type II errors occur when the United States does not enter a conflict where the expected benefits to the nation outweigh the costs, and this could occur today when the President refuses to launch a preemptive strike against a nation harboring a hostile terrorist group, for example, out of concerns over congressional opposition. It may be the case that legislative participation in warmaking could prevent the United States from entering, or delaying entry, into wars that would benefit its foreign policy or national security. The clearest example is World War II. During the inter-war period, Congress enacted several statutes designed to prevent the United States from entering into the wars in Europe and Asia. In 1940 and 1941, President Franklin D. Roosevelt recognized that America’s security would be threatened by German control of Europe, and he and his advisers gradually attempted to bring the United States to the assistance of Great Britain and the Soviet Union.16 Nonetheless, congressional resistance prevented Roosevelt from doing anything more than supplying arms and loans to the Allies, although he arguably stretched his authority to cooperate closely with Great Britain in protecting convoys in the North Atlantic, among other things. It is likely that if American pressure on Japan to withdraw from China had not helped triggered the Pacific War, American entry into World War II might have been delayed by at least another year, if not longer.17 Knowing what we now know, most would agree that America’s earlier entry into World War II would have been much to the benefit of the United States and to the world. A more recent example might be American policy in the Balkans during the middle and late 1990s.

#### Alliances are out dated, multi-polarity is stable and there is no scenario for war in a world of US decline

**Friedman et al., MIT political science PhD candidate, 2012**

(Benjamin, “Why the U.S. Military Budget is ‘Foolish and Sustainable”, Orbis, 56.2, Science Direct, ldg)

Standard arguments for maintaining the alliances come in two contradictory strains. One, drawn mostly from the run-up to World War II, says that without American protection, the ally would succumb to a rival power, either by force or threat of force, heightening the rival’s capability and danger to the United States. The other argument says that without the United States, the ally would enter a spiral of hostility with a neighbor, creating instability or war that disrupts commerce and costs America more than the protection that prevented it. The main problem with the first argument is that no hegemon today threatens to unify Europe or Asia. Europe is troubled by debt, not conquest. Russian GDP is today roughly equivalent to that of Spain and Portugal combined. Whatever Russia’s hopes, it has no ability to resurrect its Soviet Empire, beyond perhaps those nations in its near abroad that Americans have no good reason to defend. Even today, the military capabilities of Europe’s leading powers are sufficient to defend its eastern flank, and they could increase their martial exertions should a bigger threat arise. Asia is tougher case. South Korea’s military superiority over its northern neighbor is sufficient to deter it from an attempt at forcible reunification. By heightening North Korea’s security, nuclear weapons may reinforce its capacity for trouble-making, but they do not aid offensive forays. U.S. forces long ago became unnecessary to maintaining the peninsula’s territorial status quo. Chinese efforts to engage in old-fashioned conquest are unlikely, at least beyond Taiwan. Its more probable objective is a kind of Asian Monroe doctrine, meant to exclude the United States.6 China naturally prefers not to leave its maritime security at the whim of U.S. policymakers and, thus, has sought to improve its anti-access and area-denial capabilities. In the longer term, China’s leaders will likely pursue the ability to secure its trade routes by building up longer-range naval forces. They may also try to leverage military power to extract various concessions from nearby states. Washington’s defense analysts typically take those observations as sufficient to establish the necessity that U.S. forces remain in Asia to balance Chinese military power. But to justify a U.S. military presence there, one also needs to show both that Asian nations cannot or will not balance Chinese power themselves and that their failure to do so would greatly harm U.S. security. Neither is likely. Geography and economics suggest that the states of the region will successfully balance Chinese power—even if we assume that China’s economic growth allows it to continue to increase military spending.7 Bodies of water are natural defenses against offensive military operations. They allow weaker states to achieve security at relatively low cost by investing in naval forces and coastal defenses. That defensive advantage makes balances of power more stable. Not only are several of China’s Asian rivals islands, but those states have the wealth to make Chinese landings on their coast prohibitively expensive. India’s mountainous northern border creates similar dynamics. The prospects of Asian states successfully deterring future Chinese aggression will get even better if, as seems likely, threats of aggression provoke more formal security alliances. Some of that is already occurring. Note for example, the recent joint statement issued by the Philippines and Japan marking a new ‘‘strategic partnership’’ and expressing ‘‘common strategic interests’’ such as ‘‘ensuring the safety of sea lines of communication.’’8 This sort of multilateral cooperation would likely deepen with a more distant U.S. role. Alliances containing disproportionately large states historically produce free-riding; weaker alliance partners lose incentive to shore up their own defenses.9 Even if one assumes that other states in the region would fail to balance China, it is unclear exactly how U.S. citizens would suffer. China’s territorial ambitions might grow but are unlikely to span the Pacific. Nor would absorbing a few small export-oriented states slacken China’s hunger for the dollars of American consumers. The argument that U.S. alliances are necessary for stability and global commerce is only slightly more credible. One problem with this claim is that U.S. security guarantees can create moral hazard—emboldening weak allies to take risks they would otherwise avoid in their dealings with neighbors. Alliances can then discourage accommodation among neighboring states, heightening instability and threatening to pull the United States into wars facilitated by its benevolence. Another point against this argument is that even if regional balancing did lead to war, it would not obviously be more costly to the U.S. economy than the cost of the alliance said to prevent it. Neutrality historically pays.10 The larger problem with the idea that our alliances are justified by the balancing they prevent is that wars generally require more than the mutual fear that arms competition provokes. Namely, there is usually a territorial conflict or a state bent on conflict. Historical examples of arms races alone causing wars are few.11 This confusion probably results from misconstruing the causes of World War I—seeing it as a consequence of mutual fear alone rather than fear produced by the proximity of territorially ambitious states.12 Balances of power, as noted, are especially liable to be stable when water separates would-be combatants, as in modern Asia. Japan would likely increase defense spending if U.S. forces left it, and that would likely displease China. But that tension is very unlikely to provoke a regional conflagration. And even that remote scenario is far more likely than the Rube Goldberg scenario needed to argue that peace in Europe requires U.S. forces stationed there. It is not clear that European states would even increase military spending should U.S. troops depart. If they did do so, one struggles to imagine a chain of misperceived hostility sufficient to resurrect the bad old days of European history.

### 2NC Groupthink

#### Groupthink theory is based on over-generalizations, skewed studies, and ignores potential positives

**Aldag et al., Wisconsin Management and Human resources professor, 1993**

(Ramon, “Beyond Fiasco : A Reappraisal of the Groupthink Phenomenon and a New Model of Group Decision Processes”, Psychological Bulletin, 113.3, ebsco)

Groupthink has been overwhelmingly viewed as an unalayed evil, leading to uniformly negative outcomes. Indeed, such a view is universally implicit in the language of groupthink (e.g., the common references to “symptoms of groupthink,” “victims of groupthink,” and “defects of groupthink”). When used in groupthink research, such negative terminology can invite distortions in responses caused by scale-use tendencies and related psychometric difficulties and can also result in framing effects.¶ Individuals (whether subjects or researchers) presented with negatively framed terminology may adopt the readily available negative frame and respond accordingly ( Bazerman, 1990; Tversky & Kahneman, 1986). Therefore, even simple attempts by the subjects to give responses that are consistent with the tone of the questions would result in negatively oriented responses. In many cases, failed decisions are examined and characteristics of groupthink are then sought. There is evidence that when individuals are provided with knowledge of a negative outcome, they infer a negative process ( Guzzo, Wagner, Maguire, Herr, & Hawley, 1986). Furthermore, a focus only on the conjunction of groupthink characteristics and negative outcomes invites illusory correlation (cf. Einhorn, 1980; Hogarth, 1980; Kleinmuntz, 1990).¶ On a more fundamental level, this framing has resulted in a focus on error rather than on decision quality per se. Janis (1982) noted that he began studying fiascoes “for the purposes of studying sources of error in foreign policy decision-making” (p. 9). However, there is more to the performance of a football team than the absence of fumbles and interceptions, and there is more to group decision quality than the absence of error. A focus on negative outcomes of group processes may divert attention from group synergies. One example is the assembly effect bonus, which, as noted by Collins and Guetzkow (1964), “is productivity which exceeds the potential of the most capable member and also exceeds the sum of the efforts of the group members working separately” (p. 58). There is considerable evidence for this assembly effect bonus, at least in some contexts (e.g., Burleson, Levine, & Samter, 1984). Thus, researchers may learn little about superior group performance by a focus solely on fiascoes. Instead, a focus on decisions with a broad range of outcomes, including superior performance, is necessary.¶ The consequences of the groupthink model's focus on fiascoes are doubly ironic. First, the consideration only of fiascoes precludes generalization to other decision situations used in virtually all attempts to assess the validity of groupthink. Second, the focus on fiascoes makes it impossible to say anything even about the determinants of fiascoes.

#### Reject their case studies --- they’re done with students and don’t apply to military policy

**Aldag et al., Wisconsin Management and Human resources professor, 1993**

(Ramon, “Beyond Fiasco : A Reappraisal of the Groupthink Phenomenon and a New Model of Group Decision Processes”, Psychological Bulletin, 113.3, ebsco)

As suggested by the earlier review, most support for groupthink has come from retrospective case studies that have focused on decision fiascoes rather than comparing the decision-making processes associated with good versus bad decisions.¶ Experimental studies of groupthink have considered only a small portion of the model, often without a cohesive group and in situations inconsistent with Janis's (1971, 1972, 1982, 1989) antecedents. Furthermore, they have relied exclusively on student samples dealing with hypothetical or simulated decisions, with potential resultant problems for external validity. Military strategists, managers, politicians, or other “real-world” decision makers have never been used. In the laboratory, many real-world group characteristics, including ongoing power relationships and political maneuverings, have been necessarily ignored. Although student samples in laboratory settings may be valuable to address many issues relating to group problem solving, their use to examine groupthink is problematic.

## Cyber Advantage

### 1NC – OCO Good

#### Limitations wreck offensive cyber policy-they try to apply obtuse concepts and hurt flex

**Kallberg, Cyber Security Research and Educational Center researcher, 2013**

(Jan, “Offensive Cyber: Superiority or Stuck in Legal Hurdles?”, 2-17, <http://works.bepress.com/cgi/viewcontent.cgi?article=1021&context=jan_kallberg>, ldg)

In recent years, offensive cyber operations have attracted significant interest from the non-Defense Department academic legal community, prompting numerous articles seeking to create a legal theory for cyber conflicts. Naturally, cyber operations should be used in an ethical way, but the hurdles generated by the legal community are staggering. At a time when the United States has already lost an estimated $4 trillion in intellectual property as a result of foreign cyber espionage, not to mention the loss of military advantage, focusing on what the United States cannot do in cyberspace only hinders efforts to defend the country from future cyber attack. The country is facing an enemy unrestrained by limitations, clearly visible in blatant cyber attacks on military networks, major banks and media outlets. Academics who question the legality of offensive counter cyber operations often have limited technical understanding of the unique characteristics of cyberspace. The theoretical framework for an emerging cyber law under development by the legal community uses analogies from international law, such as the laws of the high seas and international commercial air treaties. But these are highly inappropriate for the cyber domain. For example, the vast majority of these academic legal scholars would require the United States ensure that malicious software attack only combatant systems and legitimate military targets, and not affect any other systems. What these requirements ignore is the issue of control. Those digital bits easily can be copied and distributed, and targeting removed or redesigned. How can a coder control the duplication of the code? While code can be targeted to a specific military system, that is no guarantee it will be limited because of the dual use of information technology. There is no control of the code once it is released. The legal perception of cyber is based on an assumption that actors are either civilian or military, but there is no such clear distinction in the militarized and contested digital world. It is digital bits; in the same way that we cannot distinguish military air and civilian air. It is just air. In cyberspace, universities, municipal utilities, communication companies and other actors are a part of the war-fighting effort without clear boundaries to being civilian or military. If the U.S. became engaged in a cyber conflict with Hezbollah in southern Lebanon, an organization that is a mix of crude arms manufacturing, terrorism training and soup kitchens for the poor, there is no way to ensure that a counter cyber attack would not affect the soup kitchens. Second, to avoid the slightest collateral damage, the counter-attacker needs to be able to identify each computer in the counter-attacked network and verify its purpose. That requires full overview of the targeted system, maybe beyond even what the defending system administrators are aware of. The only way you can verify resources in another network is to pre-emptively gain access to their networks and gain targeting information. Third, international laws rely on territorial boundaries. The laws of the high sea are effective in international water. The national laws apply to territorial waters. But there is no territorial or international cyberspace as long as attribution is unsolved — and even with attribution solved, the answer to where, when and by whom is troublesome to answer. Applying laws of war that have origins in the 1800s, when massive armies fought on a field in broad daylight, in an abundance of object permanence, is not relevant to cyber when the contested space is changed, lost, created, reborn and redesigned in real time. Inferences about cyber operations made in published articles in the academic legal press are in many cases, to use a mild word, spurious. Retired Air Force Maj. Gen. Dale Meyerrose, former associate director of national intelligence, said in regard to offensive cyber operations, “Like everything else in cyber, our legal system is about 20 years behind.” The risk for the nation is tangible. The proposed legal hurdles evaporate the opportunity to successfully conduct offensive cyber as a soft policy option. The non-DoD academics’ legal theories on how to conduct cyberwar fail to recognize the human costs in the alternative: traditional kinetic warfare. The absence of relevant legal guidance creates confusion and undermines a coherent and systematic approach. Cyber can help the U.S. achieve political and military goals. These operations will require a legal framework based on the unique tenets of cyber to enable, not disable, American options and abilities.

