# Round 1 (AFF) vs West Georgia MZ

## 1AC

### 1AC—Plan

#### The United States federal government should require the President of the United States to consult with congress prior to the use of offensive cyber operations.

### 1AC—LOAC

#### Advantage 1 is the Law of Armed Conflict

#### Status quo OCO policy violates it – 3 reasons

#### First – Lack of congressional checks make Jus in Bellum impossible to establish

Dycus 10(Professor Stephen Dycus is an internationally recognized authority on national security law and environmental law. The courses he has taught at Vermont Law School include Public International Law, National Security Law, Estates, Property, and Water Law. He was founding chair of the National Security Law Section of the Association of American Law Schools. He is the lead author of "National Security Law" (the field's leading casebook) and "Counterterrorism Law", and he was founding co-editor in chief of the Journal of National Security Law & Policy. (Stephen, "Congress' Role in Cyber Warfare," National Security Journal, Volume 4, Issue 155, 2010 http://jnslp.com/wp-content/uploads/2010/08/11\_Dycus.pdf)

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 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.

#### Second – Clandestine nature of Obama’s policies

Loon 12 (Collin Engelbert Peter van Loon Royal Netherlands Army , “Offensive Cyber What are the possibilities of the use of offensive cyber as an offensive capability within the existing international legal framework?”, https://cyberwar.nl/d/MSc-thesis\_Offensive-Cyber\_Collin-van-Loon\_June-2012.pdf)

Offensive cyber operations are not covered by an international agreed legal framework. The consequence is that it is hard to distinguish between the different kind of cyber attacks, their purpose, their origin and under which existing law the attacks fall. LoAC only covers the jus in bello kind of attacks. When the LoAC were first drafted, only nation-states had the legal ability to wage war and to execute operations. Since cyber attack weapons are easy available for everyone, non-state actors and even individuals are capable getting involved in cyber incidents, cyber operations or cyber conflict. Thus, the lines between state, non-state, and individual attackers are unclear in a legal regime that discriminates between LoAC on the one hand and national criminal laws and law enforcement on the other (Dam et al., 2009, s. 22).

The lack of a decent legal framework also endangers a decent distinction between cyber attacks conducted in the cause of warfare, or cyber attacks as a simple hacker’s activity in the cause of law enforcement. The means and methods used by a nation-state to conduct cyber attacks can vary greatly and can also be classified in a number of ways. However, although this variety, these attacks can be similar if not identical to those used by hackers in the context of cyber crimes. Moreover, cyber attacks can occur both in times of peace and war (Palojärvi, 2009). The blurring in these different types of cyber attack makes the need for a general international accepted cyber legal framework even more necessary

#### Third – Definition of ambiguous attack posture

Adkisson et al. 12 Carnagie Mellon University (CDR James Adkisson, Mr. Tokunbo Davies, LT Brian Evans, Mr. Rick Lanchantin, Ms. Patty Walters, “Law of Armed Conflict: Implications for Navy Cyber Strategy Masters of Information Technology Strategy Practicum – 2012”, http://www.cmu.edu/mits/files/random/mits-cohort1-practicumfinal-lawarmedconflict-implications-aug-2012.pdf)

The uncertain definition of the ‘use of force’ is increasingly problematic when analyzing cyber attacks. Although cyber attacks do not utilize lethal effects, cyber attacks present a clear danger due to their ability to inflict both intended and unintended damage to critical infrastructure, financial markets, banks and the overall welfare of a nation. Such attacks could lead to the paralysis of a nation due to an inability to support its population, resulting in significant suffering and/or death of non-combatants. As a result, there is a strong argument that the threat of cyber attack is itself a violation of the U.N. Charter and LOAC. In contrast, there is also an argument that cyber should be used in preference to conventional weapons in order to comply with LOAC. This argument is based on the assertion that cyber attacks are more humanitarian because they have less potential to create collateral damage than conventional weapons. These are the issues that commanders and military planners must balance when

conducting operations in cyberspace.

In a February 2012 testimony to Congress, the Director of National Intelligence (DNI), Director of the Central Intelligence Agency (CIA), and Director of the Federal Bureau of Investigations (FBI) stated that cyber security ranks among the top national security concerns. They also indicated that current policy requires revision to address how the use of force in cyberspace conforms to national and international law, including LOAC.

The previous section reviewed the applicability of LOAC to cyber operations. This section builds on that understanding and reviews national policy that impact DoD operations in cyberspace.

B. Defining Policy

The DoD does not expressly define the term ‘policy’. A standard dictionary definition implies that policy provides guidance for solving problems without explicitly defining the solution.2 Accordingly, policy for cyber operations should offer a means to arrive at solutions for achieving the established operational objectives within cyberspace.

While DoD policy is designed to guide the decision-making process, the policies must conform to LOAC. Accordingly, the DoD has stated that current policy and legal regimes that govern actions in traditional warfare domains also apply to cyberspace operations.3 The U.S. Navy has in turn stated that Navy cyberspace operations will conform to DoD and national efforts.4 Despite these efforts, cyber policy across the U.S. Government remains severely underdeveloped. Many of the policy documents from the Executive Branch, DoD, individual military services, and Department of Homeland Security (DHS) were written more than ten years ago. Despite their age, these documents continue to influence decisions about cyber operations that result in “legally acceptable plans and orders that support national security objectives.” 5

While there is significant debate regarding cyber operations amongst the international community, the U.S. Government (USG) is moving forward to try and establish domestic strategies and policies. These policies can generally be examined from the perspectives of offense and defense. Due to lack of international consensus regarding the characteristics of an ‘armed attack’ in cyberspace, there is minimal policy regarding Offensive Cyber Operations (OCO) or Exploitation Cyber Operations (ECO). Policy concerning OCO continues to suffer from a lack of authorities concerning its use. ECO is conducted under U.S. Title 50 authorities that govern the operations of the Intelligence Community (IC).

#### They uniquely antagonize china and make mutual drawdown impossible

Sanger 9/1/13 (David, A 1982 graduate of Harvard College, Sanger has been writing for the Times for 30 years covering foreign policy, globalization, nuclear proliferation, and the presidency., He has been a member of two teams that won the Pulitzer Prize, and has been awarded numerous honors for national security and foreign policy coverage. “Documents detail U.S. cyber-espionage plans”, http://www.thehindu.com/news/international/documents-detail-us-cyberespionage-plans/article5083012.ece)

231 operations planned for 2011 – both small scale and large scale

Newly disclosed budget documents for America’s intelligence agencies show how aggressively the United States is conducting offensive cyber-operations against other states, even while the Obama administration protests attacks on U.S. computer networks by China, Iran and Russia.

The documents, obtained by The Washington Post from Edward J. Snowden, the former National Security Agency contractor, indicate 231 such operations in 2011, a year after the first evidence emerged of a U.S.-and Israeli-led cyberattack against Iran’s nuclear-enrichment centre.

It suggests that President Barack Obama was not deterred by the disclosure of the Iranian operation, which became evident because of a technological error, and is pressing ahead on using cyber-weapons against a variety of targets.

The Post had said it has withheld most of the 178 pages of documents at the request of government officials because of the sensitivities of the spying operations they describe.

Unlike drone attacks, which the administration has begun to acknowledge publicly and provide legal justifications for, cyberattacks are still regarded as part of a secret arsenal.

The attacks described in the budget documents appear to be on a far smaller scale than the series of attacks on Iran, which were part of a classified operation called “Olympic Games”.

The Post talked of a parallel effort, code-named GENIE, which it described as an effort by U.S. intelligence officials working for the NSA and the military’s Cyber Command to insert surreptitious controls into foreign computer networks. That computer code, a form of malware, allows U.S. officials to hijack the computers or route some of their data to servers that enable U.S. espionage.

It is unclear how many, if any, of those 231 operations are merely for espionage or data manipulation, and how many may be intended to destroy or disable infrastructure. Mr. Obama, in an executive order signed last year, has reserved the right to decide when the United States should conduct such operations. It is not clear how many of the 231 he approved.

Diplomatically, the disclosure of the latest Snowden documents poses a new challenge to Mr. Obama. He has pressed China to cease its own cyber-operations in the United States, many of which are aimed at the theft of intellectual property — including corporate secrets and plans for the F-35 Joint Strike Fighter, the country’s most expensive new weapons system.

The Chinese have responded that America also conducts extensive cyber-operations — including against China — and will doubtless use the most recent disclosures to press that case. So far, Mr. Obama’s effort to get the Chinese engaged in a deeper dialogue on cyberissues has yielded discussions, but little fruit.

#### Impacts –

#### A. China doesn’t have a model for LOAC in cyberspace – that escalates any skirmish

VornDick 6/30/13 (Wilson VornDick is a lieutenant commander in the U.S. Navy, where he is assigned to the Pentagon. Previously, he worked at the Chinese Maritime Studies Institute at the U.S. Naval War College. , “The Real U.S.-Chinese Cyber Problem”, <http://nationalinterest.org/commentary/the-real-us-chinese-cyber-problem-8796?page=2>)

Recent waves of cyber attacks emanated from China despite their vehement denial that they possess “cyber warfare troops.” Meanwhile, the United States, sensing its own security vulnerabilities, stood up its newest military Combatant Command, USCYBERCOM, in 2009. This enabled a coordinated defensive and offensive capability in an increasingly digitized world as evident in the U.S.-led Stuxnet and Flame malware operations against Iran in 2010. As a result, both of the prominent digital players in the international community can bring forth debilitating and warlike capabilities. Washington and Beijing even agreed to a spontaneous two-day summit in June to stem the increasingly dangerous game of digital cat and mouse. Unfortunately, the norms guiding the use of cyber forces have yet to be established.

One crucial point lost amid the backdrop of the new digitized battlefield is the lack of Chinese leadership experience both military and political in utilizing key principles of the laws of armed conflict (LOAC). LOAC principles are becoming the foundation and framework for the emerging rules on cyber warfare. Some in China are slowly recognizing this shift. Given the increasingly interconnected, globalized and legally ill-defined nature of cyber technologies, one false move by either the United States or China could steer them into a cyber collision with horrendous conventional consequences.

General Escalation of Force, Proportionality and Rules of Engagement Concepts in War

Jus in bello (just conduct in war) is the set of general laws and principles that govern the way war is fought. It also incorporates the principles of escalation of force (EOF), proportionality, and the rules of engagement (ROE). This was created to promote humane standards in warfare despite the overreaching, destructive nature inherent in war. With the end of WWII, these principles now have been codified with international and customary laws into the Geneva Convention. These embody the modern concept of the law of armed conflict.

U.S. Experience with the LOAC

The U.S. Department of Defense leadership has a vast experience with these principles as they apply to the doctrine of jus in bello. They presently use various rules, approaches, and protocols to abide by the LOAC. Prior to the start of hostilities, military planners will delineate three key principles taken from the LOAC noted earlier: escalation of force (EOF), proportionality, and rules of engagement (ROE). This is to avoid confusion and miscalculation before, during and after hostilities.

The Army’s Escalation of Force Handbook defines EOF as “sequential actions that begin with nonlethal force measures (visual signals to include flags, spotlights, lasers and pyrotechnics) and may graduate to lethal measures (direct action) to include warning, disabling or deadly shots to defeat a threat and protect the force.” Meanwhile, proportionality is military action that is not excessive in relation to the concrete and direct military advantage anticipated. The Army has a uniform Standard Rules of Engagement dictating engagement of force.

Since September 11, U.S. policy makers and military strategists have been provided a tremendous opportunity to finesse those LOAC concepts based on first-hand experience gained in Iraq, Afghanistan, Libya, Guantanamo Bay, on the Korean peninsula and off the Horn of Africa. Each of these situations has spanned a wide range of possibilities in utilizing both cyber and conventional forces. U.S. commanders were required to tailor and adjust these forces to the realities on the ground. This resulted in the integral inclusion of cyber and information warfare training across all military services and senior leaderships. The significance of these experiences has pushed U.S. policy makers to shape frameworks to govern the nebulous and proliferating world of cyber warfare.

The Tallinn Manual and Emerging Cyber Norms The law-of-armed-conflict principles already established are guiding the discussion and implementation of the emerging rules, doctrines and frameworks that may one day govern the future of cyber warfare. Realizing the need for a LOAC as it applied to the cyber domain, various states, NGOs and individuals have begun to provide their own precepts. Last year, tremendous work and energy by scholars, policymakers and digital leaders from around the world was poured into the Tallinn Manual on the International Law Applicable to Cyber Warfare. This collaborative document provides a starting point to cover the use of force in cyber warfare by state and nonstate actors. However, this document is merely a guiding post and lacks enforcement mechanisms. There is still no globally recognized norm. China has not provided transparency or information regarding their cyber intentions. Despite this, China’s previous views on conventional use of force may offer some clues on future cyber warfare strategies. The Chinese have not had practical, hands-on experience with escalation of force, proportionality or rules of engagement. The Chinese military has not conducted significant operations since its shellacking in the 1979 border war with Vietnam. Their military has a dearth of expertise in applying these concepts in a real-time threat environment. This inexperience is compounded by the fact that the PRC and PLA leadership define the concepts differently from the United States and others. Because LOAC principles gained from battlefield experience are finding their way into the norms of the cyber domain, the Chinese authorities may be ill-prepared to deal with the pandora’s box of cyber warfare. This mismatch of LOAC experience potentially could cause a miscalculation in any cyber encounter. Lonnie Henley conducted a study on Chinese escalation management in 2006. He found that Chinese military strategists and theorists segregate EOF and proportionality under their concepts of containment of war (遏制战争 ezhi zhanzheng) and war control (战争控制 zhanzheng kongzhi). Further, he pointed out that Chinese perceptions on war containment and control can be described as the “deliberate actions of war leaders to limit or restrain the outbreak, development, scale, intensity, and aftermath of war” as well as controlling its vertical and horizontal escalation. The Chinese concept of war control is unique in that it seeks a united and focused national effort to maintain the political and military initiative at all cost. The concept of seizing the initiative is not new, and it was even an integral part of Mao Zedong’s war strategy. A recent article in Xinhua by Li Duaguang, a professor at the National Defense University, expounded further on war control by stating that “by preparing for war, one can curb war.” This pull towards seizing the initiative could make Chinese leadership lean too far forward on the side of miscalculation and error. Regrettably, there also has been a dearth of current Chinese discussion on these two principles, so it is difficult to assess Chinese intent in the cyber realm. Yet, Chinese media reports have filled some of the void with regards to ROE(交战规则 jiaozhan guize). Despite a lack of battle-tested ROE experience, China has linked ROE with cyber warfare and basically has asserted that the United States lacks a legal basis for any unilateral cyber rules of engagement of its own. This is because the Chinese fear that unilateral action by the United States, such as establishing a cyber ROE, would set the stage for future U.S. preemptive action in anticipation of a cyber attack that could target China. Cyber in China’s Recent Defense White Paper These pronouncements come at the heels of China’s recently published defense white paper that publicly promulgates its military’s intentions. “Cyber” is mentioned only twice in the entire paper. China did recognize however, that “changes in the form of war from mechanization to informationization are accelerating,” while “major powers are vigorously developing new and more sophisticated military technologies so as to ensure that they can maintain strategic superiorities in international competition in such areas as . . . cyber space.” China also unequivocally stated in the document that it would “counterattack” if attacked.Troubling Prospects for U.S.-Chinese Cyber Operations This is particularly troubling for Chinese and American authorities because it is unclear whether or not they could manage their cyber responses in a measured and proportional way if an unofficial or official outbreak of digital force, intentional or not, were to occur. The severity of this issue is intensified by the lack of official Chinese pronouncements or transparency on their cyber operations. Clandestine cyber units, such as the PLA-sponsored Unit 61398 in Shanghai, operate with destructive global reach, adding a layer of uncertainty to an illicit cyber response. After a thorough analysis of the defense white paper, it is clear that the Chinese leadership is reticent to articulate their intentions in cyber warfare. For defense purposes, this is troublesome for Washington. There is a variety of political and military reasons for this course of action. Perhaps this Chinese reluctance in setting the guidelines of response stems from the lack of pressure from the United States and other nations. In any case, it is doubtful that the leadership would state a different course of action than its professed desire to conduct only defensive and nonaggressive operations. Despite this, there is a distinct possibility that if push came to shove, Chinese leadership may be ill-equipped to bring its digital forces to bear or reign in these forces in a responsive, proportional manner once they are released. This is precisely because the Chinese lack LOAC doctrine, training and first-hand experience. The Chinese leadership could make a disastrous miscalculation if it were to mismatch capability or response with the objective or threat at hand, thus risking more confusion and escalation. The recent summit in June may be step toward some sort of digital détente or cyberwar norm. The two states should work to form one sooner rather than later, lest they push each other over the digital edge.