#### OCOs solves North Korean brinkmanship-speed is key to coercive leverage

**Libicki, RAND senior management scientist, 2013**

(Martin, “Brandishing Cyberattack Capabilities”, [http://www.rand.org/pub s/research\_reports/RR175.html](http://www.rand.org/pub%20s/research_reports/RR175.html), ldg)

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.

#### Global nuclear war

**Hayes and Green, Exec director of the Nautilus Institute, 2010**

(Peter, Victoria University, and Michael, Executive Director of the Nautilus Institute, “-“The Path Not Taken, the Way Still Open: Denuclearizing the Korean Peninsula and Northeast Asia”)

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.

### Norms

#### Norms fail –

#### A - trust

**Goldsmith, Harvard law professor, 2013**

(Jack, “Cybersecurity Treaties A Skeptical View”, <http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf>, ldg)

James Lewis acknowledges that verification of compliance will not work, but he nonetheless thinks that cybersecurity treaties can promote cooperation. Even in the absence of compliance verification, he argues, “multilateral agreements could increase stability and reduce the risks of miscalculation or escalation by focusing on several specific areas: confidence-building and transparency measures, such as increased transparency in doctrine; creation of norms for responsible state behavior in cyberspace; and expansion of common understandings on the application of international law to cyber conflicts, or development of assurances on the use of cyberattacks.”26 The possibility of softer norms of this sort—whether embodied in a treaty or in a less formal document—is frequently mentioned, and the subject warrants a more extended discussion than I can here give it. My skepticism can be summarized as follows: in the absence of decent verification, we cannot be confident that transparency measures are in fact transparent, or that revealed doctrine is actual doctrine. Nor can norms get much purchase in a world without serious attribution and verification; anonymity is a norm destroyer.

#### B – self interest

**Lewis, CSIS senior fellow, 2011**

(James, “Confidence-building and International Agreement in Cybersecurity”, <http://citizenlab.org/cybernorms2012/Lewis2011.pdf>, ldg)

The creation of norms for responsible state behaviour in cyberspace, the expansion of common understandings on the application of international law to cyberconflict, and the development of assurances on the use of cyber attacks would increase stability and reduce the risks of miscalculation or escalation. The single most important norm for multilateral agreement might be a norm that establishes state responsibility for the actions of its private citizens—such a norm could make it more difficult for states to tacitly encourage proxies by ignoring them or denying involvement with their actions. However, even simple norms face serious opposition. Conflicting political agendas, covert military actions, espionage and competition for global influence form the context for international discussion of cybersecurity. While there is little or no support for the idea of a treaty, and while international efforts now focus on a norms-based approach, the level of distrust among powerful states is too high for easy agreement on norms. Disparate values and deep distrust shape the environment for negotiation. Fundamental differences over values, despite formal acceptance of universal human rights, means that the initial set of norms likely to be acceptable to many states is limited. Ultimately, increased stability and security in cyberspace will require common understandings among states on their national responsibilities, on how the laws of war apply, where restraint in the use of the new military capability is possible, and where red lines or thresholds for escalation might exist. But there is too much distrust among competitors to move immediately towards global norms for cybersecurity.

#### DA is a prereq-effective offensive is the only way to have effective defense

**Limnéll, NDU military science PhD, 2012**

(Jarno, “Offensive Cyber Capabilities Need to be Built and Exposed Because of Deterrence”, 10-9, <http://infosecisland.com/blogview/22534-Offensive-Cyber-Capabilities-Need-to-be-Built-and-Exposed-Because-of-Deterrence.html>, ldg)

First, if you want be a credible player both on the military battlefield and in world politics, you must have offensive capabilities, just as you must have defensive capabilities and the ability to be resilient. You simply cannot have a credible cyber defense without offensive abilities. Second, in order to achieve and raise your deterrence, you must possess offensive capabilities. The ability to act offensively includes a strong preventive message to others, provided they understand it and believe it. Offensive capabilities represent the key components of deterrence. Third, offensive thinking and building weaponry are vital in order to create a stronger and credible defense. With only “defensive thinking” you will not succeed. You have to understand how an attacker acts and you must try to find all possible vulnerabilities in your defense. You must also develop your defensive potential, by testing your current defense and training your forces. All this becomes much more efficient if you can test it with your own capabilities. Without the ability to act as an attacker, no country can build an effective and credible cyber defense.

### Russia

#### No Russia war-no motive or capability

**Betts, Columbia war and peace studies professor, 2013**

(Richard, “The Lost Logic of Deterrence”, Foreign Affairs, March/April, ebsco, ldg)

These continuities with the Cold War would make sense only between intense adversaries. Washington and Moscow remain in an adversarial relationship, but not an intense one. If the Cold War is really over, and the West really won, then continuing implicit deterrence does less to protect against a negligible threat from Russia than to feed suspicions that aggravate political friction. In contrast to during the Cold War, it is now hard to make the case that Russia is more a threat to NATO than the reverse. First, the East-West balance of military capabilities, which at the height of the Cold War was favorable to the Warsaw Pact or at best even, has not only shifted to NATO's advantage; it has become utterly lopsided. Russia is now a lonely fraction of what the old Warsaw Pact was. It not only lost its old eastern European allies; those allies are now arrayed on the other side, as members of NATO. By every significant measure of power -- military spending, men under arms, population, economic strength, control of territory -- NATO enjoys massive advantages over Russia. The only capability that keeps Russia militarily potent is its nuclear arsenal. There is no plausible way, however, that Moscow's nuclear weapons could be used for aggression, except as a backstop for a conventional offensive -- for which NATO's capabilities are now far greater. Russia's intentions constitute no more of a threat than its capabilities. Although Moscow's ruling elites push distasteful policies, there is no plausible way they could think a military attack on the West would serve their interests. During the twentieth century, there were intense territorial conflicts between the two sides and a titanic struggle between them over whose ideology would dominate the world. Vladimir Putin's Russia is authoritarian, but unlike the Soviet Union, it is not the vanguard of a globe-spanning revolutionary ideal.

# 2NC

## T

### Limits first

### 2NC Conditions

### 2NC After the fact notification

After the fact consultation isn’t a restriction

Glennon-prof international law, Fletcher School of Law and Diplomact, Tufts University-9

103 A.J.I.L. 75, \*

NOTE AND COMMENT: THE WAR POWERS RESOLUTION, ONCE AGAIN

More important, a constitutional requirement for prior legislative authorization, if it exists, would not be fulfilled by seeking a few after-the-fact congressional opinions of the sort this proposal contemplates. Such a requirement, if it exists, would establish the constitutional predicate for the War Powers Resolution's key restriction, the sixty-day time limit. Without such a requirement, on the other hand, the constitutional case against the sixty-day limit would be stronger and the constitutional case against a statutorily imposed consultation requirement of the sort recommended by the panel would be weaker.

### 2NC Cyber-Topical Version

Authorization is the topical version of the aff

Healey-director of the Cyber Statecraft Initiative at the Atlantic Council-13

http://www.atlanticcouncil.org/publications/issue-briefs/cyber-conflict-and-the-wpr-congressional-oversight-of-hostilities-in-the-fifth-domain

With the focus on “personnel,” this passage makes clear that the WPR will typically not apply to exclusively cyber conflicts. With cyber warriors executing such operations from centers inside the United States, such as the CYBERCOM facility at Fort Meade, Maryland, at a significant distance from the systems they are attacking and well out of harm’s way. Thus, there is no relevant “introduction” of armed forces. Without such an “introduction,” even the reporting requirements are not triggered. The view that there can be no introduction of forces into cyberspace follows naturally from the administration’s argument that the purpose of the WPR is simply to keep US service personnel out of harm’s way unless authorized by Congress. If devastating unmanned missions do not fall under the scope of the resolution, it is reasonable to argue that a conflict conducted in cyberspace does not either.

## CP

### Legal Certainty – 2NC

#### Streamlines operations

**Young, Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence, 2010**

(Mark, “National Cyber Doctrine: The Missing Link in the Application of American Cyber Power”, <http://jnslp.com/wp-content/uploads/2010/08/12_Young.pdf>, ldg)

A new cyber doctrine will provide guidance on the application of cyberpower in response to a physical attack or as part of a computer network attack initiated by the U.S. government. Under the existing doctrine, a computer network attack “is not integrated with overall [warfare] planning because of the highly compartmented classification that cyber activities receive.”51 A major objective of assembling an interagency team to establish a national cyber doctrine is to improve the integration of cyber defense and offense into joint interagency operational planning. Operations in cyberspace must be “synchronized and coordinated with other operations, just as land and air operations . . . must be synchronized and coordinated.”52 With their current classification, network attack capabilities are misunderstood and not widely employed. A national cyber doctrine should be unclassified to the maximum extent possible. As with other doctrines, a classified annex may be necessary to delineate sensitive capabilities, operations, or relationships. While it is foolish to disclose all the elements of U.S. cyberpower, the foundational principles that govern the applications of cyberpower should be widely disseminated. The development of this doctrine would de-mystify the domain for the national security community and the American people. Federal agencies should participate in the debate to establish this doctrine and help institutionalize its principles across the entire government. This debate can inform the decision on what information must remain classified and what does not need to be classified.

#### Solves turf wars

**Young, Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence, 2010**

(Mark, “National Cyber Doctrine: The Missing Link in the Application of American Cyber Power”, <http://jnslp.com/wp-content/uploads/2010/08/12_Young.pdf>, ldg)

In addition to classification, another issue that can be resolved through interagency development of a national cyber doctrine is the interaction between the U.S. government and the private companies that operate commercial networks over which DoD data flow. Because the vast majority of U.S. commerce is conducted through the Internet, the DoD acknowledges that the DoD must have the capability to protect it. The DoD already relies on private and academic institutions to “assist commercially owned telecommunications networks, communications satellite systems, and other civilian critical infrastructure systems” through the Computer Emergency Response Team.61 The initiation of the doctrine development process within the national security community will force the U.S. government to establish roles and delineate responsibilities for the public and private sector concerning network defense and the use of private networks for offensive operations and intelligence collections. Without a structured forum to debate the concerns over government action on commercial information systems, national security organizations are forced to continue their individual ad hoc solutions that may not hold up in times of crisis. Commercial entities may not cooperate when the U.S. Government requests authority to control portions of their network during national emergencies or during a computer network attack by a foreign force. Jurisdictional arguments or debates about statutory interpretation should not delay national defense during times of national emergencies.