#### China perceives US policy – lack of clarity makes Chinese invasion of Taiwan inevitable

Austin & Gady 12 (Greg Austin – phD in International Relations, Vice President for the Worldwide Security Initiative, including a leadership role in the institute's work on cybersecurity, is now a Professorial Fellow. Greg has a 30-year career in international affairs, including senior posts in academia and government., Franz Stefan Gady -- M.A. in Strategic Studies/International Economics from the School of Advanced International Studies, Johns Hopkins University., “CYBER DETENTE BETWEEN THE U.S. AND CHINA: Shaping the Agenda, http://www.ewi.info/system/files/detente.pdf)

In sum, China is probably engaged in cyber warfare planning for operations against the United States on a very serious level, and possibly more so than for naval or air combat operations against it. At least in relative terms, China’s cyber warfare capability is probably far more powerful but less lethal than its conventional military capabilities. That suits China enormously in both respects. China’s military strategy is highly defensive, but to defend against U.S. operations against China over Taiwan, China has to rely mainly on unconventional operations, and these include cyber operations as well as psy-ops of the classic kind, including through fifth- column policies.

The scale and intensity of United States offensive cyber operations aimed at China on a day-to–day basis may be lower than vice versa, but without access to classified material it would be hard to characterize the difference between the potential disruptive effects of American and Chinese capabilities. This lack of clarity, in an environment of exceedingly low transparency peculiar to cyberspace compared with land, air, sea and space operations, aggravates insecurities on both sides.

The two most urgent tasks for bilateral discussions would therefore appear to be clarifying the relationship between offensive and defensive cyber operations at the strategic and operational levels of war (the thresholds of response), and clarifying the link between these thresholds and traditional notions of strategic nuclear and conventional force deterrence.

#### Cyber attacks are a prelude to all out kinetic war

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

Cyberspace matters. We know this because governments and militaries around the world are scrambling to control the digital space even as they slash defense spending in other areas, rapidly building up cyber forces with which to defend their own virtual territories and attack those of their rivals.

But we do not yet know how much cyberspace matters, at least in security terms. Is it merely warfare’s new periphery, the theatre for a 21st century Cold War that will be waged unseen, and with practically no real-world consequences? Or is it emerging as the most important battle-space of the information age, the critical domain in which future wars will be won and lost?

For the time being, some states appear quite content to err on the side of boldness when it comes to cyber. This brazen approach to cyber operations – repeated attacks followed by often flimsy denials – almost suggests a view of cyberspace as a parallel universe in which actions do not carry real-world consequences. This would be a risky assumption. The victims of cyber attacks are becoming increasingly sensitive about what they perceive as acts of aggression, and are growing more inclined to retaliate, either legally, virtually, or perhaps even kinetically.

The United States, in particular, appears to have run out of patience with the stream of cyber attacks targeting it from China – Google and The New York Times being just two of the most high-profile victims – and which President Obama has now insisted are at least partly state-sponsored.

Although setting up a cybersecurity working group with China, Washington has also signaled it intends to escalate. U.S. Cyber Command and NSA chief General Keith Alexander signaled this shift of policy gears earlier this month when he told Congress that of 40 new CYBERCOM teams currently being assembled, 13 would be focused on offensive operations. Gen Alexander also gave new insight into CYBERCOM’s operational structure. The command will consist of three groups, he said: one to protect critical infrastructure; a second to support the military’s regional commands; and a third to conduct national offensive operations.

As cyber competition intensifies between the U.S. and China in particular, the international community approaches a crossroads. States might begin to rein in their cyber operations before things get further out of hand, adopt a rules-based system governing cyberspace, and start respecting one another’s virtual sovereignty much as they do one another’s physical sovereignty. Or, if attacks and counter-attacks are left unchecked, cyberspace may become the venue for a new Cold War for the Internet generation. Much as the old Cold War was characterized by indirect conflict involving proxy forces in third-party states, its 21st century reboot might become a story of virtual conflict prosecuted by shadowy actors in the digital realm. And as this undeclared conflict poisons bilateral relations over time, the risk of it spilling over into kinetic hostilities will only grow.

#### Nuclear war

O’Hanlon 07 (Michael, adjunct professor at John Hopkins and lecturer at Princeton and Bush, “A war like no other: the truth about China's challenge to America”, p. 99-100)

War between China and Taiwan is a distinct possibility. Such a war could easily drag in the United States, pitting the worlds only superpower against its main rising power and thus leading to the first serious conflict in history between nuclear weapons states.

It seems inconceivable, in this day and age, that the United States and China could really wind up in war. Their mutual interests in cooperating are so strong, their economies are so intertwined, the dangers of war are so enormous, and the number of other problems for them to worry about is so great that it would seem the height of foolishness for the two huge powers ever to come to blows.

There is much truth to this, Indeed, as we have argued in chap- ter three, most of the reasons whv China and the United States could theoretically fight do not in the end hold water. But the Taiwan problem is different. Not only does it involve a third actor over which neither Beijing nor Washington has control. Not only does it involve a territory that China sees as an integral part of its own nation and that the United States sees as a long-standing, stalwart, and democratic friend. In addition, the way that a China-Taiwan crisis could begin and escalate would hold the inherent potential for escalation to direct superpower war. This chapter explains whv. The- next chapters get into the dynamics of what could happen if that war began, how it might be terminated before getting extremely serious—but also why it could be tough to control.

The overall message is sobering. Even if the chances of war between the United States and China are less than 25 percent— indeed, even if they are less than 10 percent—they are far from zero. And given the enormous consequences of any such war, in terms ol immediate danger as well as lasting effects on the interna- tional system, every effort must be made to prevent it. World War I did not seem very likely to most world leaders in 1912 or 1913 either; certainly a horrible four-year struggle, followed two decades later by an even worse world war, was not predicted. We must avoid dire mistakes of that era and take seriously the possibility of a war that, even if unlikely already, must be rendered more unlikely still.

In short, the reasons whv that war could occur, are as follows:

First. China really does consider Taiwan its own, and even as it has arguably adopted a more subtle and sophisticated approach to the Taiwan challenge in recent years, it has explicitly kept the threat of force on the table.1

Second, Chinas military capabilities are growing last even as Taiwan's begin to stagnate, meaning that Beijing could sense an opportunity—if it can keep the United States out of the light

Third, Taiwan could push the sovereignty' issue in a way that China interprets as the pursuit of full independence. While China would probably be wrong in reaching any such con- clusion, perceptions could matter more than reality in such a situation.

 Fourth, while Washington's commitment to Taiwan is long- standing, it is also somewhat ambiguous, so leaders in China might convince themselves that the United States real!)' would sit out a China-Taiwan war.

#### B. Human survival hangs in the balance. An international order governed by the “law of the jungle” terminally non-uniques all of their impacts

**Weston 91** – Chair of the International and Comparative Law Program @ The University of Iowa [Weston, Burns H., “Logic and Utility of a Lawful United States Foreign Policy,” Transnational Law & Contemporary Problems, Vol. 1, Issue 1 (Spring 1991), pp. 1-14

George Will and others like him are right, of course, that the rhetoric of international law can be used, like a double-edged sword, against the United States as well as by it. They are wrong, however, to bemoan this fact-unless, of course, they bemoan the nature of law itself, a process of legitimized politics that, in Benjamin Cardozo's unforgettable words, seeks the "reconciliation of the irreconcilable," the "merger of antitheses," the "synthesis of opposites," in "one unending paradox."12 Though the "real world" often is not a very nice place and though for this reason it sometimes may seem that the responsible pursuit of national interests requires realpolitik policies and practices, a foreign policy that corresponds with what most people have in mind when they think of "The Rule of Law" (i.e., notions of equality, mutuality, reciprocity, cooperation, and third-party procedure) is more likely to find itself on the winning side of most political and strategic battles than one that does not. Legality, like honesty, is generally the best policy. It enhances power used under its aegis.

In the pages following, I suggest six concrete reasons why the United States-indeed, all nations- should take international law seriously, even when others do not. Viewed in isolation, they may not persuade the hardened realpolitiker. Viewed together, however, they should.

1. Respect for International Law Assists Human Survival

To begin with, it is not healthy for people (and for other living things) to resist principles of international law in a world that is bristling with more than 50,000 nuclear weapons and other greatly expanded technologies of war and mass destruction. If the history of the last half century has taught us anything, it is that our present militarily competitive international order cannot be expected to prevent large-scale war for very long (e.g.,Kuwait). There is, therefore, little hope for genuine security, national or global, without a strengthening of the legal foundations, bilateral and multilateral, for the nonmilitary-preferably democratic-resolution of international disputes. These would include, but not be limited to, the improvement of U.N. peacekeeping and peacemaking opportunities and capabilities, and the improvement of both national and international opportunities and capabilities for legal challenges to coercive foreign policies. 13 Even if other countries do not always follow suit, surely our country and our children's future will be better served if we strive hard to build as peaceful and just a world society as we can, and while we still have the chance. 14 The Soviet Union, home to more than 25,000 nuclear weapons and many newly-awakened nationalisms, faces a world history that demonstrates little support for the proposition that collapsing empires fade quietly. And in our increasingly "high-tech" world, with military research and development fast at work on atomic guns, particle-beam cannons, and other space age deviltries that divert attention from the perils of nuclear proliferation, many regimes in Western Asia and elsewhere have been acquiring nuclear and other weapons of mass destruction-and the means to deliver them, with frightening ease and speed, to almost anywhere on earth.

In sum, it is respect (or lack of respect) for international law that, in the end, will determine the fate of the Earth. As the late Bill Bishop counseled pithily over two decades ago, "under present conditions all [States] need international law in order to continue to exist together on this planet."15 Rededication to the world rule of law and cooperation in this Age of Nuclear Anxiety is not a matter of choice. It is, quite simply, a matter of survival.

2. Respect for International Law Enhances International Stability

Living as we do in the twilight years of the global Middle Ages, characterized by more than 160 separate fiefdoms, each with a monopoly control over the military instrument and each only barely accountable in any formal sense either to each other or to the larger arena in which each operates, it is easy to be seduced by the popular claim that ours is an anarchical world. Such an outlook does not, however, comport with reality. Every hour of every day, ships ply the sea, planes pierce the clouds, and artificial satellites probe outer space. Every hour of every day, communications are transmitted, goods and services traded, and people andthings transported from one country to another. Every hour of every day, transactions are negotiated, resources exploited, and institutions established across national and equivalent frontiers. And in all these respects, the many processes of authoritative and controlling decision that help to regulate such endeavors-what we call international law-are observed rather well on the whole.

On the other hand, when States bend, twist, or otherwise show disrespect for this ordering force to suit their special interests, international law, because it is an essentially voluntarist process of decision that is seriously lacking in centralized command and enforcement structures, quickly loses its otherwise stabilizing influence. The kidnapping of sixty-two Americans at the U.S. Embassy in Teheran in 1979, for example, demonstrates well the fundamental instability that can flow from a failure or refusal to abide by international law. Without, in this instance, a commitment to the basic rules of diplomatic protection, diplomacy ceased to exist and respectable discourse became impossible. Without a commitment to the world rule of law there could be no assurance of inter-governmental stability.

Of course, States-especially the major powers-are perfectly capable of unilaterally resisting the doctrines, principles, and rules of international law without necessarily feeling directly the destabilizing impact that their noncompliance ultimately has on the wider structure of international law and order itself. The probability of being formally punished for violating international law is usually so slim that foreign policy strategists commonly give little or no weight to the cost of decision-making marked by dubious legality.

However, the increasingly interdependent and interpenetrating character of today's world is of such magnitude and complexity that no nation, least of all the United States, can sensibly afford to insist upon its own independence of action without simultaneously threatening its own ultimate good and the ultimate good of others, and potentially in very fundamental ways. Though not understood by most Americans, it is in fact the United States "which stands to lose the most in a state of world anarchy." 16 Because the United States and its citizens have such wide-ranging and far-flung international interests, we urgently need a stable, predictable environment of international legal rules and procedures that can help to secure those interests on a cooperative basis worldwide. It is not in the first instance our freedom of action that should be our concern when we refuse to commit to the world rule of law, but rather, the stability of our world public order itself.

3. Respect for International Law Advances Our Geopolitical Interests

Allowing principles of international law and multilateral cooperation to inform our foreign policy also serves our geopolitical interests, especially our long-term geopolitical interests. For example, in contrast to our recent hegemonic warmongering in Grenada, Nicaragua, and Panama, a record of faithful adherence to the principle of nonintervention and to the right to self-determination would have helped, politically at least, to neutralize the Israelis in southern Lebanon and the Occupied Territories, the Soviets in the Baltics, and the Iraqis in Kuwait. As the late L.F.E. Goldie observed a number of years ago: "Obedience to law... is not only a categorical value but also a prudential one." 1'7 My colleague and former Prime Minister of New Zealand Sir Geoffrey W. R. Palmer, referring to the need for strict compliance with arms control and disarmament treaties, once put it this way: "[I]s it possible on the one hand to look to international law to provide essential security guarantees, while on the other hand, in other areas, the right is quietly being reserved to undermine, ignore and indeed walk away from the rule of law in international affairs?"18

In recent years, however, during the Reagan presidency especially, the United States has come before the world community more to bury international law than to praise it. Selectively displaying its military strength to the general disregard of international law, it has chosen, at least when the risks have been low, to advance several broadly defined but narrowly determined national interests:

(1) demonstrating American will to act with decisiveness and reinforcing deterrence against the Soviet Union in the Third World; (2) displaying the ability of U.S. armed forces to defend American and allied interests; (3) inducing countries that challenge the U.S. to cease and desist; and (4) enhancing in the broadest terms an international perception of the U.S. as the great world power. 19

But to favor such special interests over the common interest of a world rule of law is to shoot ourselves in the geopolitical foot-perhaps not always, but more often than is commonly realized. It gets us into quagmires from which it is hard to extricate ourselves and it subverts our ability to ensure in other settings that other governments, especially our adversaries, will fulfill their obligations under international law that are in our interest for them to fulfill.

The point is depressingly simple to illustrate. If we can unilaterally reinterpret and abrogate an arms control treaty with the Soviet Union,20 why cannot the Soviets do the same with us? If we can excuse the kidnapping and killing of innocent civilians by the Nicaraguan Contras because they were "freedom fighters,"21 what right do we have to condemn the Palestinians or Shiites for doing the same thing in Lebanon? If we can ignore a World Court decision relative to the human rights violations we encouraged in Nicaragua,2 how can we complain when Iran ignores a World Court decision relative to the taking of U.S. hostages in Teheran?2 If we can claim the right to seize fugitives from abroad,2 what logic compels our right to object when the Iranian Majlis (parliament) approves legislation authorizing Iranian officials to arrest Americans anywhere in the world for violations of Iranian law?25 If we can intercept a civilian aircraft over the Mediterranean on the grounds that it appears to threaten our national security interests, 26 what is to stop the Soviet Union from doing the same thing over the Pacific for the same reason?27 If we can condone a U.S. military raid upon an ambassadorial residence in Panama despite our obligations under the 1961 Vienna Convention on Diplomatic Relations, how can we complain when Iranian students seize a U.S. embassy protected by the 1961 Vienna Convention on Diplomatic Relations? 28 And so forth.

Such partisan uses of international law are illustrative of what, during the 1980s, has been referred to as the "Reagan Corollary" of international law-which is to claim a right "to pressure the international legal system into changing in a manner beneficial to United States interests."9 However, such uses do not, in the end, correspond to our long-term national interest of ensuring that other governments in other settings fulfill their obligations under international law. Were every nation to adopt this Reagan Corollary, a perverted interpretation of international doctrines, principles, and rules would become the standard practice and the international legal system would quickly disintegrate into a system of retributive justice extremely unsafe for the geopolitical interests of even the most powerful States.

Thus, if the United States wants to insist upon compliance with international law to protect American interests, it will be to its advantage to obey international law, even when its application proves inconvenient. If we want meaningful international law to be available when we find it useful, we must respect it even when we do not.

4. Respect for International Law Promotes Policy Efficacy

A failure to adhere to international law-in particular the prohibitions against the threat and use of nondefensive force and the admonitions to promote and safeguard human rights-tends also to be counterproductive, hence not very efficacious. While militarism and support of repressive regimes to the disregard of international law may sometimes yield tactical victories that are viscerally pleasing in the short-run, they rarely achieve strategically satisfying gains, to say nothing of justice, over the long-run. Consider, for example, the Reagan administration's decision, pursuant to what came to be known as the "Schultz Doctrine," to fight terrorism with American-sponsored counterterrorism, 30 the ultimate denouement of which was the sordid Iran-Contra affair. In keeping with this decision, the United States provided Israel with diplomatic, financial, and material support of Israel's illegal invasion of southern Lebanon in 1982,31 in violation of common Article 1 of the four Geneva Conventions on the laws of war of 194932 and involving the killing of more than 20,000 people (at a time when, ironically, Palestinian terrorist attacks against American persons and property had been in decline). Not surprisingly, the victims of the invasion and their sympathizers held Washington responsible, in conjunction with Israel, for the atrocities committed by the Israeli army and the Lebanese Phalange militia against Palestinian civilians in the Sabra and Shatilla refugee camps in southern Lebanon.33 American interests immediately began to experience a pronounced increase in terrorist attacks-via airplane hijackings, kidnappings, assassinations, bombings, and other paramilitary activitiesfrom Palestinian, Shiite, and other groups throughout the Middle East.