#### Resolves allies and norm concern while maintaining flex

**Young, Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence, 2010**

(Mark, “National Cyber Doctrine: The Missing Link in the Application of American Cyber Power”, <http://jnslp.com/wp-content/uploads/2010/08/12_Young.pdf>, ldg)

In the development of doctrine, foreign partners are almostas important as the intelligence community in offering particular knowledge, expertise, and intelligence capabilities. It is unlikely that any future crisis will be met solely by the United States. Foreign countries and the United States are together on battlefield of Iraq and Afghanistan, and they will be in cyber space as well. Joint Publication 3-13 states: Allies and coalition partners recognize various [information operations] concepts and some have thorough and sophisticated doctrine, procedures, and capabilities for planning and conducting IO. The multinational force commander (MNFC) is responsible to resolve potential conflicts between each nation’s IO programs and the IO objectives and programs of the multinational force. . . . It is vital to integrate allies and coalition partners into IO planning as early as possible so that an integrated and achievable IO strategy can be developed early in the planning process.73 Foreign partners are critical to the success of U.S. military operations in all the domains. A new cyber doctrine will clarify the U.S. policy in cyberspace for all allies. IV. OTHER CONSIDERATIONS The most significant policy issues facing any cyberpower projection is the applicability of the Law of War (LOW). The legal questions must be examined and resolved in detail.74 The relationship between the laws of war and cyber operations will evolve, but a baseline policy position must involve the entire U.S. government**.** Scrutiny should focus on the definitions of “armed attack,” as well as “distinction” and “proportionality” as applied to cyber operations.75 The U.N. Charter provides guidance for responses to armed attacks. The proper classification of cyber activity as an armed attack is much more difficult than the drafters of the U.N. Charter ever envisioned. These issues are ripe for debate and could be addressed in drafting the guiding principles for a national cyber doctrine. There is a presumption that the rules of engagement in cyber doctrine “will follow the [L]aw of Armed Conflict, meaning a response taken after receiving an electronic or cyber attack will be scaled in proportion to the attack received, and distinctions will be maintained between combatants and civilians.”76 This presumption may be significant because adversaries using cyber attacks may not distinguish between civilian and military targets. “Security experts warn that all U.S. federal agencies should now be aware that in cyberspace some malicious actors consider that no boundaries exist between military and civilian targets.”77 The law frequently lags behind technology, but the consequences of adversarial actions against the United States and the responses of the Cyber Command illustrate the importance of establishing legitimate legal bases for defensive and offensive cyber operations. “The potentially nonlethal nature of cyber weapons may cloud the assessment of an attack’s legality, leading to more frequent violations of the principle of distinction in this new form of warfare than in conventional warfare.”78 For these reasons, legal experts in the national security sector must engage in the development of the new cyber doctrine**.** Now is the time for the UnitedStatesto demonstrate its leadership in establishing the proper doctrine for a governmental approach in accordance with the civil and military principles that have led to U.S. freedom of action. CONCLUSION The U.S. Cyber Command was established to defend DoD networks against cyber attacks and to develop offensive cyber capabilities. The creation of this command is a legitimate response to the growing capabilities of nations such as China and Russia as well as non-state actors such as al Qaeda and Hamas. The command was established without an adequate cyber doctrine to guide the application of joint forces in protecting U.S. freedom of action in cyberspace. Only by adopting a comprehensive government approach can the United States bring its full intellectual might to bear on the challenging domain of cyberspace. The joint doctrine development process will allow interagency elements to resolvemanyissues that currently complicate the U.S. approach to cyberpower. The joint doctrine must distinguish computer network operations from their current framework and embrace cyberspace as a war fighting domain. The process will allow debate and resolution of issues such as the training required for a cyber force, the proper classification of U.S. cyber capabilities, the authorities under which computer network attacks may be executed, and actions in cyberspace that implicate the laws of war.This new doctrine will enhance U.S. national security by normalizing cyberspace as a domain through which the UnitedStates can express national values and protect national interests.

#### Clarification is sufficient, don’t need to restrict

**Fox, Maryland Center for Health and Homeland Security, 2012**

(Peter, “Domestic Cybersecurity Requires Clearer Federal Roles and Responsibilities”, <http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/march12/domestic-cyber-security-requires-clearer-federal-roles-and-responsibilities.html>, ldg)

Ambiguities in the legal authorities that differentiate Federal cybersecurity roles and responsibilities impede the nation’s cyber defenses. Extant authorities provide agencies with vague and outdated powers that inhibit rapid response, a legacy of a century’s worth of laws and policies pieced together on an ad hoc basis. As a result, individual agencies have interpreted their authority in a fragmented, uncoordinated manner that may create cybersecurity gaps and vulnerabilities. In May 2009, just four months after his inauguration, President Barack Obama established an Office of cybersecurity within the National Security Staff and ordered a “clean-slate” review of the existing cyberspace environment. Foremost among the 2009 Cyberspace Policy Review’s findings was a lack of coherent policy guidance clarifying “authorities, roles, and responsibilities for cybersecurity-related activities across the Federal government.” The review described an inadequate “patchwork of Constitutional, domestic, foreign and international laws” resulting from a history of diverse and evolving industries and technologies. It recommended that the Federal government “integrate competing interests to derive a holistic vision and [cybersecurity] plan.” In May 2011, the Homeland Security Studies and Analysis Institute (HSI) published a report that analyzed the key legal authorities governing DHS’s role in securing civilian government cyberspace and supporting critical infrastructure defenses. HSI reviewed specific language from primary authorities including Homeland Security Presidential Directives, Executive Orders, and significant legislation such as the Communications Act of 1934, the Electronic Communications Privacy Act of 1986, the Stafford Act, and the Homeland Security Act of 2002. The report revealed that “a lack of clarity prevails” in primary authorities, whose ambiguous language typically directs DHS to coordinate, facilitate, provide, manage or identify information, standards, and resources without granting DHS explicit power to intervene or compel action by relevant entities. HSI’s research was an additional indictment of the status quo described in the White House report; it concluded that existing authorities governing DHS cybersecurity responsibilities “may not be fully sufficient” for DHS to coordinate incident response, define its own cybersecurity intervention powers, require information sharing, or protect critical infrastructure. Even worse, HSI suggested that “existing authorities may not sufficiently delineate the responsibilities of DHS and DoD for the most serious of incidents, including incidents affecting national security or defense of the United States.” While the White House focused on streamlining cyber security policy across the Federal government, DoD unified its internal cyber-defense architecture. In 2010, DoD established U.S. Cyber Command (USCYBERCOM) as a sub-unit of U.S. Strategic Command in Fort Meade, Maryland, where it is co-located with the NSA. USCYBERCOM centralizes DoD’s cyberspace operations, placing one thousand elite military cyber experts under the command of General Keith B. Alexander, who is also the Director of the NSA. DoD now considers cyberspace a fifth military domain, along with land, air, sea and space. DoD’s Strategy for Operating in Cyberspace, released in July 2011, emphasizes more “active defenses” and reduced incentives for attacks, rather than retaliatory operations. Regrettably, DoD legal authorities provide equally inadequate guidance for its participation in domestic, non-military cyber operations. The military is not empowered to take unilateral action within the U.S. to protect civilian networks or critical infrastructure, but DoD Directives 3025.12 and 5525.5, as well as 32 CFR part 215.4, authorize military intervention to support civil authorities in order to prevent “significant loss of life,” “wanton destruction of property,” or to protect Federal government property or functions when they cannot protect themselves. This language may authorize DoD to intervene in a cyber event that falls within these vague scenarios, but the triggers for such intervention are unclear. General Alexander has acknowledged that USCYBERCOM’s current authority is limited to defending military computer networks. He has stated publicly that he does not “have the authority to look at what’s going on in other government sectors nor what would happen to critical infrastructure.” The dilemma concerning unclear Federal agency responsibilities is exacerbated by the technical problem of cyber attack attribution – the ability to accurately identify the origins of web and network attacks. Who is responsible for responding to a cyber attack that impacts national security or defense – DHS or DoD? The open nature of the internet erodes distinctions between domestic criminal law enforcement and defense of the national borders because it enables an attacker to falsify their IP address and disguise their identity by routing through proxy servers or employing botnets. Even when the technical capacity exists to trace the origin of an attack to a precise location, it is impossible to know exactly who is sitting at the keyboard executing the assault. In recognition of these persistent challenges to coordinated Federal oversight of domestic cybersecurity, the agencies themselves have moved towards a whole-of-government approach to ensure a rapid response to cyber threats. In a Memorandum of Agreement (MOA) signed in September 2010 by Secretary Janet Napolitano of DHS and Secretary Robert M. Gates of DoD, the agencies adopted new procedures for leveraging DoD’s cyber warfare capabilities to defend domestic civilian networks. Similar to protocols followed during natural disasters, where military forces are dispatched by Presidential order under the direction of the Federal Emergency Management Agency, DoD’s cyber warfare expertise is now dispatched under the direction of DHS. The MOA sidesteps legal questions about DoD’s authority to operate domestically in order to utilize its capabilities to protect domestic networks and critical infrastructure. Under the agreement, DoD cyber analysts are embedded within DHS. To alleviate concerns of military mission creep that could put civil liberties at risk, privacy, civil liberties, and legal personnel from DHS monitor activities within USCYBERCOM. The DoD-DHS agreement recognizes that the decentralized nature of the internet may necessitate a decentralized, whole-of-government approach to cybersecurity. Although there may be a tendency to embrace solutions that simplify the cybersecurity landscape by centralizing power in the hands of a single agency, policy makers should be mindful that cyber attacks are multifaceted, distributed threats. Different agencies have dissimilar abilities and expertise, particularly across the civilian and military spheres. The DoD-DHS MOA is a practical first step towards reorganizing U.S. cyber defenses, but an integrated Federal response will require codifying clearly articulated roles and responsibilities for each agency. If civilian and military legal authorities are carefully amended to facilitate a combination of cyber expertise and protection of civil liberties, DHS and DoD can cooperatively maintain their separate but complementary missions.

#### The CP clears up all legal confusion

**Brennan, US Army Lieutenant Colonel, 2012**

(John, “United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?”, 3-15, <http://nsfp.web.unc.edu/files/2012/09/Brennan_UNITED-STATES-COUNTER-TERRORISM-CYBER-LAW-AND-POLICY.pdf>, ldg)

The bulk of the recommendations provided below concern possible modifications to existing CT cyber policies in order to bring them better into alignment with existing laws and strategies. Through its key cyber strategy document, DoD has determined that cyberspace is a military domain similar to the those of land, sea, and air; therefore as the overarching framework, CT cyber operations within an AOH should be governed by the law of armed conflict (LOAC).70 For those targets (and supporting cyber infrastructure) that lie outside of the current AOH, military CT cyber operations should be utilized only in the execution of targets that are pursuant to the current AUMF. The first step in rectifying the CT cyber policy should be for the IC and DoD to accurately define and properly name CT cyber operations. This may be effectively accomplished through the merger of both the IC and DoD cyber lexicon. The names given to CT cyber operations should be derived on the basis of the desired effects of the operation. If a cyber operation produces a kinetic effect that is intended to destroy terrorists or their equipment, then it should be labeled a “CT cyber attack (CCA).” If the desired effect of a CT cyber operation is to manipulate terrorists’ data, equipment, or minds (i.e. cyber deception), then the operation should be dubbed an “offensive CT cyber operation (OCCO).” Standard intelligence collection of terrorists’ cyber networks in support of either a military commander or the IC should simply be labeled “CT cyber collection (CCC). Next, the above CT cyber capabilities and operations should be appropriately matched to their approval level, and the resources to conduct such operations should likewise be provided to that approving authority. At least on the tactical U. S. military level, the approvals to conduct cyber operations that only effect a limited population or area of operation within an AOH, should be governed by a much lower level of command than current policies dictate. For that matter, the capability to conduct low-level, localized CT cyber operations that anticipate little or no international repercussions (Offensive CT Cyber Operations and CT Cyber Collection) should be provided down the O6 (Colonel) level of command or whatever level of command is authorized to conduct offensive kinetic operations of similar size and scope. Brigade Combat Team (BCT) commanders are assigned large swaths of battlespace in Afghanistan, and their ability to leverage CT cyber capabilities and approve OCCOs and CCCs would definitely increase the efficacy and pace of CT operations within the AOH. The authorities to conduct CT Cyber Attacks (CCA) should be retained by the AOH theater commander or his designated representative. If the effects of a CCA will likely spill outside of the AOH, then the Geographical Combatant Commander or his designated representative should be the approving authority to the same extent that they approve traditional kinetic operations. In each instance, the overriding theme should be to delegate execution authority down to the lowest level feasible in order to maximize the effects of CT cyber operations. Cyber operations are not exclusively a military capability, despite the fact that the great preponderance of cyber operations are conducted by the NSA (a DoD Agency), and they have proven to be a key enabler to the success of many overseas CT operations. If DoD and the greater IC continue to refuse to come to an agreement on which agency should execute which types of cyber operations, then the White House should settle the issue through the drafting of a comprehensive CT cyber policy. This policy should generally outline which agencies have primacy for certain types of operations, which will at least settle the matter of who is in charge. In order to avoid the time-consuming task of attempting to rewrite the U. S. Code (that does not require revision), the next set of recommendations will serve to attempt to generally delineate which authorities should be employed, under which circumstances, in the conduct of CT cyber operations. If a CT cyber operation is conducted in support of a military commander, and/or as a part of, or in advance of, a larger military operation, then Title 10 authorities should be employed, even in the event that 3rd party data systems are manipulated outside of an AOH. The data manipulation should be permissible so long as the manipulation does not destroy or disrupt the service or equipment of civilians uninvolved in the conflict concerned. Conversely, if a cyber operation is conducted as, or in support of, a covert action completely independent of, or outside of an existing AOH, then Title 50 authorities should be leveraged in accordance with appropriate congressional oversight. In order to perform their tasks, CT cyber professionals may be required to access servers or equipment that is not located within an AOH, and is frequently located within a friendly country. As long as that equipment or the individuals that operate it are not harmed, then the operations should not necessarily be deemed a covert action. The logic behind this recommendation is due largely to the fact that most cyber operations are by their very nature, deniable.