Consider also the refusal of the United States to accept the jurisdiction of the International Court of Justice in the case brought by Nicaragua in April 1985 in protest of Washington's illegal assistance to, and support of, the Contra guerrillas against Nicaragua's democratically elected Sandinista government.34 Instead of making its substantive case before the Court, the United States contended that what it considered to be an issue of Western Hemispheric security was not properly for the World Court to decide and that, in any event, there was no reason for the United States to submit to the Court's jurisdiction when, over the years, the Soviet Union had consistently refused to do so. 35 As one sensitive observer put it, "[this] argument was politically attractive domestically, but it eroded the stature of the World Court that American values had once tried to build up."36 More such examples could easily be recounted. It might be asked, for example, whether our aiding and abetting the assassination of Chile's Allende or our legally dubious support of the Shah of Iran really did serve our long-term national interest. And the same might be asked, as well, of the Iran-Contra affair and of our legally questionable assistance to Saddam Hussein during and after the Iran-Iraq war.

But the efficacy argument is perhaps best demonstrated by noting the large-scale political support that was extended to Washington, internationally as well as nationally, during at least the early months of the 1990-91 Persian Gulf crisis when the United States pressed hard for economic sanctions against Iraq that were, it can be said, not only timely and measured but in keeping with the collective security system authorized in San Francisco in 1945.37 Adherence to the principles and procedures of international law, President Bush discovered, was essential to gaining the world's support to force Iraq's hand. Lawful foreign policies are consensusbuilding policies-politically pragmatic or efficient policies-and they are useful even to a superpower.

To put it all another way, we abandoned lynching parties on the western frontier not only because they turned into orgies of wasteful bloodlust but also because they simply did not stop horse thieves. International law violations, like violations of law in general, have a dubious pragmatic record at best.

5. Respect for International Law Safeguards Domestic Society

Disregard of international law and institutions tends to be self destructive as well as destructive of international order. The consequences of our unilateral and disproportionate uses of force in Vietnam should be proof enough. Over a decade and a half later, as such movies as Platoon, Born on the Fourth of July, and Casualties of War alone bear witness, we are still licking the socioeconomic, political, and ethical wounds. Though not always immediately apparent or discernible, international law violations and "go-it- alone" policies that fail to show a decent respect for the rights and opinions of others invariably corrode our core essence, diminishing our national integrity and threatening even our individual liberties. As Professor Bilder has asked, can we legitimately expect to separate the standards that govern the way our government operates internationally from those that govern it internally? 8 If we tell our elected officials that it's okay to act illegally, corruptly, or brutally abroad, can we be completely sure that they will really listen when we tell them that they should not act that way at home? If we say to the Secretary of State, the CIA, or the National Security Council that it's okay to bend the law a little because we do not like another country's ideology, can we rightfully expect that the Attorney General or the FBI will not bend the law a little when it comes to those of our citizens who do not share the government's ideology in domestic affairs?

In other words, when we show contempt for international law and cooperation, we badly damage our sense of national self-respect and purpose and, in so doing, invite civil unrest. In addition to the widespread civil disobedience that characterized the era of the legally problematic Vietnam War, we may note the popular protests that, more recently, accompanied Washington's extraordinary build-up of offensive nuclear weapons, its policy of "constructive engagement" with apartheid South Africa, and its military adventurism in Central America.3 9 One of the wondrous things about our country-deep-rooted in our ideology even if not always borne out in practice-is our commitment to decent behavior and the rule of law. From our very beginnings, we have officially embraced the notion of a Higher Law based upon "principles of right and justice that prevail because of their own obvious merit:"40 liberty, equality, participation, and due process. And since at least the turn of the century, cognate international principles have been added: the self-determination of peoples, the sovereign equality of States, respect for international law and organization, and the peaceful settlement of international disputes. So, when our government resorts to foreign policy plots and maneuvers of a Machiavellian sort that sacrifice or otherwise diminish these principles, the spillover into the domestic arena is predictable. The government soon loses the support of the people.

Our Founding Fathers established that ours is a society of laws, not of men. To most of us, therefore, "standing tall" in the global community does not mean being the toughest kid on the block, pushing other countries around and breaking our promises as we once accused the Soviet Union of doing, but acting humanely and honorably. Intuitively we know that it is necessary for us to uphold the rule of law abroad in order to uphold it at home. Intuitively we know that "[t]he two are inextricably connected." 41 Intuitively we know that a double standard erodes our claim to moral leadership in the international community.42

6. Respect for International Law Ennobles Our National Rectitude

As evidenced by the U.N. General Assembly's declaration of the 1990s as the "Decade of International Law,"43 there is a growing realization that an effective system of international law is fundamental to the achievement of a world public order of human dignity. It is essential to peace and security, and it is indispensable for just solutions to the many complex and urgent problems that otherwise currently make up the human agenda.

International law provides, potentially, the most durable framework for undertaking cooperative action toward the abolition of war, the promotion of human rights, the ending of mass poverty, and the creation of a sustainable global environment. Its progressive evolution, in keeping with Article 28 of the Universal Declaration of Human Rights ("Everyone is entitled to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized"),4 is the key to all that is right and good.

To insist upon respect for international law and cooperation is, thus, the morally correct thing to do, and for this reason alone it is in our longterm best interest. Rather than throw our weight around as if at some shootout at the OK Corral, the United States should reaffirm its commitment to a law-oriented foreign policy and, from this posture, through carefully planned and diligently executed diplomatic strategy, regain a once assumed (even if not always demonstrated) moral stature among the family of nations-the "American difference," as President Reagan used to call it. Along the way, discovering that it would thus gain the upper hand in the global competition for hearts and minds, including the enthusiastic support of otherwise doubting allies, the United States would also discover that commitment to international law and cooperation is fundamentally a matter of self-interest. Our reputation as a law-abiding nation, one that genuinely honors the world rule of law in practice, is a vital asset, strongly affecting our ability to win friends and influence people. It is a reputation that cannot-must not-be squandered.

Most importantly, however, the United States has an especial obligation in this regard. Quite simply, the size of our economy, the sophistication of our technology, the ubiquity of our investments, and the power of our arsenals make us so globally consequential that the acts and omissions of our government transmit a powerful and usually lasting message. Like it or not, our words and our deeds count heavily in the normative, institutional, and procedural development of world affairs. 45 And this establishes for us, a professedly democratic and peace-loving country, an historically unique moral responsibility. Pg. 4-13 // AT: K

#### Eyes are on the US – our adherence to LOAC is modeled globally. OCO ambiguity is the biggest internal link

Bradbury 11 (Steven Assistant Attorney General for the Office of Legal Counsel, The Developing Legal Framework for Defensive and Offensive Cyber Operations, http://harvardnsj.org/wp-content/uploads/2011/02/Vol.-2\_Bradbury\_Final1.pdf)

Evolving customary law. This approach also accommodates the reality that how the U.S. chooses to use its armed forces will significantly influence the development of customary international law. As the label implies, customary law can evolve depending on the accepted conduct of major nations like the United States. The real-world practice of the United States in adapting the use of its military to the new challenges raised by computer warfare will (and should) help clarify the accepted customs of war in areas where the limits are not clearly established today. And if you just review the literature on cyber war, you quickly see that that’s where we are: precisely how the laws and customs of war should apply to offensive cyber operations is not yet crystallized in key respects. For example, there aren’t always bright lines to tell us when a cyber attack on computer systems constitutes an “armed attack” or a “use of force” that justifies a nation in launching a responsive military strike under Article 51 of the U.N. Charter. Some questions are easy: Hacking into a sensitive government computer system to steal information is an act of espionage, not an armed attack. It’s clearly not prohibited by the laws and customs of war. On the other hand, if the cyber intrusion inflicts significant physical destruction or loss of life by causing the failure of critical infrastructure, like a dam or water supply system, then it obviously would constitute an armed attack under the law of war and would justify a full military response if it could be attributed to a foreign power. Where committed as an offensive act of aggression, such an attack may violate international law. If significant enough, the effect of the attack will determine its treatment, not necessarily whether the attack is delivered through computer lines as opposed to conventional weapons systems. In these cases, the laws and customs of war provide a clear rule to apply. But there will be gray areas in the middle. Thus, it’s far less clear that a computer assault that’s limited to deleting or corrupting data or temporarily disabling or disrupting a computer network or some specific equipment associated with the network in a way that’s not life threatening or widely destructive should be considered a use of force justifying military retaliation, even if the network belongs to the military or another government agency. This was the case with the “distributed denial of service” attacks experienced by Estonia in 2007, which severely disrupted the country’s banking and communications systems. Suspecting that Russia was behind it, Estonia suggested that NATO declare that Estonia’s sovereignty had been attacked, which would have triggered the collective self-defense article of the NATO Treaty, but that suggestion was rebuffed on the ground that a cyber attack is not a clear military action.12 There’s an echo of that reasoning in Article 41 of the U.N. Charter, which says that a “complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communications” is not a “measure . . . involving armed force.” And what about Stuxnet? As I understand it from public reports, Stuxnet was a computer worm that found its way into the systems controlling Iran’s nuclear program and gave faulty commands causing the destruction of the centrifuges used for enriching uranium. Suppose President Ahmadinejad claimed that Israel was behind the Stuxnet worm and claimed that Stuxnet constituted an armed attack on Iran that justified a military response against Israel. I suspect the United States would disagree. At the same time, when it comes to a cyber attack directed against U.S. computer systems, I certainly want the President to have leeway in determining whether or not to treat the attack as a use of force that supports military retaliation. Making such judgments is a traditional power exercised by the President, and I think he retains that leeway. Similarly, I submit, it’s not clearly established that a cyber attack aimed at disrupting a server or Web site located in a neutral country or in a country outside a theater of open hostilities would be a violation of that country’s neutrality. The server might be a valid military target because it’s being used for the communications or command and control of the enemy fighters in the area of hostilities (after all, al Qaeda regularly uses the Internet in planning and ordering operations). The server might have no connection to the host country’s military, government, or critical infrastructure, and it might be readily targeted for a computer attack without inflicting widespread damage on unrelated systems used for civilian purposes. Such a focused cyber operation — with little physical impact beyond the destruction of data or the crippling of a server — is very different from the kind of physical violation of territory — such as a conventional troop incursion or a kinetic bombing raid — that we ordinarily think of as constituting an affront to neutrality.13 Although every server has a physical location, the Internet is not segmented along national borders, and the enemy may gain greater tactical advantage from a server hosted half way around the world than from one located right in the middle of hostilities. The targeting of a server in a third country may well raise significant diplomatic difficulties (and I wouldn’t minimize those), but I don’t think the law-of-war principle of neutrality categorically precludes the President from authorizing such an operation by an execute order to Cyber Command. Conclusion. So here’s my thesis: To my view, the lack of clarity on certain of these issues under international law means that with respect to those issues, the President is free to decide, as a policy matter, where and how the lines should be drawn on the limits of traditional military power in the sphere of cyberspace. For example, that means that within certain parameters, the President could decide when and to what extent military cyber operations may target computers located outside areas of hot fighting that the enemy is using for military advantage. And when a cyber attack is directed at us, the President can decide, as a matter of national policy, whether and when to treat it as an act of war. The corollary to all this is that in situations where the customs of war, in fact, are not crystallized, the lawyers at the State Department and the Justice Department shouldn’t make up new red lines — out of some aspirational sense of what they think international law ought to be — that end up putting dangerous limitations on the options available to the United States. Certainly, the advice of lawyers is always important, especially so where the legal lines are established or firmly suggested. No one would contend that the laws of war have no application to cyber operations or that cyberspace is a law-free zone. But it’s not the role of the lawyers to make up new lines that don’t yet exist in a way that preempts the development of policy.14 In the face of this lack of clarity on key questions, some advocate for the negotiation of a new international convention on cyberwarfare — perhaps a kind of arms control agreement for cyber weapons. I believe there is no foreseeable prospect that that will happen. Instead, the outlines of accepted norms and limitations in this area will develop through the practice of leading nations. And the policy decisions made by the United States in response to particular events will have great influence in shaping those international norms. I think that’s the way we should want it to work. One final admonition I’ll offer on the topic of offensive cyber operations: In cases where the President shapes new policy by choosing military action over covert action for a cyber operation, or vice versa, I would strongly urge that the President fully brief both sets of committees in Congress — the Intelligence Committees and the Armed Services Committees — and explain the basis for the choice. It’s inevitable the committees will find out anyway when a jurisdictional marker is crossed, and it will help smooth the development of consistent policies and standards for the committee members and staff to understand and appreciate the choices made on both sides of the question.

#### Prior consultation is key to check executive action

Healey and Wilson 13- Jason Healey is the director of the Cyber Statecraft Initiative at the Atlantic Council. A.J. Wilson is a visiting fellow at the

Atlantic Council (Jason, and A.J. "Cyber Conflict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain," Atlantic Council Cyber Statecraft Initiative, February 2013)

The administration’s interpretation of “hostilities” should go beyond the risk to American lives to have more logical consistency with cyberspace as a warfighting domain, like the land, sea, air, and space. Table 1 shows a more consistent vision of “logical” presence that may be useful in determining when US armed forces have been sufficiently “introduced into foreign territory [etc.]” or “into hostilities” to trigger the WPR’s reporting and/or withdrawal requirements. Involving the legislative branch in cyber conflict decisionmaking in this gradated manner—which, as the table shows, is easily transposed to the physical realm—need be neither unreasonable nor disproportionate. After all, transparency is required of those who govern open societies. Especially in this information age, we as citizens are right to expect it. The United States needs the capacity to carry out offensive operations in cyberspace, but the Executive branch must accept that the same checks and balances that apply to physical hostilities apply also to cyber conflict. Future cyber attacks may have the ability to destroy or degrade an adversary’s critical infrastructure, cripple its economy, and seriously compromise its ability to defend itself. They may cause physical injury or even death. Their strategic consequences—not to mention their fiscal and economic costs—may be just as significant as a physical attack. This is, indeed, why the Pentagon has rightly decided to treat cyberspace as the fifth domain. But it must, by the same token, accept that logical forms of presence matter in cyberspace in the same way that physical forms matter in the kinetic space, and therefore it must apply the War Powers Resolution accordingly. The Founding Fathers could not have imagined a world in which weapons made of information travel around the globe at the speed of light; but they did know how to distribute power to encourage restraint in its application. Even in cyberspace, there is a voice for both branches.

#### Congressional restrictions on OCOs send a global signal of cyber leadership that solves reckless use of OCOs

Bastby 12 (Judy, Chairwoman of the American Bar Association’s Privacy and Computer Crime Committee, CEO of Global Cyber Risk, “U.S. Administration's Reckless Cyber Policy Puts Nation at Risk” June 4, 2012, <http://www.forbes.com/sites/jodywestby/2012/06/04/u-s-administrations-reckless-cyber-policy-puts-nation-at-risk/2/>)

Perhaps more important than being out of the cyber coordination loop, is the how the U.S.’s attitude is being perceived by others in the international community. If the U.S. were a member of IMPACT and taking an active role in the investigation, it would be upholding its role as a global cybersecurity power. Instead, the U.S. appears as the shirking nation state quietly standing on the sidelines while being accused of engaging in cyberwarfare tactics. “People look to the U.S., Russia, and China for leadership and when the U.S. is absent, they will turn to the other two,” observes Dr. Amin.

The U.S. Administration’s failure to develop a strong foreign policy with respect to cybersecurity reveals a gross lack of attention at the highest levels of the U.S. Government to one of the country’s most vulnerable areas — the IT systems that underpin the functioning of our society and economy. This failure begins at basic strategy levels and extends to reckless disregard for the consequences of the risky covert Stuxnet operation and failure to secure classified information about the program. For example, in May 2011, government delegations from around the world gathered in Geneva for the World Summit on the Information Society (WSIS), one of the most important communications and technology conferences globally. Noticeably, the U.S. did not have a delegation present. Yet, it was during the WSIS event that the U.S. Administration chose to release its International Strategy for Cyberspace – from Washington, D.C. rather than Geneva. WSIS participants were dumbstruck. For the few private sector Americans who were present, including myself, it was embarrassing.