### 2NC Future Presidents Rollback

#### ---Political barriers check – new, stronger constituencies

Branum-Associate Fulbright and Jaworski- 2

Tara L, Associate, Fulbright & Jaworski L.L.P, “President or King? The Use and Abuse of Executive Orders in Modern Day America” Journal of Legislation 28 J. Legis. 1

Congressmen and private citizens besiege the President with demands  [\*58]  that action be taken on various issues. [n273](http://www.lexisnexis.com/us/lnacademic/frame.do?tokenKey=rsh-20.689002.875983458&target=results_DocumentContent&reloadEntirePage=true&rand=1220903297496&returnToKey=20_T4511783216&parent=docview" \l "n273) To make matters worse, once a president has signed an executive order, he often makes it impossible for a subsequent administration to undo his action without enduring the political fallout of such a reversal. For instance, President Clinton issued a slew of executive orders on environmental issues in the weeks before he left office. [n274](http://www.lexisnexis.com/us/lnacademic/frame.do?tokenKey=rsh-20.689002.875983458&target=results_DocumentContent&reloadEntirePage=true&rand=1220903297496&returnToKey=20_T4511783216&parent=docview" \l "n274) Many were controversial and the need for the policies he instituted was debatable. [n275](http://www.lexisnexis.com/us/lnacademic/frame.do?tokenKey=rsh-20.689002.875983458&target=results_DocumentContent&reloadEntirePage=true&rand=1220903297496&returnToKey=20_T4511783216&parent=docview" \l "n275) Nevertheless, President Bush found himself unable to reverse the orders without invoking the ire of environmentalists across the country. [n276](http://www.lexisnexis.com/us/lnacademic/frame.do?tokenKey=rsh-20.689002.875983458&target=results_DocumentContent&reloadEntirePage=true&rand=1220903297496&returnToKey=20_T4511783216&parent=docview" \l "n276) A policy became law by the action of one man without the healthy debate and discussion in Congress intended by the Framers. Subsequent presidents undo this policy and send the matter to Congress for such debate only at their own peril. This is not the way it is supposed to be.

#### ---Future administrations rarely overturn previous executive orders

Washington Times 8/23/99

“Clinton’s Executive Orders are Still Packing a Punch: Other Presidents Issued More, but His are Still Sweeping” Frank Murray [http://www.questia.com/library/1G1-55543736/clinton-s-executive-orders-still- are-packing-a-punch](http://www.questia.com/library/1G1-55543736/clinton-s-executive-orders-still-%20are-packing-a-punch)

Clearly, Mr. Clinton knew what some detractors do not: Presidential successors of the opposite party do not lightly wipe the slate clean of every order, or even most of them. Still on the books 54 years after his death are 80 executive orders issued by Franklin D. Roosevelt. No less than 187 of Mr. Truman's orders remain, including one to end military racial segregation, which former Joint Chiefs of Staff Chairman Colin Powell praised for starting the "Second Reconstruction." "President Truman gave us the order to march with Executive Order 9981," Mr. Powell said at a July 26, 1998 ceremony marking its 50th anniversary. Mr. Truman's final order, issued one day before he left office in 1953, created a national security medal of honor for the nation's top spies, which is still highly coveted and often revealed only in the obituary of its recipient.

### AT: Dycus

#### Dycus is purley theory---says Congress could play an active role in creating reporting requirements and creating a dialogue about cyber and hostilities that mirrors national values---the Young card is the only one in the debate that advocates a policy that can do those things

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

III. ALEGISLATIVE HAND ON THE CYBER WAR MOUSE Cyber warfare, as that term is used here, refers to conflicts that utilize cyber or electronic weapons either offensively or defensively, or both. Cyber weapons are currently employed offensively in kinetic warfare, for example, to suppress an enemy’s air defenses or disrupt its communications, or defensively to track enemy troop movements. These weapons might also be used offensively to disable an enemy’s cyber weaponry or defensively in response to an enemy attack, to prevent further aggression. The term “cybersecurity” might be understood to refer to defense against cyber attacks. “Cyber attack” suggests offensive use, but the label is inexact and might be misleading. A preemptive strike to ward off an imminent enemy attack is considered defensive. Digital espionage might be part of the preparation for an attack, or it might be perceived that way by the target, which might then be provoked to defend itself by responding with a preemptive attack, either cyber or kinetic. The important point here is that any use of cyber weapons, offensive or defensive, could have enormous consequences for the security and other interests of the United States. The effect of such use, actual or potential, matters more than the labels. And if the effect – on human life or property, for example, or diplomatic relations or compliance with the law of armed conflict – is substantial, Congress has a role to play in adopting policy for that use. Congress has not thus far adopted measures suited to the regulation of cyber warfare. The War Powers Resolution, for example, is concerned with sending U.S. troops into harm’s way, rather than with clicking a computer mouse to launch a cyber attack, although the strategic consequences might be similar. And the WPR’s relatively relaxed timetable for executive notice and legislative response is unrealistic for war on a digital battlefield. Similarly, if cyber warfare is regarded as an intelligence activity, the intelligence oversight measures just described cannot, for reasons already indicated, ensure that Congress will be able to play a meaningful role. In the words of the National Research Council study cited above, “Today’s policy and legal framework for guiding and regulating the use of cyberattack is ill-formed, undeveloped, and highly uncertain.”45 Our experience with nuclear weapons may point to needed reforms. Since the beginning of the Cold War, the United States has had a fairly clear nuclear policy (albeit one that deliberately includes an element of ambiguity) – one known generally to Congress, the American public, and potential enemies.46 Congress has approved or disapproved the purchase of the weapons and delivery systems. It has been briefed on the policy, and it has debated that policy vigorously.47 While Congress has not articulated U.S. nuclear policy in any coherent form, it has collaborated closely with the executive branch in the development and execution of that policy. Cyber weapons bear a striking resemblance to nuclear weapons in some important ways. An enemy’s cyber attack would, like a nuclear strike, probably come without a clear warning. There are as yet no reliable defenses against either a cyber attack or a nuclear attack. Collateral damage from a nuclear attack would almost certainly be very extensive and would linger for an extended period.48 The direct and indirect effects of a cyber attack, while different in kind and degree, still could be widespread and indiscriminate.49 In other ways, cyber weapons are critically different from their nuclear counterparts. For one thing, the time frame for response to a cyber attack might be much narrower. A nuclear weapon delivered by a land-based ICBM could take 30 minutes to reach its target. An electronic attack would arrive instantaneously, and leave no time to consult with or even inform anyone outside the executive branch before launching a counterstrike, if that were U.S. policy. What most distinguishes digital warfare, however, is the potential difficulty in identifying the source of a cyber attack. It is always possible, of course, that an enemy might covertly deliver a nuclear device to the U.S. homeland in a shipping container or a Cessna. But the apparent ease with which a cyber attack may be carried out without attribution could make it impossible to fight back at all. If an attacker made it appear that the source was an innocent neutral state or perhaps another enemy of the attacker, a misdirected U.S. response might provoke a wider conflict. The potential difficulty in tracking the source also makes a policy of deterrence based on a threat of retaliation far less credible. Given these characteristics of cyber warfare, and the continuing refinement of cyber weaponry, we approach a state of extreme strategic instability, with each nation on hair-trigger alert. The execution of an illconceived cyber war policy calling for a prompt response – or any response – to an attack or threatened attack could have disastrous, unanticipated consequences. It also might, depending on the circumstances, violate the law of armed conflict. Congress accordingly needs to work closely with the executive branch in the development of a policy for this new kind of conflict. Such a policy ought to reflect the distinctive technology and strategy of digital warfare, and it should be reviewed constantly as the technology evolves. Like other regulations dealing with dynamic subjects, this policy should include general approaches that reflect this nation’s broad strategic concerns and fundamental values. But the policy must also be crafted with enough flexibility to allow those charged with its execution to deal with future developments that cannot now be predicted. And it should set out a procedure for such adaptive use by identifying, for example, who must be consulted under what circumstances, and who will make the final critical decisions. It is at least theoretically possible that Congress could play an active, real-time role in the implementation of whatever cyber warfare policy is adopted. The policy might, for example, like the War Powers Resolution, require consultation “in every possible circumstance.”50 But it seems more likely that a digital war would begin and end before any notice could ever reach Capitol Hill. Congress therefore needs to lay down clear guidelines, with as much flexibility as prudence requires, for executive branch officials to follow if consultation is not reasonably possible. And Congress should require a prompt and full account of every significant use of cyber weapons.

### 2NC Perm-Do CP-Statutory

#### A. It severs congressional action

Kershner-JD Candidate, Cardoza-10 (Joshua, Articles Editor, Cardozo Law Review. J.D. Candidate (June 2011), Benjamin N. Cardozo School of Law, “Political Party Restrictions and the Appointments Clause: The Federal Election Commission's Appointments Process Is Constitutional” Cardozo Law Review de novo 2010 Cardozo L. Rev. De Novo 615)

n17 The phrase "statutory restrictions" is used hereinafter to mean statutory language that restricts the President's powers of nomination and appointment to those individuals meeting specific criteria. Examples include gender, state of residence, and most importantly political party. n18 Since 1980, more than one hundred Presidential signing statements have specifically mentioned the Appointments Clause. See The Public Papers of the Presidents, AM. PRESIDENCY PROJECT, http://www.presidency.ucsb.edu/ws (search for "Appointments Clause"). n19 These signing statements typically invoke the authority of the Appointments Clause to argue that statutory restrictions on appointment or removal of Officers of the United States are merely advisory. For numerous examples, see id. See also infra note 175. n20 The phrase "hyper-partisan atmosphere" has been frequently used by the news media and commentators to describe the political gridlock in Washington during the first years of the Obama administration. See, e.g., Eric Moskowitz, Hundreds Brave Cold to Hear From Scott Brown, THE BOSTON GLOBE, Jan. 29, 2010, http://www.boston.com/news/local/breaking\_news/2010/01/scores\_wait\_for.html (reporting on then Senator-Elect Scott Brown explaining that "he felt the hyper-partisan atmosphere in Washington was already changing as a result of his election" ten days earlier); Editorial, Bayh Bailout No Cause to Mourn Moderation, ORANGE COUNTY REG., Feb. 17, 2010, at H, available at http://www.ocregister.com/opinion/bayh-234673-sen-one.html (describing Senator Bayh's verbal attacks on the operation of the Senate after announcing his decision not to run for reelection as "using the occasion to decry the hyperpartisan atmosphere in Washington"). n21 As political battles over delays in approving Presidential nominations continue to be the norm, it is progressively more likely that Presidents will seek to bypass the Senate in the nomination process. This could include recess appointments bypassing both the "advice and consent" of the Senate, as well as any statutory restrictions. See, e.g., Scott Wilson, Obama Considers Recess Appointments, WASH. POST, Feb. 9, 2010 ("President Obama is considering recess appointments to fill some or all of the nominations held up in the Senate. President Bush used a recess appointment to make John Bolton the U.S. ambassador to the United Nations bypassing Democrats."). n22 Statutory restrictions date back to the first Congress and continue today. See infra notes 116, 118, 122. n23 See discussion infra Part I.D and note 128. n24 The phrase "political party restrictions" is used hereinafter to mean statutory restrictions on the President's powers of nomination and appointment by political party.