If in fact the Administration did authorize targeting Iranian nuclear systems with Stuxnet and/or Flame, it was a dangerous and reckless decision, especially since the U.S. Government has no idea how many computers in America may be infected with malware capable of being activated by Iran or one of its allies in retaliation. Such “backdoor” malware is capable of having enormous consequences to life and property. A similar CIA covert operation successfully destroyed a Soviet pipeline. In 1982, President Reagan approved a plan to transfer software used to run pipeline pumps, turbines, and valves to the Soviet Union that had embedded features designed to cause pump speeds and valve settings to malfunction. The plot was revealed in a 2004 Washington Post article by David Hoffman in advance of its discussion in former Air Force Secretary Thomas C. Reed’s book, At the Abyss: An Insider’s History of the Cold War. Reed recalled to Hoffman that, “The result was the most monumental non-nuclear explosion and fire ever seen from space.” Unlike Stuxnet, however, the program remained classified for 22 years until the CIA authorized Reed to discuss it in his book. Sanger’s information came from loose-lipped persons involved with the Stuxnet operation.

Before pulling a trigger (or launching malware) a nation should assess its strengths and resources and its correlation of vulnerabilities, which, in 2012, includes understanding what an adversary can do when firing back using cyber capabilities. In addition, before launching covert operations, such as Stuxnet, a nation also should ensure that the secrecy of the intelligence operations can be maintained.

Conversations with Hill staffers indicate that Congress believes the State Department’s 2011 appointment of Coordinator for Cyber Issues has sufficiently addressed concerns about the lack of U.S. involvement in international cybersecurity matters. Clearly, this is narrow, wishful thinking. Congress needs to stop focusing on what it believes it should force businesses to do about cybersecurity and instead focus on what it should demand that the U.S. Government do to protect our critical infrastructure businesses and avoid retaliatory cyber attacks. The kind of reckless cyber diplomacy and foreign policy now at work has put our nation at risk and demonstrates cyber irresponsiblity, not cyber leadership.

### 1AC—Deterrence

#### Advantage 2 is Deterrence

#### No OCO regulations now that creates a zone of twilight around inter branch relations

Healey and Wilson 13- Jason Healey is the director of the Cyber Statecraft Initiative at the Atlantic Council. A.J. Wilson is a visiting fellow at the

Atlantic Council (Jason, and A.J. "Cyber Conflict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain," Atlantic Council Cyber Statecraft Initiative, February 2013)

Even as the Obama administration is pushing Congress to pass strong legislation to avert a “Cyber Pearl Harbor,” it is insisting Congress should have little oversight in when the military engages in cyber conflicts. Cyber conflicts are too new and affect the American private sector too much to leave to the administration alone. Despite the administration’s actions to the contrary, if the Department of Defense’s own policies mean what they say, then Congress should have a voice in cyber operations. Since 1973, Congress has claimed the right to terminate military engagements under the War Powers Resolution (WPR). Beginning with Richard Nixon, whose veto had to be overridden to pass the WPR, presidents have typically regarded its provisions as unconstitutional limits on the authority of the commander-in-chief. The Obama administration has taken a slightly different tack, however, accepting “that Congress has powers to regulate and terminate uses of force, and that the [War Powers Resolution] plays an important role in promoting interbranch dialogue and deliberation on these critical matters,” but is seeking nonetheless to limit its application to certain types of conflicts.1 All presidents since Nixon’s successor, Gerald Ford, have submitted reports consistent with the resolution’s terms, although using varying thresholds.2 Under the WPR, the president is obliged to report to Congress within forty-eight hours of: [A]ny case in which United States Armed Forces are introduced—(1) into hostilities or situations where imminent involvement in hostilities is clearly indicated by the circumstances; (2) into the territory, airspace or waters of a foreign nation...; or (3) in numbers which substantially enlarge United States Armed Forces equipped for combat already located in a foreign nation. Situations falling within items (2) or (3) trigger only this reporting requirement. However, in the circumstances contemplated by item (1), the president must, in addition to satisfying the reporting obligation (and absent congressional approval of his actions), terminate the use of United States armed forces within sixty days. A further thirty days are available if the president certifies that only with such an extension can the forces committed be safely withdrawn. In other words, the president, as commander-in-chief, may commit forces for a maximum of ninety days after reporting without the approval of Congress. The text of the War Powers Resolution has four operative terms—none of which is defined—each critical to understanding the requirement set by Congress: “Armed Forces,” “Hostilities,” “Territory,” and “Introduction.” With regard to US operations over Libya, Obama administration officials sought to limit the scope of the WPR by adopting a narrow approach to the definition of “hostilities.” Initially, the president reported the Libyan engagement to Congress within the forty-eight hour window, describing his report as “part of my efforts to keep the Congress fully informed, consistent with the War Powers Resolution.”3 As noted, sixty days after the submission of his initial report the president is required either to pull the forces out or to certify that a thirty-day extension is necessary in order to withdraw them safely. When that deadline arrived with respect to Libya, Obama did neither of these things. Instead, on May 20, 2011, the sixtieth day, he sent another letter soliciting congressional support for the deployment. This second letter did not mention the WPR. 4 Subsequently, a few days before the ninety day outer limit of the WPR, the president provided to Congress a “supplemental consolidated report . . . consistent with the War Powers Resolution,” which reported on a number of ongoing deployments around the world, including the one in Libya.5 At the same time, the Pentagon and State Department sent congressional leaders a report with a legal analysis section justifying the non-application of the WPR, but also calling again for a congressional resolution supporting the war.6 Later, State Department legal adviser Harold Koh expanded upon this analysis in testimony before the Senate Foreign Relations Committee, arguing that operations in Libya should not be considered relevant “hostilities” because there was no chance of US casualties, limited risk of escalation, no “active exchanges of fire,” and only “modest” levels of violence. It is apparent that in defining “hostilities” the administration’s focus is on kinetic operations passing a certain threshold of intensity: while there is no detailed indication in Koh’s testimony of what weight is to be accorded to each of the factors he enumerates, the overriding emphasis is on physical risk to US personnel. As Koh himself said, “we in no way advocate a legal theory that is indifferent to the loss of non-American lives. But . . . the Congress that adopted the War Powers Resolution was principally concerned with the safety of US forces.” The consequences for opposing forces, and for the foreign relations of the United States, matter less—or not at all. Libyan units were decimated by NATO airstrikes; indeed, it was a US strike that initially hit Muammar Gaddafi’s convoy in October 2011, leading directly to his capture and extra-legal execution. Significantly, though, the strike came not from an F-16 but from a pilotless Predator drone flown from a base in Nevada.8 The significance of this for present purposes is that, apparently, even an operation targeting a foreign head of state does not count as “hostilities,” provided there is no involvement of US troops. This is not a new view; indeed, Koh relied heavily on a memorandum from his predecessor in the Ford administration, which defined “hostilities” as “a situation in which units of the US armed forces are actively engaged in exchanges of fire with opposing units of hostile forces.” This formulation would presumably exclude drone attacks and, most importantly for present purposes, remote cyber operations.7As remote war-fighting technology becomes ever more capable, reliable, and ubiquitous, the administration’s restrictive definition of “hostilities” could open up a huge area of unchecked executive power. For example, neither the current administration nor its immediate predecessor has reported under the WPR any of the hundreds of remote drone strikes carried out in Pakistan, Yemen, or Somalia over the past decade. Likewise, the Pentagon has made clear its position that other forms of remote warfare, cyber operations, are also not covered by the WPR.

#### The US has no cyber deterrence strategy. We’re shooting in the dark. Inter-branch consensus is critical

Kramer et. al 12 (Franklin D. Kramer is a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He served as the assistant secretary of defense for international security affairs from 1996 to 2001. Stuart H. Starr is also a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He concurrently serves as the president of the Barcroft Research Institute. Larry Wentz is a senior research fellow in the Center for Technology and National Security Policy at the National Defense University., “Cyberpower and National Security”, p. 318)

No cyber deterrence strategy can hope to be airtight to prevent all minor attacks. However, a strategy can increase the chances that major cyber attacks can be prevented; this could protect the United States and its allies not only from a single major attack but also from serial cyber aggressions and resulting damage. A worthwhile goal of a cyber deterrence strategy would be to transform medium-sized attacks into low-probability events and to provide practically 100 percent deterrence of major attacks.

A cyber deterrence strategy could contribute to other key defense activities and goals, including assurance of allies, dissuasion, and readiness to defeat adversaries in the event of actual combat. The goal of dissuading adversaries is crucially important. Thus far, the United States has not been noticeably forceful in stating its intentions to deter major cyber attacks and, if necessary, to respond to them with decisive force employing multiple instruments of power. Meanwhile, several countries and terrorist groups are reportedly developing cyber attack capabilities. Dissuasion of such activities is not an easy task: it requires investment in technical capabilities as well as building an internal consensus to employ these capabilities. If some of these actors can be dissuaded from entering into cyber competition with the United States and its allies, the dangers of actual cyber aggression will diminish.

How would a cyber deterrence strategy operate, and how can its potential effectiveness be judged? Deterrence depends on the capacity of the United States to project an image of resolve, willpower, and capability in sufficient strength to convince a potential adversary to refrain from activities that threaten U.S. and allied interests. As recent experience shows, deterrence can be especially difficult in the face of adversaries who are inclined to challenge the United States and otherwise take dangerous risks. In cases of failure, deterrence might well have been sound in theory but not carried out effectively enough to work. The aggressions of Saddam Hussein, Slobodan Milosevic, and al Qaeda might not have been carried out had these actors been convinced that the United States would respond with massive military force. These aggressions resulted because of a failure to communicate U.S. willpower and resolve, not because the attackers were wholly oblivious to any sense of restraint or self-preservation, nor because the logic of deterrence had lost its relevance.

#### Deterrence works by changing the incentive model of adversaries

Kramer et. al 12 (Franklin D. Kramer is a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He served as the assistant secretary of defense for international security affairs from 1996 to 2001. Stuart H. Starr is also a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He concurrently serves as the president of the Barcroft Research Institute. Larry Wentz is a senior research fellow in the Center for Technology and National Security Policy at the National Defense University., “Cyberpower and National Security”, p. 318)

Ends, Ways, and Means

The goal of a cyber deterrence strategy would be to influence an adversary’s decisionmaking calculus so decisively that it will not launch cyber attacks against the United States, its military forces, or its allies. Coordinated actions reduce the chances for attacker success, so that the dangers, costs, risks, and uncertainties of a cyber attack are perceived to outweigh any expected success, benefits, or rewards. In the case of an adversary who seeks to use threats of cyber attacks, or actual attacks, to coerce the United States into conduct that would serve its larger interests and goals, a cyber deterrence strategy will work if the adversary judges that this attempted coercion would not succeed and that the attack would provoke U.S. retaliation, resulting in a net strategic setback for the would-be attacker. For example, if Iran were to contemplate cyber attacks to try to coerce the United States into making political concessions in the Persian Gulf and Middle East, it might be deterred from this course if its decisionmakers were to judge that the cyber attack would not physically succeed in inflicting the desired damage; that even if the attack succeeded, the United States would not make the desired concessions; or that the United States would be likely to retaliate in ways that inflict unacceptable damage on Iran in return, in the cyber realm or elsewhere.

The same strategic calculus applies to Chinese use of cyber threats and attacks, as well as actions by other plausible adversaries in the cyber domain. Potential U.S. counteractions in such situations are encapsulated in the three principal ways of pursuing deterrence articulated in the JOC model: deterrence by denying benefits, deterrence by imposing costs, and deterrence by offering incentives for adversary restraint.

Deterrence by denying benefits entails credibly threatening to deprive the attacker of the benefits or gains being sought: convincing it that a cyber attack will not achieve its goals. Deterrence by imposing costs entails credibly threatening to impose costs, losses, and risks that are too painful to accept, thus convincing the adversary that punishment would outweigh any expected successes. Deterrence by encouraging restraint means convincing the adversary that not attacking will result in an acceptable, attractive outcome.

#### Cyber war causes extinction

Rothkopf 11 (David, Visiting Scholar at Carnegie, “Where Fukushima meets Stuxnet: The growing threat of cyber war”, 3/17/11, http://rothkopf.foreignpolicy.com/posts/2011/03/17/where\_fukushima\_meets\_stuxnet\_the\_growing\_threat\_of\_cyber\_war)

The Japanese nuclear crisis, though still unfolding, may, in a way, already be yesterday's news. For a peek at tomorrow's, review the testimony of General Keith Alexander, head of U.S. Cyber Command. Testifying before Congress this week and seeking support to pump up his agency budget, the general argued that all future conflicts would involve cyber warfare tactics and that the U.S. was ill-equipped to defend itself against them.

Alexander said, "We are finding that we do not have the capacity to do everything we need to accomplish. To put it bluntly, we are very thin, and a crisis would quickly stress our cyber forces. ... This is not a hypothetical danger."

The way to look at this story is to link in your mind the Stuxnet revelations about the reportedly U.S. and Israeli-led cyber attacks on the Iranian nuclear enrichment facility at Natanz and the calamities at the Fukushima power facilities over the past week. While seemingly unconnected, the stories together speak to the before and after of what cyber conflict may look like. Enemies will be able to target one another's critical infrastructure as was done by the U.S. and Israeli team (likely working with British and German assistance) targeting the Iranian program and burrowing into their operating systems, they will seek to produce malfunctions that bring economies to their knees, put societies in the dark, or undercut national defenses.

Those infrastructures might well be nuclear power systems and the results could be akin to what we are seeing in Japan. (Although one power company executive yesterday joked to me that many plants in the U.S. would be safe because the technology they use is so old that software hardly plays any role in it at all. This hints at a bit of a blessing and a curse in the fractured U.S. power system: it's decentralized which makes it hard to target overall but security is left to many power companies that lack the sophistication or resources to anticipate, prepare for or manage the growing threats.)

Importantly, not only does the apparent success of the Stuxnet worm demonstrate that such approaches are now in play but it may just be the tip of the iceberg. I remember over a decade ago speaking to one of the top U.S. cyber defenders who noted that even during the late 90s banks were losing millions and millions every year to cyber theft -- only they didn't want to report it because they felt it would spook customers. (Yes.) Recently, we have seen significant market glitches worldwide that could easily have been caused by interventions rather than just malfunctions. A couple years back I participated in a scenario at Davos in which just such a manipulation of market data was simulated and the conclusion was it wouldn't take much to undermine confidence in the markets and perhaps even force traders to move to paper trading or other venues until it was restored. It wouldn't even have to be a real cyber intrusion -- just the perception that one might have happened.

What makes the nuclear threat so unsettling to many is that it is invisible. It shares this with the cyber threat. But the cyber attacks have other dimensions that suggest that General Alexander is not just trying to beef up his agency's bank accounts with his description of how future warfare will always involve a cyber component. Not only are they invisible but it is hard to detect who has launched them, so hard, in fact, that one can imagine future tense international relationships in which opposing sides were constantly, quietly, engaging in an undeclared but damaging "non-war," something cooler than a Cold War because it is stripped of rhetoric and cloaked in deniability, but which might be much more damaging. While there is still ongoing debate about the exact definition of cyber warfare there is a growing consensus that the threats posed by both state-sponsored and non-state actors to power grids, telecom systems, water supplies, transport systems and computer networks are reaching critical levels. This is the deeply unsettling situation effectively framed by General Alexander in his testimony and rather than having been obscured by this week's news it should only have been amplified by it.

#### Cyber-attacks will destroy US space assets

**Donahue, 10** – USAF Major (Jack, “CATASTROPHE ON THE HORIZON: A SCENARIO-BASED FUTURE EFFECT OF ORBITAL SPACE DEBRIS,” https://www.afresearch.org/skins/rims/q\_mod\_be0e99f3-fc56-4ccb-8dfe-670c0822a153/q\_act\_downloadpaper/q\_obj\_af691818-359f-4999-be24-f88ca154bd94/display.aspx?rs=enginespage)

Another unpredictable driving force that needs to be considered is adversary exploitation of space vulnerabilities via the cyber domain. Through cyberspace, enemies (both state and non-state actors) will target industry, academia, government, as well as the military in the air, land, maritime, and space domains.86 One of the easiest ways to disrupt, deny, degrade, or destroy the utility of space assets is to attack or sabotage the associated ground segments through cyberspace.87 The ground segment includes telemetry, tracking, and commanding of space assets and space-launch functions. Ground stations are an extremely critical piece of a satellites continued operation. However, many satellite tracking and control stations are lightly guarded and many satellite communications, launch, data reception, and control facilities are described in numerous open-source materials making the ground segment extremely vulnerable to cyber-attack.88 An attack on a fixed ground facility can stop data transmission, render launch facilities unusable, and prevent control of satellites.89 Thus, rendering affected orbiting satellites inoperative from the communication disruption and creating a risk to other active satellites and a potential for additional orbital debris. A single incident or a small number of incidents could significantly impact space systems for years.90

#### Loss of space assets risks miscalculation --- unique escalation to nuclear war

**Tyson 07** (Rhianna Tyson, Program Officer of the Global Security Institute, “Advancing a Cooperative Security Regime in Outer Space,” Global Security Institute, May 2007, http://www.worldacademy.org/files/Advancing%20a%20Cooperative%20Security%20Regime%20in%20Outer%20Space.pdf)

Beyond the severe economic repercussions resulting from disrupted commercial satellite communications, hostile actions in space can result in grave security threats, especially in times of war. Militaries rely on satellites for monitoring of and communication with troops on the ground. If a military satellite was deceived, disrupted, denied, degraded or destroyed, commanders lose their communication capabilities, resulting in mounting tensions and an escalation of conflict. A worst-case scenario could involve inadvertent use of nuclear weapons; without satellite-enabled monitoring capability in a time of tension, or, if early warning systems give a false reading of an attack, governments may resort to using nuclear weapons.