B. Severance is illegitimate and a voting issue. It destroys negative ground since no counterplan would compete if the 2AC could pick and choose what parts of the plan to defend. It also makes the plan a moving target and conditional. Affirmative conditionality is worse than negative conditionality because the plan is the focus of

## WPR Adv

### 2NC Groupthink

### A2: Bad Interventions/Better Decisionmaking

#### Checks on executive overreach-no bad interventions

**Yoo, UC Berkeely law professor, 2009**

(John, Crisis and Command, google books)

A second lesson of this book is that the notion of an unchecked executive, wielding dictatorial powers to plunge the nation into disaster, is a myth born of Vietnam and Watergate. Congresses have always possessed ample ability to stalemate and check an executive run amok. Congress regularly ignores executive proposals for legislation, rejects nominees, and overrides vetoes. It can use its power over legislation, funding, and oversight to exercise significant control over the administrative state. There would be no agencies, no delegated powers, and no rule-making without Congress's basic decisions to create the federal bureaucracy. It can use these authorities even at the zenith of presidential power: foreign affairs. Congress can cut off war funding, shrink the military, stop economic aid, and block treaties. It used its sole control of the purse to limit the Mexican-American War and to end the Vietnam conflict, for example.

### Heg D

#### No transition wars-disengagement doesn’t correlate with aggression

**Parent et al., Miami political science professor, 2011**

(Joseph, “The Wisdom of Retrenchment”, Foreign Affairs, November/December, ebsco, ldg)

A somewhat more compelling concern raised by opponents of retrenchment is that the policy might undermine deterrence. Reducing the defense budget or repositioning forces would make the United States look weak and embolden upstarts, they argue. "The very signaling of such an aloof intention may encourage regional bullies," Kaplan worries. This anxiety is rooted in the assumption that the best barrier to adventurism by adversaries is forward defenses--the deployment of military assets in large bases near enemy borders, which serve as tripwires or, to some eyes, a Great Wall of America. There are many problems with this position. For starters, the policies that have gotten the United States in trouble in recent years have been activist, not passive or defensive. The U.S.-led invasion of Iraq alienated important U.S. allies, such as Germany and Turkey, and increased Iran's regional power. NATO's expansion eastward has strained the alliance and intensified Russia's ambitions in Georgia and Ukraine. More generally, U.S. forward deployments are no longer the main barrier to great-power land grabs. Taking and holding territory is more expensive than it once was, and great powers have little incentive or interest in expanding further. The United States' chief allies have developed the wherewithal to defend their territorial boundaries and deter restive neighbors. Of course, retrenchment might tempt reckless rivals to pursue unexpected or incautious policies, as states sometimes do. Should that occur, however, U.S. superiority in conventional arms and its power-projection capabilities would assure the option of quick U.S. intervention. Outcomes of that sort would be costly, but the risks of retrenchment must be compared to the risks of the status quo. In difficult financial circumstances, the United States must prioritize. The biggest menace to a superpower is not the possibility of belated entry into a regional crisis; it is the temptation of imperial overstretch. That is exactly the trap into which opponents of the United States, such as al Qaeda, want it to fall. Nor is there good evidence that reducing Washington's overseas commitments would lead friends and rivals to question its credibility. Despite some glum prophecies, the withdrawal of U.S. armed forces from western Europe after the Cold War neither doomed NATO nor discredited the United States. Similar reductions in U.S. military forces and the forces' repositioning in South Korea have improved the sometimes tense relationship between Washington and Seoul. Calls for Japan to assume a greater defense burden have likewise resulted in deeper integration of U.S. and Japanese forces. Faith in forward defenses is a holdover from the Cold War, rooted in visions of implacable adversaries and falling dominoes. It is ill suited to contemporary world politics, where balancing coalitions are notably absent and ideological disputes remarkably mild.

#### No transition war-countries buy into the syste

**Ikenberry, Princeton international affairs professor, 2010**

(John, “The Liberal International Order and its Discontents”, Millennium - Journal of International Studies, May, Sage, ldg)

Secondly, this order is also distinctive in its integrative and expansive character. In essence, it is ‘easy to join and hard to overturn’. This follows most fundamentally from the fact that it is a liberal international order – in effect, it is an order that is relatively open and loosely rulebased. The order generates participants and stakeholders. Beyond this, there are three reasons why the architectural features of this post-war liberal order reinforce downward and outward integration. One is that the multilateral character of the rules and institutions create opportunities for access and participation. Countries that want to join in can do so; Japan found itself integrating through participation in the trade system and alliance partnership. More recently, China has taken steps to join, at least through the world trading system. Joining is not costless. Membership in institutional bodies such as the WTO must be voted upon by existing members and states must meet specific requirements. But these bodies are not exclusive or imperial. Secondly, the liberal order is organised around shared leadership and not just the United States. The G-7/8 is an example of a governance organisation that is based on a collective leadership, and the new G-20 grouping has emerged to provide expanded leadership. Finally, the order also provides opportunities for a wide array of states to gain access to the ‘spoils of modernity’. Again, this is not an imperial system in which the riches accrue disproportionately to the centre. States across the system have found ways to integrate into this order and experience economic gains and rapid growth along the way. Thirdly, rising states do not constitute a bloc that seeks to overturn or reorganise the existing international order. China, India, Russia, Brazil, South Africa and others all are seeking new roles and more influence within the global system. But they do not constitute a new coalition of states seeking global transformation. All of these states are capitalist and as such are deeply embedded in the world economy. Most of them are democratic and embrace the political principles of the older Western liberal democracies. At the same time, they all have different geopolitical interests. They are as diverse in their orientations as the rest of the world in regard to energy, religion and ideologies of development. They are not united by a common principled belief in a post-liberal world order. They are all very much inside the existing order and integrated in various ways into existing governance institutions.

#### Can’t leverage hegemony

**Maher, Brown political science professor, 2011**

(Richard, “The Paradox of American Unipolarity: Why the United States May Be Better Off in a Post-Unipolar World”, Orbis, 55.1, Science Direct, ldg)