#### Independently undermines the balance of deterrence and leads to global preemptive aggression

**Burke 06** – Lt Col, USAF, command space professional with operational experience in missile operations, space surveillance, space control, missile warning, and command and control (Alan, “SPACE THREAT WARNING: FOUNDATION FOR SPACE SUPERIORITY, AVOIDING A SPACE PEARL HARBOR,” https://www.afresearch.org/skins/RIMS/display.aspx?moduleid=be0e99f3-fc56-4ccb-8dfe-670c0822a153&mode=user&action=researchproject&objectid=07acf878-3a5f-4a2c-8259-4a34c0717e9b)

The erosion of the US ability to execute the space threat warning mission has serious implications for US national security to include: the loss of a key early warning indicator of an attack on the US homeland; the loss of space capabilities which would degrade US warfighting effectiveness; the preventable loss of critical high-value satellites, facilities or services; the increased possibility that adversaries could develop new weapons or covertly conduct probing attacks on US space systems; and the lack of a credible means to execute stated US policy in response to an attack against space assets. One of the most serious impacts of the failure to develop or execute a reliable space threat warning and attack verification system is the loss of a key early warning indicator of an attack on the US homeland or an attack that is part of a major regional action by a near-peer adversary such as an attack on Taiwan by the Chinese mainland. The Japanese attack on Pearl Harbor, whose goal was the destruction of the Pacific Fleet, was not done as an isolated act, but as part of the start of a larger campaign to establish a Japanese Pacific sphere of influence which included the forceful acquisition of US territories. At this time, the Pacific Fleet was viewed as a US center of gravity whose destruction would enable Japan to achieve regional domination and discourage future US intervention. Today, our space-based assets may represent the equivalent of the WWII Pacific Fleet. Further, other nations have stated they view the US reliance on space as a potential Achilles ’ heel and a center of gravity whose destruction or disruption is critical to future military success against the US.44 Although a major attack on the US is not likely, the loss of US space-based early warning capability and ground-based missile warning radars could undermine nuclear deterrence strategy resulting in a devastating miscalculation that the US was vulnerable to a nuclear first strike. The perception that US space capabilities are vulnerable to a surprise attack also [hurts] ~~weakens~~ conventional deterrence. In the case of a US-China conflict over Taiwan, the Chinese might seek to disrupt or destroy regional space capabilities as part of a delaying strategy to deny US forces access to the region until their military operations were well underway, making the Chinese takeover of Taiwan a fait accompli.45 A successful Pearl Harbor-type attack on US space assets would degrade US fighting effectiveness. Today, space represents the ultimate high ground and it is unlikely that a nation, whose military ambitions might provoke US involvement, will willingly cede that high ground. The level of battlespace awareness space-based platforms provide makes any attack using large massed forces difficult to accomplish. The ability to neutralize these platforms would improve the circumstances required to gain a strategic advantage over US and allied forces. As General Lord stated in his Congressional testimony: “A resourceful enemy will look at our centers of gravity and try to attack them. Our adversaries understand our global dependence on space capabilities, and we must be ready to handle any threat to our space infrastructure.”46 With the increased US reliance on space assets for communication, intelligence, surveillance, and reconnaissance (ISR); and command and control of our deployed forces; a successful space attack could significantly delay US response to regional aggression. During Operation IRAQI FREEDOM (OIF), over 60% of theater communications traveled via satellites.47 The Defense Satellite Communication System (DSCS) provided 90% of all protected communications and 70% of all military satellite communications into theater.48 These capabilities significantly enhanced command and control of US and allied forces. Further, the employment of the satellite-based Blue Force Tracker system resulted in an unprecedented level of situational awareness which decreased fratricide and facilitating search and rescue operations and reinforcement operations.49

#### The lack of settled framework makes the threat of retaliation and counterstrike impossible – the aff makes counterstrike effective

Kesan & Hayes 12 \* Professor, H. Ross & Helen Workman Research Scholar, and Director of the Program in Intellectual Property & Technology Law, University of Illinois College of Law. \*\* Research Fellow, University of Illinois College of Law [Jay P. Kesan\* and Carol M. Hayes\*\*, MITIGATIVE COUNTERSTRIKING: SELF-DEFENSE AND DETERRENCE IN CYBERSPACE, Spring, 2012, Harvard Journal of Law & Technology, 25 Harv. J. Law & Tec 415]

Ideas, computers, and intellectual property have become extremely important in the modern Information Age. The Internet has become so essential to modern life that several countries have declared Internet access to be a fundamental right. n4 But the importance of technology in the Information Age comes with a downside: the vulnerability of modern society and the global economy to minimally funded cyberat-tacks from remote corners of the world.

In the 1950s, American school children were taught to "duck and cover" in the event of an atomic bomb explosion. n5 A popular cautionary film from 1951 warns that a flash of light brighter than the sun accompanies such an explosion and that the flash could cause an injury [\*418] more painful than a terrible sunburn. n6 The film, however, asserts that a child who "ducks and covers" will be more protected from the aftermath of nuclear detonation than otherwise. n7 Fortunately, no American city has ever experienced a nuclear attack, so no child has ever learned the hard way that a newspaper or a coat affords little protection against the heat from the detonation of an atomic bomb. The nuclear capabilities on both sides of the Cold War served as a deterrent against nuclear strikes and helped avoid an all-out nuclear conflict. n8 "Duck and cover," however, had no deterrent effect.

The Cold War ended about two decades ago, but new threats have emerged. The conflicts have shifted, the battlefields have morphed, and technologies that were not even dreamed of in 1951 now form the foundations for our everyday lives. The Internet, a technology partially developed to facilitate communication in the event of a nuclear attack, n9 changed the world forever. It is quite possible that future wars will be fought primarily in cyberspace, with the lines between civilian and military becoming increasingly blurred. n10 Instead of "duck and cover," computer users must now "scan, firewall, and patch." n11 However, like "duck and cover," purely passive defenses have questionable utility in the face of zero-day vulnerabilities n12 and sophisticated cyberweapons like the Stuxnet worm. n13 Likewise, law enforcement [\*419] and judicial action against malicious cyber intrusions currently do not present enough of a practical threat to deter potential attackers. n14

The weaknesses of the current reliance on employing passive defense methods and seeking help from the authorities -- who are both technologically and legally ill-equipped to seek justice for victims -- present a difficult situation. Considering how modern society relies on the Internet and networked services, there is an urgent need for proactive policy to help insulate critical services from damage as well as mitigate harm from potential attacks. For a number of reasons explored below, we argue that, in some circumstances, permitting mitigative counterstrikes in response to cyberattacks would be more optimal. There is an urgent need for dialog on this topic as the development of technology has outpaced the law in this area. n15 While progress has been made in the form of executive orders addressing cybersecurity, n16 the proposed Cyber Intelligence Sharing and Protection Act ("CISPA"), n17 and cybersecurity provisions of the National Defense Authorization Act ("NDAA"), n18 these measures do not go far enough. New discussions and analyses are needed to ensure that responsive actions can be grounded in sound policy.

Because of the inadequacy in current means to address cyber threats, this Article examines other possible methods to deter cyberattacks, specifically the use of cyber counterstrikes as part of a model of active defense. Active defense involves (1) detecting an intrusion, (2) tracing the intruder, and (3) some form of cyber counterstrike. n19

 [\*420] Though intrusion detection and tracing are essential, counterstriking is key to enhancing the deterrent effects of active defense. At its core, cyber counterstriking is about two things: (1) deterring attackers and (2) ensuring that attacked parties are not deprived of the inherent right to defend themselves and their property. There are many views of deterrence, but deterrence is generally accomplished by the threat of some combination of the following elements: (1) punishing attackers by inflicting unacceptable costs, or (2) preventing attackers from succeeding in their attacks. n20 These two elements of deterrence have led us to apply the terms "retributive counterstriking" and "mitigative counterstriking," respectively, to the counterstriking component of active defense.

In the cyber context, a "counterstrike" can involve any number of actions. As discussed in Part III.B, a counterstrike can involve the target executing its own Denial of Service ("DoS") attack against the attacker (for example, by redirecting the attacker's packets back at the attacker to knock the attacker's systems offline), n21 infecting the attacker's system with a virus or worm to permit the victim to take control, or a number of other options. The technologies available to execute counterstrikes are generally the same ones used in initial attacks; as we examine in more detail below, some of these currently available technologies permit an attack to be traced back to its origin -- with varying degrees of accuracy. Furthermore, there is now evidence that "cyber contractors" exist as part of what some have termed the new "military digital complex," whose work involves creating offensive cyber technologies that can have applications in the context of counterstriking. n22

The goal of a counterstrike can vary, from punishing the attacker to simply mitigating the harm to the target. We call the former "retributive counterstriking"; this type should remain under the sole control [\*421] of the military, as a national security matter relating to sensitive domestic and international legal issues. We define "mitigative counterstriking" as taking active efforts to mitigate harm to a targeted system, in a manner strictly limited to the amount of force necessary to protect the victim from further damage. We recognize there may be overlap between retributive and mitigative counterstriking, as the latter could potentially result in damage to the attacker's system. How-ever, the goal of mitigative counterstriking must be to mitigate damage from a current and immediate threat. We argue that whatever measures are deployed must be justifiable under a mitigation frame-work.

Cyber counterstrikes, however, are currently controversial, and it can be difficult under the current framework to differentiate between "hack back" vigilantism and legitimate exercises of a right to self-help. n23 Our proposal in this area is both modest and bold. Modest, because while we also discuss active defense as a broad topic, our primary focus is on mitigative counterstriking as a discrete subcategory of active defense activities. Bold, because we advocate for a significant shift from the prevailing approach to cyber intrusions. In recommending a new regime, we have chosen to focus on mitigative counterstriking as a starting point for two reasons. First, it is likely to be more effective than passive defense at accomplishing the goal of deterrence by denial. Second, a mitigative counterstriking regime would endow network administrators with the right to actively defend their property, thereby legitimizing the right to self-defense in the cyber realm. The current regime creates an unconscionable situation where parties are expected to give up the right to actively defend themselves against threats and instead rely on passive defense measures that may prove ineffective. Parties are left with no practical recourse through criminal enforcement or civil litigation for a number of reasons we discuss below.

Currently, the biggest barrier to defending against cyberattacks is the lack of a legal method to respond to cyberattacks that also has a credible deterrent effect on potential attackers. We posit that accurate and consistent use of mitigative counterstrikes could serve to deter cyberattacks against sensitive systems such as hospitals, government defense systems, and critical national infrastructure ("CNI"), and argue that implementing a regime to permit these sorts of counterattacks should be a priority. There is some evidence that the private sector has [\*422] been tacitly utilizing this sort of technology to protect their systems, n24 effectively acting as cyber vigilantes under the current regime. Such behavior is at best legally ambiguous, and at worst illegal. Currently, the idea of mitigative counterstriking is treated like the proverbial elephant in the room, with legal commentators largely ignoring it. n25 After careful analysis, we conclude that this neglect is due to the lack of an analytical framework distinguishing between the perceived vigilantism of retributive counterstriking and the employment of self-help through mitigative counterstriking.

We thus propose a new policy and legal regime to address the threat of cyberattacks using active defense and mitigative counterstriking. There is a grave need to standardize approaches to mitigative counterstrikes, n26 and we must determine when the use of mitigative counterstrikes is appropriate, as well as who should be permitted to conduct mitigative counterstrikes. We recognize that counterstrikes of any variety can raise a number of legal and diplomatic concerns. While additional analysis and technological development may be desirable before implementing a broad self-defense regime, we argue that implementing mitigative counterstriking capabilities to protect CNI should be the first priority. Cyberattacks significantly affect private parties, including owners of CNI, n27 so it is important to legitimize active defense and mitigative counterstriking approaches in order to afford these private parties more protection against these threats.

#### This solves future cyber conflict which escalates

Kramer et. al 12 (Franklin D. Kramer is a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He served as the assistant secretary of defense for international security affairs from 1996 to 2001. Stuart H. Starr is also a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He concurrently serves as the president of the Barcroft Research Institute. Larry Wentz is a senior research fellow in the Center for Technology and National Security Policy at the National Defense University., “Cyberpower and National Security”)

Cyber attacks—hacking of various kinds—are a fact of modern life. Nationstates, such as China, have been publicly accused of hacking for espionage purposes, and nonstate actors, such as criminals and terrorists, likewise have substantial capabilities. The steady state of modern life is that thousands of intrusions occur each day, some with important consequences. More ominously, there are concerns that attacks could be undertaken for geopolitical purposes by states or nonstate actors that would have far greater negative impact than has thus far occurred. The capacity to deter such attacks would be enormously valuable.

Cyber deterrence has been considered challenging because of the difficulty of attributing the source of cyber attacks. While attribution unquestionably is a consequential issue, we believe that deterrence in the context of cyber is a viable strategy and one on which the United States ought to embark much more advertently. The components of such a strategy would consist of the following elements, some of which would require development as discussed below.

First, any approach to deterrence of cyber attacks needs to be considered in an overall concept of deterrence, not as a separate cyber arena. Such an effort would use a combination of potential retaliation, defense, and dissuasion. It would be based on all elements of national power so that, for example, any retaliation would not necessarily be by cyber but could be by diplomatic, economic, or kinetic—or cyber—means, depending on the circumstances. Retaliation, when and if it occurred, would be at a time, place, and manner of our choosing.

In generating policy, some important differentiations could be consequential. State actors generally act for classic geopolitical aims and often are susceptible to classic geopolitical strategies. Retaliation of various sorts might be more available against state actors, and dissuasion likewise might be more effective. By contrast, nonstate actors could be less susceptible to classic geopolitical strategies (though indirect strategies, such as affecting the country in which they are based, may have impact). Cyber defense, law enforcement, and, for terrorists, classic counterterrorist techniques may be most effective.

One important question is whether there is a threshold at which more significant responses become appropriate. It bears restating that there are a great many intrusions already ongoing, and responses to them have not been dramatic. In analyzing this issue, it may be useful to separate what might be termed high-end attacks from low-end attacks. If one hypothesized a serious attack that rendered, for example, military or key financial systems inoperative, the probability would be that an extremely robust response would be appropriate. A state actor that undertook a high-end attack should certainly understand that the United States could carry out a countervalue response that would not be limited to a response on cyber assets. The potential of a response against the high-value elements of a state should add considerably to deterrence. Likewise, it should be clear that an attack in the context of an ongoing conflict, whether against a state or a nonstate actor, likely will receive a very significant response. Dealing with cyber actions by an actor with whom we are militarily engaged, such as al Qaeda or the insurgents in Iraq, seems different than dealing with a new problem where force has not already been used.

#### AND, they can’t win an impact turn – mission failure is inevitable without Congressional deliberation

**Griffin 12** – Professor of Constitutional Law @ Tulane University [Stephen Griffin, “The Tragedy of the War Power: Presidential Decisionmaking from Truman to Obama,” APSA 2012 Annual Meeting Paper, July 15, 2012, Pg. http://ssrn.com/abstract=2107467

As a comparison of the relative ability of the executive and legislative branches to make speedy decisions, Hamilton’s argument is certainly plausible as far as it goes, but in the kind of government we have had since the Cold War began, it does not take us very far. Swift decisionmaking has little to do with a presidential decision to initiate the kind of war that has occupied us here. Wars involving the potential of thousands of American casualties, millions of foreign casualties, and the expenditure of hundreds of billions of dollars are usually not based on off-the-cuff decisions. Korea (especially taking into consideration the decision to cross the 38th parallel), Vietnam and the 1991 Gulf War were enormous undertakings and required layers of complex interagency decisionmaking, not a single swift move. Indeed, these considerations were part of what made it necessary in 1947 to establish the NSC to coordinate policy within the executive branch.

During the Cold War and after, the pre-Pearl Harbor constitutional order was identified with isolationism and no one thought a return to that policy after 1945 was realistic. But while it is relevant to ask if there was an alternative, there is no escaping the ineluctable reality that the post-1945 order was a tragedy waiting to happen. That order was inconsistent with the historical meaning of the Constitution and the original constitutional order remained relevant to making decisions for war. Whether the post-1945 order was necessary or not, it introduced deep tensions into the American system of governance.