At the same time, preeminence creates burdens and facilitates imprudent behavior. Indeed, because of America’s unique political ideology, which sees its own domestic values and ideals as universal, and the relative openness of the foreign policymaking process, the United States is particularly susceptible to both the temptations and burdens of preponderance. For decades, perhaps since its very founding, the United States has viewed what is good for itself as good for the world. During its period of preeminence, the United States has both tried to maintain its position at the top and to transform world politics in fundamental ways, combining elements of realpolitik and liberal universalism (democratic government, free trade, basic human rights). At times, these desires have conflicted with each other but they also capture the enduring tensions of America’s role in the world. The absence of constraints and America’s overestimation of its own ability to shape outcomes has served to weaken its overall position. And because foreign policy is not the reserved and exclusive domain of the president---who presumably calculates strategy according to the pursuit of the state’s enduring national interests---the policymaking process is open to special interests and outside influences and, thus, susceptible to the cultivation of misperceptions, miscalculations, and misunderstandings. Five features in particular, each a consequence of how America has used its power in the unipolar era, have worked to diminish America’s long-term material and strategic position. Overextension. During its period of preeminence, the United States has found it difficult to stand aloof from threats (real or imagined) to its security, interests, and values. Most states are concerned with what happens in their immediate neighborhoods. The United States has interests that span virtually the entire globe, from its own Western Hemisphere, to Europe, the Middle East, Persian Gulf, South Asia, and East Asia. As its preeminence enters its third decade, the United States continues to define its interests in increasingly expansive terms. This has been facilitated by the massive forward presence of the American military, even when excluding the tens of thousands of troops stationed in Iraq and Afghanistan. The U.S. military has permanent bases in over 30 countries and maintains a troop presence in dozens more.13 There are two logics that lead a preeminent state to overextend, and these logics of overextension lead to goals and policies that exceed even the considerable capabilities of a superpower. First, by definition, preeminent states face few external constraints. Unlike in bipolar or multipolar systems, there are no other states that can serve to reliably check or counterbalance the power and influence of a single hegemon. This gives preeminent states a staggering freedom of action and provides a tempting opportunity to shape world politics in fundamental ways. Rather than pursuing its own narrow interests, preeminence provides an opportunity to mix ideology, values, and normative beliefs with foreign policy. The United States has been susceptible to this temptation, going to great lengths to slay dragons abroad, and even to remake whole societies in its own (liberal democratic) image.14 The costs and risks of taking such bold action or pursuing transformative foreign policies often seem manageable or even remote. We know from both theory and history that external powers can impose important checks on calculated risk-taking and serve as a moderating influence. The bipolar system of the Cold War forced policymakers in both the United States and the Soviet Union to exercise extreme caution and prudence. One wrong move could have led to a crisis that quickly spiraled out of policymakers’ control. Second, preeminent states have a strong incentive to seek to maintain their preeminence in the international system. Being number one has clear strategic, political, and psychological benefits. Preeminent states may, therefore, overestimate the intensity and immediacy of threats, or to fundamentally redefine what constitutes an acceptable level of threat to live with. To protect itself from emerging or even future threats, preeminent states may be more likely to take unilateral action, particularly compared to when power is distributed more evenly in the international system. Preeminence has not only made it possible for the United States to overestimate its power, but also to overestimate the degree to which other states and societies see American power as legitimate and even as worthy of emulation. There is almost a belief in historical determinism, or the feeling that one was destined to stand atop world politics as a colossus, and this preeminence gives one a special prerogative for one’s role and purpose in world politics. The security doctrine that the George W. Bush administration adopted took an aggressive approach to maintaining American preeminence and eliminating threats to American security, including waging preventive war. The invasion of Iraq, based on claims that Saddam Hussein possessed weapons of mass destruction (WMD) and had ties to al Qaeda, both of which turned out to be false, produced huge costs for the United States---in political, material, and human terms. After seven years of war, tens of thousands of American military personnel remain in Iraq. Estimates of its long-term cost are in the trillions of dollars.15 At the same time, the United States has fought a parallel conflict in Afghanistan. While the Obama administration looks to dramatically reduce the American military presence in Iraq, President Obama has committed tens of thousands of additional U.S. troops to Afghanistan. Distraction. Preeminent states have a tendency to seek to shape world politics in fundamental ways, which can lead to conflicting priorities and unnecessary diversions. As resources, attention, and prestige are devoted to one issue or set of issues, others are necessarily disregarded or given reduced importance. There are always trade-offs and opportunity costs in international politics, even for a state as powerful as the United States. Most states are required to define their priorities in highly specific terms. Because the preeminent state has such a large stake in world politics, it feels the need to be vigilant against any changes that could impact its short-, medium-, or longterm interests. The result is taking on commitments on an expansive number of issues all over the globe. The United States has been very active in its ambition to shape the postCold War world. It has expanded NATO to Russia’s doorstep; waged war in Bosnia, Kosovo, Iraq, and Afghanistan; sought to export its own democratic principles and institutions around the world; assembled an international coalition against transnational terrorism; imposed sanctions on North Korea and Iran for their nuclear programs; undertaken ‘‘nation building’’ in Iraq and Afghanistan; announced plans for a missile defense system to be stationed in Poland and the Czech Republic; and, with the United Kingdom, led the response to the recent global financial and economic crisis. By being so involved in so many parts of the world, there often emerges ambiguity over priorities. The United States defines its interests and obligations in global terms, and defending all of them simultaneously is beyond the pale even for a superpower like the United States. Issues that may have received benign neglect during the Cold War, for example, when U.S. attention and resources were almost exclusively devoted to its strategic competition with the Soviet Union, are now viewed as central to U.S. interests. Bearing Disproportionate Costs of Maintaining the Status Quo. As the preeminent power, the United States has the largest stake in maintaining the status quo. The world the United States took the lead in creating---one based on open markets and free trade, democratic norms and institutions, private property rights and the rule of law---has created enormous benefits for the United States. This is true both in terms of reaching unprecedented levels of domestic prosperity and in institutionalizing U.S. preferences, norms, and values globally. But at the same time, this system has proven costly to maintain. Smaller, less powerful states have a strong incentive to free ride, meaning that preeminent states bear a disproportionate share of the costs of maintaining the basic rules and institutions that give world politics order, stability, and predictability. While this might be frustrating to U.S. policymakers, it is perfectly understandable. Other countries know that the United States will continue to provide these goods out of its own self-interest, so there is little incentive for these other states to contribute significant resources to help maintain these public goods.16 The U.S. Navy patrols the oceans keeping vital sea lanes open. During financial crises around the globe---such as in Asia in 1997-1998, Mexico in 1994, or the global financial and economic crisis that began in October 2008--- the U.S. Treasury rather than the IMF takes the lead in setting out and implementing a plan to stabilize global financial markets. The United States has spent massive amounts on defense in part to prevent great power war. The United States, therefore, provides an indisputable collective good---a world, particularly compared to past eras, that is marked by order, stability, and predictability. A number of countries---in Europe, the Middle East, and East Asia---continue to rely on the American security guarantee for their own security. Rather than devoting more resources to defense, they are able to finance generous social welfare programs. To maintain these commitments, the United States has accumulated staggering budget deficits and national debt. As the sole superpower, the United States bears an additional though different kind of weight. From the Israeli-Palestinian dispute to the India Pakistan rivalry over Kashmir, the United States is expected to assert leadership to bring these disagreements to a peaceful resolution. The United States puts its reputation on the line, and as years and decades pass without lasting settlements, U.S. prestige and influence is further eroded. The only way to get other states to contribute more to the provision of public goods is if the United States dramatically decreases its share. At the same time, the United States would have to give other states an expanded role and greater responsibility given the proportionate increase in paying for public goods. This is a political decision for the United States---maintain predominant control over the provision of collective goods or reduce its burden but lose influence in how these public goods are used. Creation of Feelings of Enmity and Anti-Americanism. It is not necessary that everyone admire the United States or accept its ideals, values, and goals. Indeed, such dramatic imbalances of power that characterize world politics today almost always produce in others feelings of mistrust, resentment, and outright hostility. At the same time, it is easier for the United States to realize its own goals and values when these are shared by others, and are viewed as legitimate and in the common interest. As a result of both its vast power but also some of the decisions it has made, particularly over the past eight years, feelings of resentment and hostility toward the United States have grown, and perceptions of the legitimacy of its role and place in the world have correspondingly declined. Multiple factors give rise toanti-American sentiment, and anti-Americanism takes different shapes and forms.17 It emerges partly as a response to the vast disparity in power the United States enjoys over other states. Taking satisfaction in themissteps and indiscretions of the imposing Gulliver is a natural reaction. In societies that globalization (which in many parts of the world is interpreted as equivalent to Americanization) has largely passed over, resentment and alienation are felt when comparing one’s own impoverished, ill-governed, unstable society with the wealth, stability, and influence enjoyed by the United States.18 Anti-Americanism also emerges as a consequence of specific American actions and certain values and principles to which the United States ascribes. Opinion polls showed that a dramatic rise in anti-American sentiment followed the perceived unilateral decision to invade Iraq (under pretences that failed to convince much of the rest of the world) and to depose Saddam Hussein and his government and replace itwith a governmentmuchmore friendly to the United States. To many, this appeared as an arrogant and completely unilateral decision by a single state to decide for itselfwhen---and under what conditions---military force could be used. A number of other policy decisions by not just the George W. Bush but also the Clinton and Obama administrations have provoked feelings of anti-American sentiment. However, it seemed that a large portion of theworld had a particular animus for GeorgeW. Bush and a number of policy decisions of his administration, from voiding the U.S. signature on the International Criminal Court (ICC), resisting a global climate change treaty, detainee abuse at Abu Ghraib in Iraq and at Guantanamo Bay in Cuba, and what many viewed as a simplistic worldview that declared a ‘‘war’’ on terrorism and the division of theworld between goodand evil.Withpopulations around theworld mobilized and politicized to a degree never before seen---let alone barely contemplated---such feelings of anti-American sentiment makes it more difficult for the United States to convince other governments that the U.S.’ own preferences and priorities are legitimate and worthy of emulation. Decreased Allied Dependence. It is counterintuitive to think that America’s unprecedented power decreases its allies’ dependence on it. During the Cold War, for example, America’s allies were highly dependent on the United States for their own security. The security relationship that the United States had with Western Europe and Japan allowed these societies to rebuild and reach a stunning level of economic prosperity in the decades following World War II. Now that the United States is the sole superpower and the threat posed by the Soviet Union no longer exists, these countries have charted more autonomous courses in foreign and security policy. A reversion to a bipolar or multipolar system could change that, making these allies more dependent on the United States for their security. Russia’s reemergence could unnerve America’s European allies, just as China’s continued ascent could provoke unease in Japan. Either possibility would disrupt the equilibrium in Europe and East Asia that the United States has cultivated over the past several decades. New geopolitical rivalries could serve to create incentives for America’s allies to reduce the disagreements they have with Washington and to reinforce their security relationships with the United States.

# 1NR

### O/V

#### Turns case

#### -Cyberwar – OCO solves their arms race adv-deters cyber escalation

Beidleman, USAF lieutenant colonel, 2009

(Scott, “Defining and Deterring Cyber War”, <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA500795>, ldg)

In general, deterrence is a state of mind. It is the concept of one state influencing another state to choose not to do something that would conflict with the interests of the influencing state. Similarly, the central idea of deterrence from the perspective of the Department of Defense is “to decisively influence the adversary’s decision-making calculus in order to prevent hostile actions against U.S. vital interests.”82 Deterred states decide not to take certain actions because they perceive or fear that such actions would produce intolerable consequences.83 The idea of influencing states’ decisions assumes that states are rational actors “willing to weigh the perceived costs of an action against the perceived benefits, and to choose a course of action” logically based on “some reasonable cost-benefit ratio.”84 Thus the efficacy of cyber deterrence relies on the ability to impose or raise costs and to deny or lower benefits related to cyber attack in a state’s decision-making calculus. Credible cyber deterrence is also dependent on a state’s willingness to use these abilities and a potential aggressor’s awareness that these abilities, and the will to use them, exist. While a state’s ability to deter cyber attacks is a subset of its overarching defense strategy comprised of all instruments of national power, this paper focuses on states’ actions to deter cyber attack within the cyberspace domain. Effective cyber deterrence in cyberspace will employ a comprehensive scheme of offensive and defensive cyber capabilities supported by a robust international legal framework. Offensive capabilities are the primary tools used to impose or raise costs in deterrence. Offensive cyber capabilities and operations provide a state the means and ways for retaliation and enhance the perceived probability that aggressors will pay severely for their actions. A more robust capability translates to a more credible imposition of costs. Until recently, U.S. efforts to develop offensive cyber capabilities have lagged efforts on the defensive side. The daily onslaught of attacks on U.S. networks, coupled with the likelihood that potential U.S. adversaries will be less dependent on electronic networks than the U.S., has prioritized intelligence gathering and defending U.S. capabilities over disrupting enemy capabilities.85 However, the United States has recently gained momentum in the development of offensive cyber capabilities. In 2006, the U.S. published the National Military Strategy for Cyber Operations with the expressed intent to achieve “military strategic superiority in cyberspace.”86 One of its main goals is to ensure “adversaries are deterred from establishing or employing offensive capabilities against U.S. interests in cyberspace.”87 Unlike the air, land, and sea domains, the U.S. currently lacks dominance in cyberspace.88 In fact, without a significant effort, the U.S. will lose its current technological advantages and “risks parity with adversaries” in cyberspace.89 To this end, the U.S. has taken measures in support of offensive cyber operations. While each military service has some form of cyber footprint, the U.S. Air Force has incorporated operating in cyberspace as part of its core mission on par with flying and space operations. For instance, the commander of the Air Force’s provisional cyber operations command envisions initial offensive cyber operations as subduing or killing data packets that threaten U.S. systems, with the potential to expand in the future to missions normally executed by conventional forces in the past.90 The U.S. continues to modernize its cyber forces, create new hacker units, and conduct cyberwar exercises,91 with the intent to “penetrate and disrupt foreign computer systems.”92 However, the U.S. is not alone in pursuing cyber attack. Over 120 countries already have or are developing computer attack capabilities, reinforcing the need for a strong defense.93

#### -China – Offensive doctrine critical to prevent US-China war and solve IP theft

Blumenthal 2/28/13 (Dan, the director of Asian Studies at the American Enterprise Institute, where he focuses on East Asian security issues and Sino-American relations. Mr. Blumenthal has both served in and advised the U.S. government on China issues for over a decade. From 2001 to 2004, he served as senior director for China, Taiwan, and Mongolia at the Department of Defense. Additionally, he served as a commissioner on the congressionally-mandated U.S.-China Economic and Security Review Commission since 2006-2012, and held the position of vice chairman in 2007. He has also served on the Academic Advisory Board of the congressional U.S.-China Working Group. J.D., Duke Law School M.A., School of Advanced International Studies, Johns Hopkins University B.A., Washington University Chinese language studies, Capital Normal University “How to Win a Cyberwar with China” <http://www.foreignpolicy.com/articles/2013/02/28/how_to_win_a_cyberwar_with_china>)