The case studies presented above show that the interagency process taking place inside the executive branch was not an adequate substitute for the constitutionally mandated interbranch process. The inability of the executive branch to deliberate and make effective decisions on its own manifested itself in surprising ways. The executive branch has repeatedly failed to engage in effective war planning. With respect to Korea, Truman had to cope with the novelty of limited war and the fact that he would have been criticized by Republicans if he had ordered MacArthur to stop at the 38th parallel to restore the status quo ante. Nonetheless, it was his decision alone to unite the peninsula, a decision made essentially on the fly. In turn, that caused China to intervene. Korea then became a conflict of unanticipated scope that ended in stalemate and ruined Truman’s last years in office. True to his initial decision to intervene, Truman did not share responsibility with Congress and so Congress escaped both a valuable learning experience and the blame for the war.

In addition, the case studies show that there is considerable evidence that the executive branch has had problems determining on war aims. President George H. W. Bush studiously avoided consulting Congress during the crucial period of decision in fall 1990 when it became possible to contemplate turning Operation Desert Shield into Desert Storm. This meant that he did not have to resolve on a unified set of war aims that would have been a necessary part of convincing Congress to authorize the war. Like Truman, Bush waited until it was too late to convince Congress and the public that the war had a point beyond forcing Iraq out of Kuwait. Thus the war had no substantial implications for policy and could not even help Bush remain in office. Not submitting the war to a timely congressional decision that Bush would have respected turned out not only to be counterproductive in terms of policy, but contrary to Bush’s political interests. Similarly, President George W. Bush failed to clarify what the war in Afghanistan was for beyond the removal of al Qaeda from Afghan territory. Partly as a consequence, the war became an endless struggle against the Taliban in both Afghanistan and Pakistan that is still ongoing as of 2012. It is striking that the executive, often represented by presidentialists as the branch that is most decisive and expert on matters of war, could consistently both fail to deliberate and fail to reach agreement on its goals in going to war. This suggests strongly that the pressures to shirk hard choices are too great to be overcome by one branch working alone. As I have argued throughout this article, the post-1945 constitutional order tended to derange the policy process inside the executive branch, producing not a set of swift successful decisions, but rather a series of policy disasters. The formulation of policy on Vietnam in the Johnson administration, for example, showed serious deficiencies that have not been taken into account by contemporary presidentialists. In essence, the advisers in the White House and the different departments in the executive branch found it impossible to move beyond the narrow orbit established by the president. Rather, the president and the idiosyncratic process he establishes tends to dominate the undoubted policymaking expertise of the different departments. The lack of planning for the aftermath of the Iraq War, with the president and policymakers in the White House falling prey to all sorts of false assumptions, showed that nothing had changed since Vietnam. I have also highlighted the costs of decisions for war on presidents. In doing so, I am not arguing that presidents who go to war suffer some sort of trauma. But there is good evidence that decisions for war are considerably different from other sorts of policy decisions. They can clearly impair presidential decision making, as was the case with Presidents Johnson and Nixon and probably both Bushes, father and son. There can be other, more subtle effects on policy. War can take up so much of the president’s time that other pressing concerns, including those related to foreign affairs, are crowded out. So President Johnson probably lost several chances to negotiate meaningful arms control agreements with the Soviet Union.217 This helped undermine the structure of détente in the 1970s by continuing the arms race. Preparing for and fighting the 1991 Gulf War so exhausted President Bush and his advisers that they had less capacity to make decisions with respect to the postwar environment in Iraq.218 This helped undermined the credibility of Bush’s decision not to depose Saddam Hussein. The 2003 Iraq War so consumed President George W. Bush and his advisers that they lost track of the situation in Afghanistan, leaving to President Obama the knotty task of sorting out the mess. As the discussion in this article has thus demonstrated, the defects of the post-1945 constitutional order are manifest. Experience has shown that the executive branch is incapable of handling the deliberation necessary for decisions for war on its own. Perhaps this is what we should expect, given the continued tidal pull of the original constitutional order. Yet it is still striking how consistently poor executive decision making for war has been in the post-1945 period. These defects create several distinct challenges for executive enthusiasts. For example, supporters of the presidentialist position often stress its unitary character. With a single person at the helm, the executive branch can act quickly to address foreign crises. We can now see more clearly that when the executive branch is not subject to oversight it is too easy either for presidents to dominate their advisers, thus suppressing valuable policy input (Johnson) or to so rearrange the White House policy process that an effective decisionmaking process becomes nearly impossible (Bush II). This supports the inference, which may come as a surprise to presidentialists, that a chief purpose of interbranch deliberation is to ensure that the executive branch is truly unitary and effective with respect to the all-important decision for war. Oversight also has the potential to counter the scenario in which the president totally dominates his advisers. Congressional hearings might give advisers a public forum in which they can finally get through to the president, although this is obviously a more difficult case. Without oversight, policy in the executive branch can be unsound or even deranged. One pathway to policy disaster, seen in Vietnam, is that the various departments responsible for war are never forced to agree on a unified set of goals and what means are necessary to achieve those goals. Without strong external compulsion it is too easy for the different parts of the executive branch to fall to quarreling amongst themselves without any ability to resolve their differences. When the State Department, Defense Department and the CIA fail to agree, the NSC process has been insufficient to create a consensus on a proposed course of policy. While it is reasonable to assume that the nation requires a unified foreign policy, nothing in the internal architecture of the executive branch that guarantees unity. Again, this can strike us as surprising, because the executive branch is a hierarchy and we expect presidents to have the ability to lead. Experience shows, however, that leadership is usually expressed either through domination involving the suppression of dissident views or by the president being unable or unwilling to manage the many different parts of the executive branch together with their often strong-willed department heads. Striking the appropriate balance has been difficult for presidents who are, after all, politicians, not experienced managers. Another pathway to disaster already mentioned is that it has proven difficult for the executive branch to determine war aims. Understandably the president and his advisers tend to respond to the exigencies of the moment, rather than concerning themselves with how a given military operation relates to the overall strategy of the U.S. in foreign affairs. The executive branch does not have any inherent ability to relate short-term responses to long-term goals. As we saw with the 1991 Gulf War, this inability to justify a war in terms of long-term goals can run contrary to the president’s own political interests. It is not necessary to assume anything about the policy knowledge of individual members of Congress or the quality of congressional hearings to appreciate that a world in which the executive branch is required to justify itself publicly provides a significant incentive for the president to insist on a unified approach

 to policy. It is plausible that repeated iterations of oversight would build up congressional expertise in foreign policy and thus begin a meaningful cycle of accountability where each branch could learn over time from experience. While there is a sense in which everyone accepts that oversight is a traditional function of Congress, it is noteworthy that there was no strong tradition of external review established in the early Cold War. The situation with respect to the CIA eventually became notorious, with a small group of senators handling oversight on a basis akin to a private club.219 But the situation with respect to foreign affairs in general was little better, with many hearings and exchanges held in executive session or off the books in private gatherings. While it is a mistake to think that the congressional leadership had no influence over the early Cold War administrations, the lack of public oversight meant that the proper incentives were never provided to executive branch agencies. As recounted by historian Robert Johnson, later in the Cold War the influence and prestige of the Senate Foreign Relations Committee waned in comparison with the growing power of the Armed Services Committee.220 This further undermined accountability and was emblematic of the dominant militarized approach to the Cold War. While the executive branch was retooled to a certain extent for Cold War duty after 1947, nothing was done to the structure of Congress. Members of Congress assumed that the existing committee structure would suffice. Eventually the costs of this approach became apparent, at least with respect to intelligence policy. Part of the intelligence reforms of the 1970s was to establish committees to oversee the intelligence community. The subsequent difficulties with implementing this oversight have been well analyzed by a number of scholars and presidential commissions, including the 9/11 Commission. Some of the ignored proposals of the 9/11 Commission had to do with changes to congressional oversight of intelligence.221 What oversight there is has been rendered less effective by the use of term limits for service on the intelligence committees and the fact that budgetary authority is located elsewhere.222 As Amy Zegart concluded in her study of Congress, the intelligence community and 9/11: It was no secret that this fragmented oversight system desperately needed fixing. Restructuring the Congress was recommended in seven of the twelve intelligence and terrorism studies between 1991 and 2001. Yet Congress never acted. In fact, Congress was the only government entity that failed to implement a single recommendation for reform during the decade—a record worse than either the CIA’s or the FBI’s.223 One purpose of the interbranch cycle of accountability is to test the executive branch’s claims with respect to war and foreign affairs. Of all the shibboleths of the Cold War, none have arguably done more harm than the idea that the executive branch’s undoubted expertise with respect to diplomacy is relevant to the expertise necessary for planning and running a war. The experience of presidential administrations in the post-1945 period is clear – there is no such thing as a civilian “expert” in making the policy choices and decisions necessary for war. Even if we accept the reasonable point that military leaders are expert in planning and running military operations, this sort of expertise is built up over many years of service and such experience was not available to any post-1945 president except Eisenhower. Consider that the substantial expertise FDR had acquired with respect to foreign policy by the time he was elected to a third term in 1940 is barred to any contemporary president by the 22nd Amendment. Further, cabinet officials and advisers are rarely drawn from a pool of those expert in war. As we drew away from the World War II generation, the Secretaries of State and Defense have usually been different sorts of careerists or politicians. While there is nothing inherently wrong with this, none of them were experts in making war decisions.224 In fact, there have been too few major wars for any civilian adviser to acquire the sort of experience necessary before true expertise is possible. At the same time, the major wars since 1945 show that effective consultation with Congress is pragmatically possible. Because American armies have been fighting far from home in the post-World War II period, considerable time has been required to transport them to the theatre of conflict and assemble the necessary enormous amount of supply material. Aside from true crises such as the 1962 Cuban missile crisis, there has always been plenty of time for interbranch deliberation over the decision to go to war. This has not always been highlighted by presidents. In Korea, many weeks were required before the Inchon landing and break-out from the Pusan perimeter became possible. In Vietnam, it took two years, until 1967, for General Westmoreland to assemble the supply chain necessary to support the kind of military operations he envisioned in 1965.225 The build-up time required to simply provide an effective defense for Saudi Arabia (Operation Desert Shield) in the Gulf War was seventeen weeks. More weeks were required to attain an offensive capability. Months were required after 9/11 before there were sufficient regular armed forces in Afghanistan and the same was true for the Iraq War. The fact of a crisis or apparent emergency that arguably requires a military response does not necessarily mean that there is little time for proper interbranch deliberation. The war powers debate should occur on the terrain of a realistic appraisal of presidential success in making decisions for war and the possible contributions a true interbranch dialogue could make to effective decisionmaking. Such an appraisal is not found in recent works by executive enthusiasts. Eric Posner and Adrian Vermeule, for example, have recently provided a provocative theoretical grounding for executive enthusiasm. 226 They present a tightly woven argument that challenges what they describe as the “Madisonian” understanding of separation of powers. Their target, which they call “liberal legalism,” is the idea that the executive can be constrained primarily through legal means, including the constitutional law promulgated by judges as well as statutes passed by Congress.227 While their argument is wide-ranging, extending to administrative law and “global liberal legalism,” my comments here are directed at the parts of their argument most nearly relevant to war and foreign affairs. There is arguably a subtle bias in the Posner and Vermeule analysis. They criticize the eighteenth-century “Madisonian” view of how an executive should be constrained. But why constrain the executive at all? Here Posner and Vermeule confine themselves to critiquing what might be called an eighteenth-century view of the dangers posed by the executive – chiefly the threat to civil liberties and the possibility, which they rightly discount, that the American term-limited president might turn into a tyrant.228 But they do not consider reasons for caution about the executive branch connected with our twentieth-century experience with war and foreign affairs. They believe one fatal problem with liberal legalism is that Congress can never catch up with emergencies. The nature of emergencies is that rules cannot be created in advance to handle them. By contrast, the executive is well suited to handling fast-changing situations – “in emergencies, only the executive can supply new policies and real-world action with sufficient speed to manage events.”229 While this is superficially plausible, it will have a strange ring to anyone who lived through Hurricane Katrina in 2005. Of course, this does not mean Congress somehow would have done better. Posner and Vermeule’s analysis is relentlessly comparative. The fact that the executive inevitably makes mistakes and fails sometimes does not show that liberal legalism is a workable alternative. What Posner and Vermeule do not consider is the enormous influence, amply demonstrated by the narrative I have presented, of the original constitutional order. Because Posner and Vermeule do not consider how constitutional orders work, they miss the significance of the original constitutional design. My argument has concerned war and foreign affairs. But it supports the general inference that the original design made it difficult for either branch to make good policy on its own. Sound policy with respect to war requires the branches to cooperate. While political parties have made such cooperation more difficult, parties are an example of how constitutional change tends to add to, rather than completely replacing, the original constitutional order.230 The discussion in this article has shown that policymaking in the executive branch becomes deranged without the oversight and input of the legislature. Posner and Vermeule have no way to account for this because they assume that executive branch is generally competent not only to execute the law but to make policy on its own. Strangely, they do not consider the generally poor record of the executive branch in war making in the post-1945 period. This period is littered not simply with mistakes, but with policy catastrophes that undermined the stability of the government as a whole. It is also noteworthy that Posner and Vermeule focus on the executive branch without managing to say much about the person of the president or how the president runs the White House. The post-World War II experience showed that the president was incapable of managing the tasks of war without the substantial support of Congress. Briefly summarized, the biggest problem with the arguments of executive enthusiasts is that they reflect pre-Vietnam understandings of how the executive branch makes decisions in foreign policy. It is as if the substantial and closely documented historical scholarship on the Vietnam War has made no impression on legal scholars who study presidential power. These scholars continue to treat the executive branch as if it were a black box full of the “best and the brightest” – knowledgeable experts willing to make hard choices and swift, yet measured and effective decisions.231 History shows differently. Conclusion War is a unique kind of policy. Even “limited” wars tend to subordinate the rest of the nation’s foreign policy to their requirements rather than the reverse. This has meant that in starting any major military conflict, the president is almost literally betting the ranch. All the more reason to ensure that there is sufficient deliberation before going forward. In the restrained phrasing of political scientist James Kurth, the U.S. would have been better off had “an authentic democratic process” been used to approve wars since 1945.232 The question for the future is whether such a process is possible. Pg. 31-37

## 2AC

### AT: Circumvention

#### Congressional opposition to the authority curbs Presidential action – robust statistical and empirical proof

Kriner 10 Assistant professor of political science at Boston University [Douglas L. Kriner, “After the Rubicon: Congress, Presidents, and the Politics of Waging War”, page 228-231]

Conclusion The sequence of events leading up to the sudden reversal of administration policy and the dramatic withdrawal of U.S. Marines from Lebanon clearly demonstrates that open congressional opposition to Reagan's conduct of the mission in Beirut was critically important in precipitating the change in course. By tracing the pathways of congressional in- fluence, the case study achieves two important objectives. First, it vividly illustrates Congress's capacity to influence the scope and duration of a use of force independent of major shifts in public opinion and changing conditions on the ground. The analysis makes clear that there was no dramatic shift in public opinion after the Beirut barracks bombing that compelled the Reagan administration to withdraw the Marines; in fact, in the wake of the attack the public rallied behind the president. As such, opponents of Reagan's policies in Congress initially fought against the tide of public opinion, and the modest decline in popular support for the president's handling of the Lebanon mission occurred only after a sustained campaign against the deployment on Capitol Hilt.89 Similarly, the administration's own internal analysis of the situation in early January 1984 makes clear that changing conditions on the ground did not necessitate a dramatic change in the nature of the Marine mission. Indeed, by the National Security Council's own estimate, some conditions in the region were actually improving. Instead, administration officials repeatedly emphasized domestic pressures to curtail the scope and duration of the Marine mission.90 Moreover, as the political and military situation in Lebanon worsened in late January and early February 1984, it is interesting that a number of key administration officials publicly and privately believed that there was a direct link between congressional opposition at home and the deterioration of the situation on the ground in the Middle East. Second, the case study illustrates how the formal and informal congressional actions examined in the statistical analyses of chapter 4 affected presidential decision-making through the proposed theoretical mechanisms for congressional influence over presidential conduct of military affairs developed in chapter 2. Vocal opposition to the president in Congress-expressed through hearings and legislative initiatives to curtail presidential authority, and the visible defection from the White House of a number of prominent Republicans and erstwhile Democratic allies-raised the political stakes of staying the course in Lebanon. Nothing shook Reagan's basic belief in the benefits to be gained from a strong, defiant stand in Beirut. But the political pressure generated by congressional opposition to his policies on both sides of the aisle raised the likely political costs of obtaining these policy benefits. Congressional opposition also influenced the Reagan administration's decision-making indirectly by affecting its estimate of the military costs that would have to be paid to achieve American objectives. In the final analysis, through both the domestic political costs and signaling mechanisms discussed in chapter 2 , congressional opposition contributed to the administration's ultimate judgment that the benefits the United States might reap by continuing the Marine mission no longer outweighed the heightened political and military costs necessary to obtain them. Finally, while the Marine mission in Lebanon is admittedly but one case, it is a case that many in the Reagan administration believed had important implications for subsequent military policymaking. In a postmortem review, Don Fortier of the National Security Council and Steve Sestanovich at the State Department warned that the debacle in Lebanon raised the possibility that, in the future, the decision to use force might be akin to an all-or-nothing decision. "If the public and Congress reject any prolonged U.S. role (even when the number of troops is small)," the administration analysts lamented, "we will always be under pressure to resolve problems through briefer, but more massive involvements-or to do nothing at all." Thus, from the administration's "conspicuously losing to the Congress" over Lebanon policy, Fortier and Sestanovich argued that the White House would have to anticipate costly congressional opposition if similar actions were launched in the future and adjust its conduct of military operations accordingly, with the end result being a "narrowing of options" on the table and more "limited flexibility" when deploying major contingents of American military might abroad.91 This last point echoes the first anticipatory mechanism posited in chapter 2, and reminds us that Congress need not overtly act to rein in a military action of which it disapproves for it to have an important influence on the scope and duration of a major military endeavor. Rather, presidents, having observed Congress's capacity to raise the political and tangible costs of a given course of military action, may anticipate the likelihood of congressional opposition and adjust their conduct of military operations accordingly.