The Internet is now a battlefield. China is not only militarizing cyberspace -- it is also deploying its cyberwarriors against the United States and other countries to conduct corporate espionage, hack think tanks, and engage in retaliatory harassment of news organizations. These attacks are another dimension of the ongoing strategic competition between the United States and China -- a competition playing out in the waters of the East and South China seas, in Iran and Syria, across the Taiwan Strait, and in outer space. With a number of recent high-profile attacks in cyberspace traced to the Chinese government, the cybercompetition seems particularly pressing. It is time for Washington to develop a clear, concerted strategy to deter cyberwar, theft of intellectual property, espionage, and digital harassment. Simply put, the United States must make China pay for conducting these activities, in addition to defending cybernetworks and critical infrastructure such as power stations and cell towers. The U.S. government needs to go on the offensive and enact a set of diplomatic, security, and legal measures designed to impose serious costs on China for its flagrant violations of the law and to deter a conflict in the cybersphere. Fashioning an adequate response to this challenge requires understanding that China places clear value on the cyber military capability. During the wars of the last two decades, China was terrified by the U.S. military's joint, highly networked capabilities. The People's Liberation Army (PLA) began paying attention to the role of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) assets in the conduct of war. But the PLA also concluded that the seeds of weakness were planted within this new way of war that allowed the United States to find, fix, and kill targets quickly and precisely -- an overdependence on information networks. Consider what might happen in a broader U.S.-China conflict. The PLA could conduct major efforts to disable critical U.S. military information systems (it already demonstrates these capabilities for purposes of deterrence). Even more ominously, PLA cyberwarriors could turn their attention to strategic attacks on critical infrastructure in America. This may be a highly risky option, but the PLA may view cyber-escalation as justified if, for example, the United States struck military targets on Chinese soil. China is, of course, using attacks in cyberspace to achieve other strategic goals as well, from stealing trade secrets to advance its wish for a more innovative economy to harassing organizations and individuals who criticize its officials or policies. Barack Obama's administration has begun to fight back. On Feb. 20, the White House announced enhanced efforts to fight the theft of American trade secrets through several initiatives: building a program of cooperative diplomacy with like-minded nations to press leaders of "countries of concern," enhancing domestic investigation and prosecution of theft, promoting intelligence sharing, and improving current legislation that would enable these initiatives. These largely defensive measures are important but should be paired with more initiatives that start to play offense. Offensive measures may be gaining some steam. The U.S. Justice Department, in creating the National Security Cyber Specialists' Network (NSCS) last year, recognizes the need for such an approach. The NSCS -- consisting of almost 100 prosecutors from U.S. attorneys' offices working in partnership with cyber-experts from the Justice Department's National Security Division and the Criminal Division's Computer Crime and Intellectual Property Section -- is tasked with "exploring investigations and prosecutions as viable options for deterrence and disruption" of cyberattacks, including indictments of governments or individuals working on the government's behalf. It's a good first step, but Congress could also consider passing laws forbidding individuals and entities from doing business in the United States if there is clear evidence of involvement in cyberattacks. Congress could also create a cyberattack exception to the Foreign Sovereign Immunities Act, which currently precludes civil suits against a foreign government or entity acting on its behalf in the cyber-realm. There is precedent: In the case of terrorism, Congress enacted an exception to immunity for states and their agents that sponsor terrorism, allowing individuals to sue them. Enterprising companies and intelligence personnel are already able to trace attacks with an increasing degree of accuracy. For example, the U.S. security company Mandiant traced numerous incidents going back several years to the Shanghai-based Unit 61398 of the PLA, which was first identified publicly by the Project 2049 Institute, a Virginia-based think tank. Scholars Jeremy and Ariel Rabkin have identified another way to initiate nongovernmental legal action: rekindling the 19th-century legal practice of issuing "letters of marque" -- the act of commissioning privateers to attack enemy ships on behalf of the state -- to selectively and cautiously legitimize retaliation by private U.S. actors against hacking and cyber-espionage. This would allow the U.S. government to effectively employ its own cybermilitia. Creating new laws or using current ones would force the Chinese government and the entities that support its cyberstrategy to consider the reputational and financial costs of their actions. Of course, if the United States retaliates by committing similar acts of harassment and hacking, it risks Chinese legal action. But America has a key advantage in that its legal system is respected and trusted; China's is not. Diplomatic action should bolster these efforts. The Obama administration's suggestions for pressuring China and other countries are a good start, but U.S. diplomacy must be tougher. In presenting Chinese leaders with overwhelming evidence of cyber-misdeeds (but without giving away too many details), Washington should communicate how it could respond. To control escalation, the administration should explain what it views as proportionate reprisals to different kinds of attacks. (For instance, an attack on critical infrastructure that led to deaths would merit a different response than harassment of the New York Times.) As the administration's report suggests, the United States is not the only victim and should engage in cooperative diplomacy. The United States should set up a center for cyberdefense that would bring together the best minds from allied countries to develop countermeasures and conduct offensive activities. One such center could be Taiwan, as its understanding of Chinese language, culture, business networks, and political landscape make it invaluable in the fight against cyberattacks. Of course, centers could be placed elsewhere and still utilize Taiwan's knowledge, but even the threat of placing a cyberdefense center just across the strait would be very embarrassing for China's leaders, as Taiwan is viewed as a renegade province. The point is not to be gratuitously provocative, but rather to demonstrate that the United States options that China would not favor. The U.S. military's cyber-efforts presumably already include it own probes, penetrations, and demonstrations of capability. While the leaks claiming the U.S. government's involvement in the Stuxnet operation -- the computer worm that disabled centrifuges in the Iranian nuclear program -- may have damaged U.S. national security, at least China knows that Washington is quite capable of carrying out strategic cyberattacks. To enhance deterrence, the U.S. government needs to demonstrate these sorts of capabilities more regularly, perhaps through cyber-exercises modeled after military exercises. For example, the U.S. military could set up an allied public training exercise in which it conducted cyberattacks against a "Country X" to disable its military infrastructure such as radars, satellites, and computer-based command-and-control systems. To use the tools at America's disposal in the fight for cybersecurity will require a high degree of interagency coordination, a much-maligned process. But Washington has made all the levers of power work together previously. The successful use of unified legal, law enforcement, financial, intelligence, and military deterrence against the Kim regime of North Korea during a short period of George W. Bush's administration met the strategic goals of imposing serious costs on a dangerous government. China is not North Korea -- it is far more responsible and less totalitarian. But America must target those acting irresponsibly in cyberspace. By taking the offensive, the United States can start to impose, rather than simply incur, costs in this element of strategic competition with China. Sitting by idly, however, presents a much greater likelihood that China's dangerous cyberstrategy could spark a wider conflict.

### AT: Space War

#### China won’t attack—not practical and wouldn’t be effective

**Forden. Former UN weapons inspector and strategic weapons analyst, 2008** – PhD, MIT research associate, former UN weapons inspector and strategic weapons analyst at the Congressional Budget Office (1/10, Geoffrey, Wired, “How China Loses the Coming Space War (Pt. 1)”, http://www.wired.com/dangerroom/2008/01/inside-the-chin/#more, WEA)

For years, the American armed forces have worried about an attack on US satellites; this could be how it begins. The United States military has become increasingly dependent on space. It uses photo-reconnaissance satellites to observe potential adversaries, GPS satellites to guide munitions with pin-point accuracy, communications satellites to handle the flow of information into and out of a theater of operations, and early warning satellites to detect and track enemy missile launches to name just a few of the better known applications. Because of this increasing dependence, many analysts have worried that the US is most vulnerable to asymmetric attacks against its space assets; in their view US satellites are “sitting ducks” without any sort of defense and their destruction would cripple the US military. China’s test of a sophisticated anti-satellite (ASAT) weapon a year ago, Friday — 11 January 2007, when it shot down its own obsolete weather satellite — has only increased these concerns. But is this true? Could a country—even a powerful country like China that has demonstrated a very sophisticated, if nascent, ability to shoot down satellites at all altitudes—inflict anything close to a knock-out blow against the US in space? And if it was anything less than a knock-out, how seriously would it affect US war fighting capabilities? The answers to these questions should influence how the US responds to the threats China’s ASAT represents. There is at least one way to answer these questions: “war-gaming” a massive Chinese attack on US satellites, where China is only limited by the laws of physics and the known properties of their ASAT, and see how much damage could be done. Such an exercise also reveals what the US could do, and what it could not do, to minimize the consequences. The results of my calculations are reported here. They assume that China launches a massive attack and that everything works exactly as planned: every ASAT launches, the US does not respond until after the attacks are launched even though it will have overwhelming evidence ahead of time, and every ASAT hits its target. Thus, this is a worst case scenario for the United States. In the end, we’ll show, the US would still has sufficient space assets to fight a major conventional war with China, even after such an attack. America’s military capabilities would be reduced, for a few hours at a time. But they would not be crippled. Back in 2001, a commission lead by Donald Rumsfeld warned of a "space Pearl Harbor," a single strike that could cripple America’s satellite network. It turns out, there is no such thing.

#### China’s space program poses no threat – they are and will continue to be against weaponization

Xinhau 3/12 **(Reporter for China Daily, “China’s Space Programs Threaten No One”,** [**http://www.chinadaily.com.cn/china/2012-03/01/content\_14734999.htm**](http://www.chinadaily.com.cn/china/2012-03/01/content_14734999.htm)**)**

BEIJING - A leading Chinese space engineer on Thursday defended the rapid development of China's space industry, saying such programs pose no threat to any other country. "It's inappropriate to say that China's space industry will threaten other countries," said Qi Faren, the former chief designer of the Shenzhou spaceships series, in an exclusive interview with Xinhua ahead of the annual session of the National Committee of the Chinese People's Political Consultative Conference (CPPCC), the country's top political advisory body, to open Saturday. "A rapidly developing space industry does not mean China has renounced its peaceful commitment," **said Qi, who is a member of the CPPCC National Committee.** "All China is doing is to pursue a peaceful development of the space industry as planned." "Objectively speaking, China and the United States are now in a competition situation in developing space industry," Qi said when asked to comment on the two countries' space programs. The engineer said, in rapidly developing its own space industry, China has learned lessons from countries such as the United States and Russia. "We've avoided mistakes they made and did not detour," Qi said. In a white paper on China's space activities in 2011, **China vowed to maintain a principle of peaceful development in its space missions and the use of outer space for peaceful purposes. China opposes the weaponization of, or an arms race in, outer space, according to the paper.**

### Flex/Offense Key

### Link – Cyber

#### Legal wrangling only creates uncertainty and hampers operation development.

**Baker, former Department of Homeland Security first assistant, 2012**

(Stewart, “What Is the Role of Lawyers in Cyberwarfare?”, 5-1, <http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/?utm_source=rss&utm_medium=topics&utm_campaign=cybersecurity>, ldg)