### 2AC Consult Not Restriction

#### We meet and CI -- statutory restrictions include 5 things

KAISER 80 The Official Specialist in American National Government, Congressional Research Service, the Library of Congress [Congressional Action to Overturn Agency Rules: Alternatives to the Legislative Veto; Kaiser, Frederick M., 32 Admin. L. Rev. 667 (1980)]

In addition to direct statutory overrides, there are a variety of statutory and nonstatutory techniques that have the effect of overturning rules, that prevent their enforcement, or that seriously impede or even preempt the promulgation of projected rules. For instance, a statute may alter the jurisdiction of a regulatory agency or extend the exemptions to its authority, thereby affecting existing or anticipated rules. Legislation that affects an agency's funding may be used to prevent enforcement of particular rules or to revoke funding discretion for rulemaking activity or both. Still other actions, less direct but potentially significant, are mandating agency consultation with other federal or state authorities and requiring prior congressional review of proposed rules (separate from the legislative veto sanctions). These last two provisions may change or even halt proposed rules by interjecting novel procedural requirements along with different perspectives and influences into the process.

It is also valuable to examine nonstatutory controls available to the Congress:

1. legislative, oversight, investigative, and confirmation hearings;

2. establishment of select committees and specialized subcommittees to oversee agency rulemaking and enforcement; 3. directives in committee reports, especially those accompanying legislation, authorizations, and appropriations, regarding rules or their implementation; 4. House and Senate floor statements critical of proposed, projected, or ongoing administrative action; and 5. direct contact between a congressional office and the agency or office in question. Such mechanisms are all indirect influences; unlike statutory provisions, they are neither self-enforcing nor legally binding by themselves. Nonetheless, nonstatutory devices are more readily available and more easily effectuated than controls imposed by statute. And some observers have attributed substantial influence to nonstatutory controls in regulatory as well as other matters.3 It is impossible, in a limited space, to provide a comprehensive and exhaustive listing of congressional actions that override, have the effect of overturning, or prevent the promulgation of administrative rules. Consequently, this report concentrates upon the more direct statutory devices, although it also encompasses committee reports accompanying bills, the one nonstatutory instrument that is frequently most authoritatively connected with the final legislative product. The statutory mechanisms surveyed here cross a wide spectrum of possible congressional action: 1. single-purpose provisions to overturn or preempt a specific rule; 2. alterations in program authority that remove jurisdiction from an agency; 3. agency authorization and appropriation limitations; 4. inter-agency **consultation requirements**; and 5. congressional prior notification provisions

### 2AC Ableism

#### And—changing language doesn’t subvert ableism—their critique of language choices prevents genuine contestation of ableist oppression.

Perpetually Myself 11 — Perpetually Myself—a blog by an anonymous author self-described as “a historian, cat lover, autistic woman, Yankee fan, neurodiversity advocate, feminist, Harry Potter fan, Hunger Games fan, fantasy/science fiction reader, and general supporter of social justice,” 2011 (“It’s not enough to call out ableist language,” *Perpetually Myself*—a blog, May 2nd, Available Online at http://allies-person.tumblr.com/post/5141183778/its-not-enough-to-call-out-ableist-language, Accessed 03-02-2012)

Language is important, but more important still are the underlying assumptions which shape our society. Assumptions about who is valuable and who isn’t, about what the proper way to behave is, about what counts as “contributing” to to society/the economy/whatever…the list goes on and on. Widespread use of “crazy” and “lame” (etc.) are but symptoms of the larger problem—society is full of ableist assumptions, some of which are very obvious and some of which may be more subtle—but ableist nonetheless. The elimination of ableist words is but a small part of what needs to be done, and it frustrates and disappointments me that so much “social justice” work has stopped at language—which is in many ways the easiest part.

Take stigma against people with intellectual disabilities. I am glad that it’s no longer acceptable to use the r-word in many circles, and that other words are making some headway. (I struggle with ”idiot” and “crazy” and a lot of others myself in everyday speech.) But I don’t think this has actually done all that much to promote the equality and worth of people with intellectual disabilities. There is still the assumption that it is better to be “intelligent” (whatever that means), that mental illness (however you define that) is something to be pitied, and that, in short, it’s better to be non-disabled than not. The end result is a very shallow sort of “social justice” discourse that keeps all of the underlying problematic assumptions in place while giving lip service to equality. It’s very troubling.

Truly examining one’s ableism does not mean renaming the tags on your blog so that “lame” and “crazy” no longer appear. It is not being the fifth person on a thread to self-righteously proclaim that “idiot” is ableist, and then simply stopping at that. That is superficial, and oftentimes little more than a way for neurotypical and/or able-bodied people to publicly demonstrate their Good Ally status and pat themselves on the back. Examining one’s ableism means constantly questioning and re-formulating basic assumptions which are oftentimes so deeply ingrained that it’s hard even to see them, let alone disavow them. Take the assumption that “intelligence” is valuable, for instance. It’s so ingrained in our society, so hard to root out—I’ll not pretend to be perfect on this score—and yet doing so is vital if we are to create a world in which people with intellectual disabilities are equals—not simply people-seen-as-lesser whom are condescended to.

#### They dichotomize the able and disabled—turns the K

Bickenbacha et al WHO, Division of Mental Health and Prevention of Substance Abuse, Assessment and Classification Unit 1999 Jerome Models of disablement, universalism and the international classification of impairments, disabilities and handicaps Social Science & Medicine 48.9 Science Direct

Zola noticed that, quite unintentionally, the minority group approach tended to reinforce salient aspects of the medical conception of disability (see as well Barnartt and Seelman, 1988). Because of the medical understanding of impairments and the statistical requirement that measured phenomena be stable, disability, he argued, tends to be viewed as dichotomous and fixed: one either has (and so can be counted as having) a disability or not, and if one has a disability, one is limited by it to a fixed and determined degree in standardized contexts. While these may be features of impairments — given their biomedical grounding — they are not features that make sense when disabilities are fully contextualized in people’s lives.

As it happens, the developing sciences of rehabilitative and occupational therapy have moved away from this conception of disability and are sensitive to the spread of disability and its discontinuous nature. However, and here the irony is thickest, the minority group approach finds itself requiring a fixed and dichotomous sense of disability precisely in order to define the minority group of people with disabilities. One cannot engage in identity politics without establishing clear eligibility requirements for membership in the group. And this is precisely what Zola doubted could be done in any nonarbitrary manner.

#### Alt cannot overcome attitudes and impairments that contribute to societal inaccessibility

Burleson ‘11 [Elizabeth is a Professor at Pace University School of Law, “Perspective on Economic Critiques of Disability Law: The Multifaceted Federal Role in Balancing Equity and Efficiency” 1/1]

A. Administrative and Judicial Enforcement

It is important to ensure not only a strong, well-funded, and capable infrastructure to enforce the ADA, but also a staff knowledgeable and supportive of its statutory goal of eliminating discrimination against individuals with disabilities. Ultimately, neither Congress nor the judiciary is capable of legislating a change in attitudes towards people with disabilities. Laura Rothstein notes that institutions of “[h]igher education had evolved practices, policies, and procedures before other sectors affected by the ADA (with the exception of K-12 education).”103 Society-wide, integration is at best a precursor to acceptance. It is not acceptance itself. Carrie Basas notes that, “the daily struggle of managing other people’s reactions to and stereotypes about disability can become a job in itself.”104 She goes on to point out that, When “reasonable accommodation” is bandied about, minds ultimately turn to a list of tangible tools, equipment, and changes in the physical environment such as large-screen monitors, curb cuts, automatic doors . . . . without considering the combined effects of impairments, the cultural weight of disability, and the longterm impact of societal inaccessibility.105

#### Rejecting discourse does nothing and leaves attitudes unchanged.

**Kelly**, 12/**98** Peace Review

One might ask, in "listening" to violent language and to the people who use it, whether we are actually condoning such language. This is far from the case. To listen is not to pass judgment. When I listen to a person who, for example, uses sexist language, I am not lending my approval to sexist language. Instead, what I am saying is that the person behind the language, and my desire to make a connection with that person, are more important than the sexist language. If I refuse to listen to the person who uses sexist language, then I might prevent one particular case where sexist language is used. But I do nothing to overcome the person's sexist attitudes. She will continue to use sexist language long after I am out of sight. But if I give her a voice, if I show her respect, if I try to take her seriously as a person, then In the future pershapes she will be more apt to take what I say about sexism seriously. If she knows that sexist language bothers me, then perhaps she will be less likely to use it around me.

#### Exclusive focus on representations erodes meaningful reversal of structures of exploitation---discursive focus must supplement discussion of reform---key to survival

Henry **Giroux**, prof of edu and cultural studies at Penn State, **6** (Comparative Studies of South Asia)

Abstracted from the ideal of public commitment, the new authoritarianism represents a political and economic practice and form of militarism that loosen[s] the connections among substantive democracy, critical agency, and critical education. In opposition to the rising tide of authoritarianism, educators across the globe must make a case for linking **learning** to **progressive social change** while struggling to pluralize and critically engage the diverse sites where public pedagogy takes place. In part, this suggests forming alliances that can make sure every sphere of social life is recognized as an important site of the political, social, and cultural struggle that is so crucial to any attempt to forge the knowledge, identifications, effective investments, and social relations that constitute political subjects and social agents capable of energizing and spreading the basis for a substantive global democracy. Such circumstances **require** that pedagogy be embraced as a moral **and** political practice, one that is directive and not dogmatic, an outgrowth of struggles designed to resist the increasing depoliticization of political culture that is the hallmark of the current Bush revolution. Education is the terrain where consciousness is shaped, needs are constructed, and the capacity for individual self-reflection and **broad social change** is nurtured and produced. Education has assumed an unparalleled significance in shaping the language, values, and ideologies that legitimize the structures and organizations that support the imperatives of global capitalism. Efforts to reduce it to a technique or methodology set aside, education remains a crucial site for the production and struggle over those pedagogical and political conditions that provide the possibilities for people to develop forms of agency that enable them individually and collectively to intervene in the processes through which the material relations of power shape the meaning and practices of their everyday lives. Within the current historical context, struggles over power take on a symbolic and discursive as well as a material and institutional form. The struggle over education is about more than the struggle over meaning and identity; it is also about how meaning, knowledge, and values are produced, authorized, and made operational within economic and structural relations of power. Education is not at odds with politics; it is an important and crucial element in any definition of the political and offers not only the theoretical tools for a systematic critique of authoritarianism but also a language of possibility for creating actual movements for democratic social change and a new biopolitics that affirms life rather than death, shared responsibility rather than shared fears, and engaged citizenship rather than the stripped-down values of consumerism. At stake here is combining symbolic forms and processes conducive to democratization with broader social contexts and the **institutional formations** of power itself. The **key point** here is to understand and engage educational and pedagogical practices from the point of view of how they are bound up with larger relations of power. Educators, students, and parents need to be clearer about how power works through and in texts, representations, and discourses, **while at the same time** recognizing that power **cannot be limited** to the study of representations and discourses, even at the level of public policy. Changing consciousness is **not the same** as **altering the institutional basis of oppression**; at the same time, institutional reform c**annot take place** without a change in consciousness capable of recognizing not only injustice but also the **very possibility for reform**, the capacity to reinvent the conditions [End Page 176] and **practices** that make a **more just future possible**. In addition, it is crucial to raise questions about the relationship between pedagogy and civic culture, on the one hand, and what it takes for individuals and social groups to believe that they have any responsibility whatsoever even to address the realities of class, race, gender, and other specific forms of domination, on the other hand. For too long, the progressives have ignored that the strategic dimension of politics is inextricably connected to questions of critical education and pedagogy, to what it means to acknowledge that education is always tangled up with power, ideologies, values, and the acquisition of both particular forms of agency and specific visions of the future. The primacy of critical pedagogy to politics, social change, and the radical imagination in such dark times is dramatically captured by the internationally renowned sociologist Zygmunt Bauman. He writes, Adverse odds may be overwhelming, and yet a democratic (or, as Cornelius Castoriadis would say, an autonomous) society knows of no substitute for education and self-education as a means to influence the turn of events that can be squared with its own nature, while that nature cannot be preserved for long without "critical pedagogy"—an education sharpening its critical edge, "making society feel guilty" and "stirring things up" through stirring human consciences. The fates of freedom, of democracy that makes it possible while being made possible by it, and of education that breeds dissatisfaction with the level of both freedom and democracy achieved thus far, are inextricably connected and not to be detached from one another. One may view that intimate connection as another specimen of a vicious circle—but it is within that circle that human hopes and the chances of humanity are inscribed, and can be nowhere else.59

### 2AC LOJ

#### Appeals for institutional restrain are a crucial supplement to political resistance to executive power

David Cole Law @ Georgetown 12 “The Politics of the Rule of Law: The Role of Civil Society in the Surprising Resilience of Human Rights in the Decade after 9/11” http://www.law.uchicago.edu/files/files/Cole%201.12.12.pdf p. 51-53

As I have shown above, while political forces played a significant role in checking President Bush, what was significant was the particular substantive content of that politics; it was not just any political pressure, but pressure to maintain fidelity to the rule of law. Politics standing alone is as likely to fuel as to deter executive abuse; consider the lynch mob, the Nazi Party in Germany, or xenophobia more generally. What we need if we are to check abuses of executive power is a politics that champions the rule of law. Unlike the politics Posner and Vermeule imagine, this type of politics cannot be segregated neatly from the law. On the contrary, it will often coalesce around a distinctly legal challenge, objecting to departures from distinctly legal norms, heard in a court case, as we saw with Guantanamo. Congress’s actions make clear that had Guantanamo been left to the political process, there would have been few if any advances. The litigation generated and concentrated political pressure on claims for a restoration of the values of legality, and, as discussed above, that pressure then played a critical role in the litigation’s outcome, which in turn affected the political pressure for reform. There is, to be sure, something paradoxical about this assessment. The rule of law, the separation of powers, and human rights are designed to discipline and constrain politics, out of a concern that pure majoritarian politics, focused on the short term, is likely to discount the long-term values of these principles. Yet without a critical mass of political support for these legal principles, they are unlikely to be effective checks on abuse, for many of the reasons Posner andVermeule identify. The answer, however, is not to abandon the rule of law for politics, but to develop and nurture a political culture that values the rule of law itself. Civil society organizations devoted to such values, such as Human Rights Watch, the Center for Constitutional Rights, and the American Civil Liberties Union, play a central role in facilitating, informing, and generating that politics. Indeed, they have no alternative. Unlike governmental institutions, civil society groups have no formal authority to impose the limits of law themselves. Their recourse to the law’s limits is necessarily indirect: they can file lawsuits seeking judicial enforcement, lobby Congress for statutory reform or other legislative responses, or seek to influence the executive branch. But they necessarily and simultaneously pursue these goals through political avenues – by appealing to the public for support, educating the public, exposing abuses, and engaging in public advocacy around rule-of-law values. Unlike ordinary politics, which tends to focus on the preferences of the moment, the politics of the rule of law is committed to a set of long-term principles. Civil society organizations are uniquely situated to bring these long-term interests to bear on the public debate. Much like a constitution itself, civil society groups are institutionally designed to emphasize and reinforce our long-term interests. When the ordinary political process is consumed by the heat of a crisis, organizations like the ACLU, Human Rights First, and the Center for Constitutional Rights, designed to protect the rule of law, are therefore especially important. While Congress and the courts were at best compromised and at worst complicit in the abuses of the post-9/11 period, civil society performed admirably. The Center for Constitutional Rights brought the first lawsuit seeking habeas review at Guantanamo, and went on to coordinate a nationwide network of volunteer attorneys who represented Guantanamo habeas petitioners. The ACLU filed important lawsuits challenging secrecy and government excesses, and succeeded in disclosing many details about the government’s illegal interrogation program. Both the ACLU and CCR filed lawsuits and engaged in public advocacy on behalf of torture and rendition victims, and challenging warrantless wiretapping. Human Rights Watch and Human Rights First wrote important reports on detention, torture, and Guantanamo, and Human Rights First organized former military generals and admirals to speak out in defense of humanitarian law and human rights. These efforts are but a small subset of the broader activities of civil society, at home and abroad, that helped to bring to public attention the Bush administration’s most questionable initiatives, and to portray the initiatives as contrary to the rule of law. At their best, civil society organizations help forge a politics of the rule of law, in which there is a symbiotic relationship between politics and law: the appeal to law informs a particular politics, and that politics reinforces the law’s appeal, in a mutually reinforcing relation. Posner and Vermeule understand the importance of politics as a checking force in the modern world, but fail to see the critical qualification that the politics must be organized around a commitment to fundamental principles of liberty, equality, due process, and the separation of powers – in short, the rule of law. Margulies and Metcalf recognize that politics as much as law determines the reality of rights protections, but fail to identify the unique role that civil society organizations play in that process. It is not that the “rule of politics” has replaced the “rule of law,” but that, properly understood, a politics of law is a critical supplement to the rule of law. We cannot survive as a constitutional democracy true to our principles without both. And our survival turns, not only on a vibrant constitution, but on a vibrant civil society dedicated to reinforcing and defending constitutional values.