Lawyers don’t win wars. But can they lose a war? We’re likely to find out, and soon. Lawyers across the government have raised so many showstopping legal questions about cyberwar that they’ve left our military unable to fight, or even plan for, a war in cyberspace. No one seriously denies that cyberwar is coming. Russia may have pioneered cyberattacks in its conflicts with Georgia and Estonia, but cyberweapons went mainstream when the developers of Stuxnet sabotaged Iran’s Natanz enrichment plant, proving that computer network attacks can be more effective than 500-pound bombs. In war, weapons that work get used again. Unfortunately, it turns out that cyberweapons may work best against civilians. The necessities of modern life—pipelines, power grids, refineries, sewer and water lines—all run on the same industrial control systems that Stuxnet subverted so successfully. These systems may be even easier to sabotage than the notoriously porous computer networks that support our financial and telecommunications infrastructure. No one has good defenses against such attacks. The hackers will get through. Even very sophisticated network defenders—RSA, HBGary, even the Department of Defense’s classified systems—have failed to keep attackers out. Once they’re in, attackers have stolen the networks’ most precious secrets. But they could just as easily bring the network down, possibly causing severe physical damage, as in the case of Stuxnet. So as things now stand, a serious cyberattack could leave civilians without power, without gasoline, without banks or telecommunications or water—perhaps for weeks or months. If the crisis drags on, deaths will multiply: first in hospitals and nursing homes, then in cities and on the road as civil order breaks down. It will be a nightmare. And especially for the United States, which has trusted more of its infrastructure to digital systems than most other countries. We’ve been in this spot before. As Brig. Gen. Billy Mitchell predicted, airpower allowed a devastating and unprecedented strike on our ships in Pearl Harbor. We responded with an outpouring of new technologies, new weapons and new strategies. Today the threat of new cyberweapons is just as real, but we have responded with an outpouring—not of technology or strategy but of law review articles, legal opinions and legal restrictions. Military lawyers are tying themselves in knots trying to articulate when a cyberattack can be classed as an armed attack that permits the use of force in response. State Department and National Security Council lawyers are implementing an international cyberwar strategy that relies on international law “norms” to restrict cyberwar. CIA lawyers are invoking the strict laws that govern covert action to prevent the Pentagon from launching cyberattacks. Justice Department lawyers are telling our military that it violates the law of war to do what every cybercriminal has learned to do—cover their tracks by routing attacks through computers located in other countries. And the Air Force recently surrendered to its own lawyers, allowing them to order that all cyberweapons be reviewed for “legality under [the law of armed conflict], domestic law and international law” before cyberwar capabilities are even acquired. (And that’s just the lawyers’ first bite at the apple; the directive requires yet another legal review before the weapons are used.) The result is predictable, and depressing. Top Defense Department officials recently adopted a cyberwar strategy that simply omitted any plan for conducting offensive operations. Apparently, they’re still waiting for all these lawyers to agree on what kind of offensive operations the military is allowed to mount. I have no doubt that the lawyers think they’re doing the right thing. Cyberwar will be terrible. If the law of war can stave off the worst civilian harms, they’d argue, surely we should embrace it. There’s just one problem: That’s exactly what we tried when airpower transformed war. And we failed. In the first half of the 20th century, the airplane did for war fighters what information technology has done in the last quarter-century. Like cyberattacks, airpower was first used to gather intelligence and not to fight. Perhaps for this reason, there was never a taboo about using either airpower or cyberweapons. By the time officials realized just how ugly these weapons could be, the cat was already out of the bag. By the 1930s, though, everyone saw that aerial bombing would reduce cities to rubble in the next war. We have trouble today imagining how unprecedented and terrible airpower must have seemed at that time. Just a few years earlier, the hellish slaughter where armies met in the trenches of World War I had destroyed the Victorian world; now airpower promised to bring that hellish slaughter to the home front. Former Prime Minister Stanley Baldwin summed up Britain’s strategic position in 1932 with a candor no American leader has dared to match in talking about cyberwar: “I think it is well also for the man in the street to realize that there is no power on earth that can protect him from being bombed, whatever people may tell him. The bomber will always get through. ... The only defense is in offense, which means that you have got to kill more women and children more quickly than the enemy if you want to save yourselves.” The British may have been realists about air war, but Americans still hoped to head off the nightmare. The American tool of choice was international law. (Some things never change.) When war broke out on Sept. 1, 1939, President Franklin D. Roosevelt sent a cable to all the combatants seeking express limits on the use of airpower and expressing his view that “ruthless bombing from the air of civilians in unfortified centers of population … has sickened the hearts of every civilized man and woman, and has profoundly shocked the conscience of humanity. ... I am therefore addressing this urgent appeal to every government which may be engaged in hostilities publicly to affirm its determination that its armed forces shall in no event, and under no circumstances, undertake the bombardment from the air of civilian populations or of unfortified cities.” Roosevelt had a pretty good legal case. The Hague Conventions on the Law of War, adopted just two years after the Wright Brothers’ first flight, declared that in bombardments “all necessary steps should be taken to spare as far as possible edifices devoted to religion, art, science, and charity, hospitals, and places where the sick and wounded are collected, provided they are not used at the same time for military purposes.” The League of Nations had recently declared that, in air war, “the intentional bombing of civilian populations is illegal.” But FDR didn’t rely just on law. He asked for a public pledge that would bind all sides. Remarkably, he got it. The horror of aerial bombardment ran so deep in that era that England, France, Germany and Poland all agreed—before nightfall on the same day. What’s more, they tried to honor their pledges. In a June 1940 order for Luftwaffe operations against Britain, Hermann Göring “stressed that every effort should be made to avoid unnecessary loss of life amongst the civilian population.” It began to look like a great victory for the international law of war. All sides had stared into the pit of horrors that civilian bombing would open up. And all had stepped back. It was exactly what the lawyers and diplomats now dealing with cyberwar hope to achieve. But as we know, that’s not how this story ends. On the night of Aug. 24, a Luftwaffe air group made a fateful navigational error. Aiming for oil terminals along the Thames, they miscalculated, instead dropping their bombs in the civilian heart of the city of London. It was a mistake. But that’s not how Churchill saw it. He insisted on immediate retaliation. The next night, British bombers hit targets in Berlin for the first time. The military effect was negligible, but the political impact was profound. Göring had promised that the Luftwaffe would never allow a successful attack on Berlin. The Nazi regime was humiliated, the German people enraged. Ten days later, Hitler told a wildly cheering crowd that he had ordered the bombing of London: “Since they attack our cities, we will extirpate theirs.” The Blitz was on. In the end, London survived. But the extirpation of enemy cities became a permanent part of both sides’ strategy. No longer an illegal horror to be avoided at all costs, the destruction of enemy cities became deliberate policy. Later in the war, British strategists would launch aerial attacks with the avowed aim of causing “the destruction of German cities, the killing of German workers, … the disruption of civilized life throughout Germany … the creation of a refugee problem on an unprecedented scale, and the breakdown of morale both at home and at the battle fronts.” The Hague Conventions, the League of Nations resolution, even the explicit pledges given to President Roosevelt—all these “norms” for the use of airpower had been swept away by the logic of the technology and the predictable psychology of war. So, why do today’s lawyers think that their limits on cyberwar will fare better than FDR’s limits on air war? It beats me. If anything, they have a much harder task. Roosevelt could count on a shared European horror at the aerial destruction of cities. He used that to extract an explicit and reciprocal understanding from both sides as the war was beginning. We have no such understanding, indeed no such shared horror. Quite the contrary, for some of our potential adversaries, cyberweapons are uniquely asymmetric—a horror for us, another day in the field for them. It doesn’t take a high-tech infrastructure to maintain an army that is ready in a pinch to live on grass. What’s more, cheating is easy and strategically profitable. American compliance will be enforced by all those lawyers. Our adversaries can ignore the rules and say—hell, they are saying—“We’re not carrying out cyberattacks. We’re victims too. Maybe you’re the attacker. Or maybe it’s Anonymous. Where’s your proof?” Even if all sides were genuinely committed to limiting cyberwar, as all sides were in 1939, we’ve seen that the logic of airpower eventually drove all sides to the horror they had originally recoiled from. Each side felt that it had observed the limits longer than the other. Each had lawyerly justifications for what it did, and neither understood or gave credence to the other’s justifications. In that climate, all it took was a single error to break the legal limits irreparably. And error was inevitable. Bombs dropped by desperate pilots under fire go astray. But so do cyberweapons. Stuxnet infected thousands of networks as it searched blindly for Natanz. The infections lasted far longer than intended. Should we expect fewer errors from code drafted in the heat of battle and flung at hazard toward the enemy? Of course not. But the lesson for the lawyers and the diplomats is stark: Their effort to impose limits on cyberwar is almost certainly doomed. No one can welcome this conclusion, at least not in the United States. We have advantages in traditional war that we lack in cyberwar. We are not used to the idea that launching even small wars on distant continents may cause death and suffering here at home. That is what drives the lawyers. They hope to maintain the old world. But they’re driving down a dead end. If we want to defend against the horrors of cyberwar, we need first to face them with the candor of a Stanley Baldwin. Then we need to charge our military strategists, not our lawyers, with constructing a cyberwar strategy for the world we live in, not the world we’d like to live in. That strategy needs both an offense and a defense. The offense must be powerful enough to deter every adversary with something to lose in cyberspace, and so it must include a way to identify our attacker with certainty. The defense too must be realistic, making successful cyberattacks more difficult and less effective because we have built resilience and redundancy into our infrastructure. Once we have a strategy for winning a cyberwar, we can ask the lawyers for their thoughts. We can’t do it the other way ’round.

### Link – WPR

#### WPR wrecks military operations-Congress is too slow, creates artificial restraints AND leads to enemy manipulation

**Turner, Principal Deputy Assistant Secretary of State for Legislative and Intergovernmental Affairs, 1984**

(Robert, “The War Powers Resolution: Unconstitutional, Unnecessary, and Unhelpful”, 6-1, <http://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1433&context=llr>, ldg)

Even were there no constitutional difficulties with the War Powers Resolution, a review of its implementation during the past nine years demonstrates that it has been as ineffective in practice as it is unwise in theory. Congress lacks the expertise to deal hurriedly with complex foreign policy emergencies, and most members are too busy with other duties to remain up-to-date on even a prolonged crisis. During times of crisis, decisiveness is often essential. Failure will almost be guaranteed if there are 536 potential secretaries of state trying to make decisions by consensus. Congress is not structured to make rapid decisions, and the more controversial and important the decision, the more likely it is that at least some members will want to prolong the debate to avoid having to take a position that might later prove to have been politically unwise. The experience during the Indochina evacuations provides a good example. President Ford asked the Congress on April 10, 1975, to quickly consider and clarify his authority to carry out a humanitarian evacuation. He requested action within nine days and was promised expeditious consideration, but nearly three weeks later Congress was still debating as communist troops overran the last areas of Indochina. As the last congressional staff member evacuated from Saigon during the final days of April 1975, I am particularly grateful that President Ford decided to proceed with the evacuation on his own authority. Another individual might have found it more politically expedient to continue beseeching Congress for authorization legislation, and then to point the finger of blame at the Democrat-controlled Congress for failing to act to prevent hundreds of Americans from being seized by Vietnamese communist forces. There is no guarantee that in a future crisis another United States President would act with the same degree of courage displayed in 1975 by President Ford. After the failure of President Carter's attempted Iranian resbue there were calls for his impeachment for violating the War Powers Resolution, and during hearings in the House Committee on International Relations following the Korean tree trimming incident in 1976 it was asserted that if in the future a President did not comply with the provisions of the resolution: "We will have to get a new President."9 The requirement that the President must obtain congressional authorization or terminate hostilities after a sixty-day period may also prove to be mischievous in practice. It might encourage a President to escalate a conflict unnecessarily-with accompanying increased loss of life and property on all sides-in order to try to achieve a quick victory. President Nixon's fear that Congress would soon enact legislation terminating United States involvement in Indochina, for example, was a factor in the decision to bomb the Hanoi area in December 1972: "Faced with a perceived deadline in Congress and continued intransigence in both Saigon and Hanoi, the President's instincts were for a massive post-election escalation of the conflict to force North Vietnam to an agreement."' 10 While in the view of many (including myself) this was also a sound decision on military grounds, irrespective of possible congressional action, the fact remains that ideally such decisions should not be influenced by extrinsic domestic political considerations. Alternatively, such a requirement might encourage an enemy to be more recalcitrant in the hope that by holding out a few weeks longer Congress would undercut the President's ability to prosecute the action. In such a situation, the President might conclude that it was necessary to make major concessions and sacrifice substantial United States interests in order to negotiate a quick truce and avoid the risk of having his commander-in-chief powers withdrawn and losing everything to the enemy. Something of an analogy can be found in the experience of French Socialist Premier Pierre Mend~s-France, who announced in June 1954 that he would resign if he did not succeed in arranging a cease-fire in Indochina by July 20 of that year. The communist delegations at the Geneva Conference realized that the longer they stalled the more concessions he would be willing to make to preserve his job. The serious negotiations took place during the final hours of July 20, and shortly before midnight the wall clock was unplugged to permit the French delegation to make a few more concessions within the artificial time deadline.II Another, more recent, example of the harmful effects of an artificial negotiating deadline can be found in a review of the background to the Panama Canal treaties. Because President Carter re- fused to submit the nomination of his negotiator (Sol Linowitz) to the Senate for confirmation, by law the appointment could not extend beyond a period of six months.12 The treaties, which were filled with serious ambiguities, were agreed upon six months to the day after the appointment was made. 3 The War Powers Resolution might contribute to unnecessarily high United States casualties in other ways as well. Writing in the October 1980 issue of the Marine Corps Gazette, Major A. J. Ponnwitz argued: "An enemy who knows a withdrawal is imminent has most of the information necessary to prevent the success of the military mission, or at least, to inflict severe casualties on the retreating forces."' 4 In addition, the Resolution encourages the President to commit United States military personnel into potentially dangerous situations-where involvement in hostilities is possible but not so clearly indicated by the circumstances as to invoke section 4(a)(1) of the War Powers Resolution- either unarmed (as in the Zaire airlift and the 1976 evacuation of Lebanon), or inadequately armed for effective self-defense (as may be the case in El Salvador'-), so as to avoid the provisions of section 4(a)(2). Rules prohibiting United States military personnel from entering certain areas or accompanying host-nation troops on "offensive" operations may help to reduce the likelihood of their direct involvement in hostilities; but requiring that, if attacked, they defend themselves with rocks or other inadequate weapons makes little sense and should be unacceptable as a matter of national policy. Even the formal reporting requirement, which was unchallenged by President Nixon or any of his successors-is not without risks. Senate Armed Services Committee Chairman John Tower has observed: Although the act does not specify whether the report to Congress must be unclassified, there remains the possibility that a confidential report would become public knowledge. In many cases the more urgent the requirement that a decision remain confidential, the greater the pressures for disclosure. Thus, by notifying Congress of the size, disposition and objectives of U.S. forces dispatched in a crisis, we run the risk that the report may get into the public domain. If this information becomes available to the enemy, he then knows exactly what he can expect from American forces and thus what risks he runs in countering American actions. This removes any element of surprise the U.S. forces might have enjoyed and eliminates any uncertainties the adversary might have as to American plans.'6