#### Indeterminacy makes advocacy of legal restraint *more* important for long-term checks on the executive

David Cole Law @ Georgetown 12 “The Politics of the Rule of Law: The Role of Civil Society in the Surprising Resilience of Human Rights in the Decade after 9/11” http://www.law.uchicago.edu/files/files/Cole%201.12.12.pdf p. 44-49

If political pressure from civil society, rather than the force of law itself or the separation of powers, is to be credited for the partial restoration of the rule of law in the decade afterSeptember 11, then it is essential that we understand how that politics works. In my view, it is a particular politics – a politics of the rule of law – that is required. And civil society has a peculiar role to play in facilitating and propagating that politics. Thus, a robust civil society devoted to the rule of law may be as important as the more formal elements of the rule of law in checking executive abuse. At the same time, as the Guantanamo cases illustrate, there is a complex interrelationship between this type of politics and more formal legal constraints. Legal disputes form the focal point for political organizing and advocacy for claims founded on rule-of-law values, and that organizing and advocacy in turn can affect the outcomes of legal disputes.

Politics, however, is not sufficient on its own. In The Executive Unbound, Eric Posner and Adrian Vermeule maintain that a robust political process is sufficient to deter executive abuse in times of crisis. They argue that in the modern era, the rule of law cannot effectively constrain the executive, especially in emergencies, but that the executive is sufficiently limited by political checks. 82

82 Eric Posner and Adrian Vermeule, The Executive Unbound: After the Madisonian Republic (2010). At first glance the past decade seems to vindicate Posner and Vermeule’s views, as political forces were more effective at checking the president than were Congress or the judiciary. But Posner and Vermeule’s valorization of politics over law overstates the power of politics, understates the force of law, and misses the complicated and essential interplay between the two. Posner and Vermeule may be right that the law alone is not enough, but they fail to see that politics alone is at least as wanting. In the end, the rule of law and politics must work in tandem. When they do, as they arguably did to an important extent in the wake of September 11, they can mount a significant defense of basic human rights and the rule of law against executive overreaching. To Posner and Vermeule, the rule of law and the separation of powers are, for all practical purposes, defunct. In their view, the modern executive cannot possibly be constrained by the legislative and judicial branches, or even by law itself. Like many commentators before them, they attribute this development largely to the growth of the administrative state and to the near constant state of emergency in which modern American government now seems to operate. 83 As a practical matter, the vast and complex matters subject to federal regulation require Congress to cede control to the executive, through broad delegations of authority to administrative agencies. Members of Congress lack the time and experience to micromanage such diverse matters as energy, commerce, transportation, telecommunications, the environment, and immigration. And the executive vastly outnumbers the other branches; about 98 percent of the federal government’s nearly two million employees work in the executive branch. Globalization exacerbates these trends, as the president is the nation’s primary voice abroad, and increasingly addressing our own social problems requires coordination across borders. In emergencies, the executive’s characteristics of speed, flexibility, unified command, and secrecy are especially valued, so Congress tends to delegate even more broadly, and courts in turn typically defer to executive action. Under these conditions, Posner and Vermeule maintain, it’s just not feasible for the other two branches to keep effective tabs on what the executive is up to. But where other commentators view these developments as profound challenges to our constitutional order, Posner and Vermeule insist that they are of little concern because political constraints on the executive render the rule of law unnecessary. That view, however, both underestimates the constraining force of law and overestimates the extent of political limits onexecutive overreaching. Dismissing the role of law, Posner and Vermeule sweepingly claim, sounding almost like critical legal studies scholars, that law is so indeterminate and manipulable as to constitute only a “façade of legality.” 85 But in assessing law’s effect, they look almost exclusively to formal indicia – statutes and court decisions. That approach disregards the possibility that law has a disciplining function long before cases get to court, and even when no case is ever filed, a reality to which anyone who has worked in the executive branch will attest. Executive officials generally cannot know in advance whether court review will be strict or deferential, and that uncertainty itself has a deterrent effect on the choices they make. There are plenty of reasons why executive lawyers generally take legal limits seriously: they take an oath and are acculturated to do so, they know that claims of illegality can undermine their programmatic objectives, and they cannot predict when they will end up in court. Similarly, in focusing on statutes and their enforcement by courts, Posner and Vermeule disregard the considerable checking function that Congress plays through means short of formal statutes, such as by holding oversight hearings, requesting information about or investigations of doubtful executive practices, or restricting federal expenditures. President Obama, who has had to fight tooth and nail with an obstructionist Congress on his every initiative, from economic reform to health care to closing Guantanamo, would certainly be surprised to learn that his power is “unbound.” At the same time, Posner and Vermeule have an unrealistically romantic view of the constraining force of politics. The “politics” they identify consists solely of the fact that presidents must worry about election returns, and must cultivate credibility and trust among the electorate. There are several reasons to doubt that these political realities are sufficient to guard against executive overreaching. First, and most fundamentally, while the democratic process is well designed to protect the majority’s rights and interests, it is terrible at protecting the rights of minorities, and even worse at protecting the rights of foreign nationals, who have no say in the political process. In times of crisis, the executive nearly always selectively sacrifices the rights of foreign nationals, often defending its actions by claiming that “they” don’t deserve the same rights that “we” do. To say the rule of law is superfluous because we have elections is to relegate foreign nationals, and minorities generally, to largely unchecked abuse. The political process did nothing to protect the foreign nationals rounded up during the Palmer Raids of 1919, the Japanese nationals and Japanese Americans interned during World War II, or the Arab and Muslim immigrants detained and abused after September 11Second, the ability of the political process to police the executive is hampered by secrecy. Much of what the executive does, especially in times of crisis, is secret, and even when some aspects of executive action are public, its justifications often rest on grounds that are assertedly secret. Courts and Congress have at least some ability to pierce that veil and to insist on accountability. Absent legal rights, such as those created by the Freedom of Information Act, the public has virtually no ability to do so. Third, the political process is a blunt-edged sword. Presidential elections occur only once every four years, and necessarily encompass a broad range of issues. They are therefore unlikelyto be effective at addressing specific abuses of power. Voters’ concerns about abstract institutional issues such as executive power may clash with their interests on the substantive merits of particular issues, such as whether to use military force in support of Libyan rebels. There is no guarantee that citizens will separate these issues in their minds, and no reason to believe that if they do so, they will favor abstract institutional concerns over specific policy preferences. Fourth, the political process is notoriously focused on the short term, while structural issues of separation of powers generally serve long-term values. It was precisely because ordinary politics tend to be short-sighted that the framers adopted a constitutional democracy. A constitution identifies those values that society understands as important to preserve for the long term, but knows it will be tempted to sacrifice in the short term. If ordinary politics were sufficient to protect such concerns, we would not need a constitution in the first place.

#### Adopting a prescriptive realist theory as a guide for foreign policy is critical to correct policy errors and minimize violence

**Rosato and Schuessler 11** –Assistant Professor of Political Science at the University of Notre Dame AND Assistant Professor of Strategy and International Security at the Air War College (Sebastian and John, “A Realist Foreign Policy for the United States”, Perspectives on Politics December 2011 Vol. 9 No. 4)

 With these requirements in mind, we describe and defend a prescriptive realist theoryof foreign policy to guide American decision makers as they navigate the current environment. Brieﬂy, the theory says that if they want to ensure their security, great powers such as the United States should **balance against other great powers** and also against hostile minor powers that inhabit strategically important regions of the world. We then show that had the great powers followed our theory’s prescriptions, some of the most important wars **of the past century might have been averted**. Speciﬁcally, the world wars might not have occurred, and the United States might not have gone to war in either Vietnam or Iraq. In other words, realism as we conceive it offers the prospect of **security without war**. Our argument is likely to be controversial because few observers think that a realist foreign policy can minimize the chances of war. Indeed, the main reason that “no one loves a political realist” arises from the intimate **association that realism is thought to have with war**. 13 The criticism takes several forms: some argue that realism is a license for aggression; others that it perpetuates competitive behavior; still others that it advances few ideas on how to overcome interstate conﬂict, thus foreclosing possibilities for progressive change. 14 As a result, most analysts consider realism an inappropriate guide to current US foreign policy. Liberals have been quite outspoken in leveling these kinds of charges, claiming that realism neglects transformative developments such as globalization, democratization, and the proliferation of international institutions, all of which offer the possibility of an enduring peace. 15 Robert Keohane observes that realism “is better at telling us why we are in such trouble than how to get out of it.” 16 Realism, that is, may explain why international politics is conﬂictual, but provides little guidance for overcoming that conﬂict peacefully. For Keohane, such complacency is morally unacceptable, leading him to conclude that “no serious thinker could . . . be satisﬁed with Realism as the correct theory of world politics.” He advises scholars to focus on international institutions instead: “Unlike Realism, theories that attempt to explain rules, norms, and institutions help us to understand how to create patterns of cooperation that could be essential to our survival.” 17 Bruce Russett adopts a similar tack in his defense of democratic peace theory. Realism, he notes, “has no place for an expectation that democracies will not ﬁght each other.” 18 This is important because understanding the sources of the democratic peace can have the effect of a self-fulﬁlling prophecy. By adopting a skeptical attitude toward the democratic peace, then, realists are at least indirectly diminishing the prospects for a world without war. 19 The constructivist charge is that realist discourse **perpetuates the very competition for power that realists purport to explain**. Anarchy, after all, is what states make of it; so if realists describe international politics as competitive, then states are more likely to act in precisely that way. 20 This is, in fact, Alexander Wendt’s critique in his seminal statement of constructivism. The problem with realism, he argues, is that it refuses to acknowledge that international politics can be anything but Hobbesian and in doing so impedes progress. In Wendt’s own words, “Realism’s commitment to self-interest participates in creating and reifying self-help worlds in international politics. To that extent Realism is taking an at least implicit stand not only on what international life is, but on what it should be; it becomes a normative as well as a positive theory.” 21 Critics have zeroed in on modern realism, the branch of the tradition that informs our theory. 22 Classical realism has recently undergone a revival among realism’s critics. Classical realists are described as being less ﬁxated **on narrow power considerations** than their successors and more attuned **to transformative developments** in world politics. They therefore have **more to contribute to** the cause of peace. Richard Ned Lebow has been a forceful advocate of this position, lamenting that the structural turn in realism has led to a vicious circle: “The language of classical realism, with all its subtlety, commitment to caution and respect for conventions, has been replaced by the cruder language of modern realism and its emphasis on power and expediency. These maxims, which have become conventional wisdom, guide policymakers, and their behavior in turn appears to conﬁrm the assumptions of the modern realist discourse.” Lebow concedes that many realists opposed the Iraq War and cannot be held responsible for the failures of US foreign policy, but in the same breath warns that modern realist discourse “has the potential to turn American hegemony into another tragedy.” 23 Michael Williams has joined the debate in a similar fashion, reconstructing a “wilful” realist tradition from the writings of Hobbes, Rousseau, and Morgenthau. For him, “wilful Realism is deeply concerned that a recognition of the centrality of power in politics does not result in the reduction of politics to pure power, and particularly to the capacity to wield violence. It seeks, on the contrary, a politics of limits that recognizes the destructive and productive dimensions of politics, and that maximizes its positive possibilities while minimizing its destructive potential.” 24 Williams is explicit that his “wilful” variant stands in stark contrast to most understandings of realism today, implying that modern realists do reduce politics to power maximization and eschew any limits on the exercise of that power, with destructive consequences. We dispute the conventional characterization of realism. Our position is that it is possible to develop a prescriptive realist theory—one derived from the core assumptions of modern realism—that meets a state’s security needs **while** minimizing **the likelihood of war**. 25 Our case proceeds as follows. We begin by describing our prescriptive realist theory of foreign policy. Next we describe an alternative liberal approach that promises perpetual peace rather than the mere stability implied by our theory. We then suggest that had the great powers behaved as our theory advises, **some of the most important wars of the past century** might have been avoided. At the same time, we show that **liberalism was at least partially to blame** for the outbreak of these wars. We conclude by us[e]ing our theory to outline a foreign policy for the United States, one that we argue should make the US secure, while simultaneously minimizing the likelihood **that it will become embroiled in future wars**.

### 2AC Security

#### Policy simulation is key to agency

Shane 12 [Peter, Jacob E. Davis and Jacob E. Davis II Chair of Law at Ohio State University, June 26, “Cybersecurity Policy as if 'Ordinary Citizens' Mattered: The Case for Public Participation in Cyber Policy Making,” I/S: A Journal of Law and Policy for the Information Society, Ohio State Public Law Working Paper No. 211, p. 433-6]

The total abdication of cybersecurity policy to “experts,” however, has been, and continues to be, a profound mistake. Given the ubiquity of computer networks and our reliance as a society on their integrity and robustness, the quality of cybersecurity is an issue that affects everyone’s interests. Excluding the general public from any meaningful voice [dialogue] in cyber policymaking removes citizens from democratic governance in an area where our welfare is deeply implicated. Further, as the papers in this volume amply testify, the “technologies” and the “processes” entailed in cybersecurity are costly, likely requiring significant public investment.2 Cybersecurity builds on “practices” that include routines and procedures in the hands of ordinary individual computer users.3 Mobilizing citizen backing for the requisite public investment in cybersecurity, and even more for the common commitment to adopt responsible computing habits, will be substantially more difficult if people have virtually no understanding of what they are being asked to do or to support.

Finally, the concern over decision-making competence is easy to overstate. The design of cybersecurity involves technical choices requiring specialized competence, just as does the implementation of environmental policy, biomedical research policy, or, for that matter, counterinsurgency strategy in Afghanistan. But the design of cybersecurity also implicates a series of choices among competing values and priorities that are the ordinary stuff of politics. The lay public’s inability to address strictly technical or expert questions does not mean it is incompetent to weigh competing policy answers to the general question, “What should the government do?”4

Indeed, I would argue that an administration explicitly committed to unprecedented levels of both transparency and collaboration5 should regard cybersecurity as offering an ideal opportunity to engage the public more meaningfully in policy deliberation than has so far been the American norm. Models abound, both in other nations’ use of citizen consultations to involve the public in technology-related policy making and in U.S. experience with citizen consultation in environmental decision making.6 Not only do such models offer the prospect of improving our cyber policy posture through public engagement, but meaningful citizen engagement in this area of complex decision making could provide a pivotal model for how to deepen the meaning of citizenship in the digital age.

In Part I of this essay, I will revisit the other contributions to this volume to illustrate the range of policy tradeoffs that could sensibly be opened up for public discussion. In Part II, I will discuss what ought to be the aims behind any project to incorporate public deliberation into cyber policymaking. Part III will review models of public input that could give lay citizens a meaningful recommending voice in the formulation of government cyber policy, and suggest the model best suited to meet the aims set forth in Part II. Part IV discusses the typical objections to genuinely collaborative public input, but argues that cyber policy provides an exceptional opportunity to set a precedent for the institutionalization of collaborative public involvement in policy making more generally.

The obvious threshold difficulty in creating a cybersecurity regime that resembles a “kinetic world” security regime is one of attribution: it is often exceedingly difficult, if not impossible, to discern the source of aggressive efforts to exploit the vulnerabilities of cyber systems.7 That fact directly implies that any cyber policy discussion is sooner or later going to focus on attribution, and set up a familiar debate between champions of security and champions of privacy. Before even contemplating how public input might be useful to that debate, however, it is worth emphasizing that the typical security-versus-privacy frame barely scratches the surface in terms of what Americans have at stake in the framing of cyber policy.

As a starting point, it is useful to note the contrast that the National Research Council (NRC) has delineated between “cyber attack” and “cyber exploitation.” The former term “refers to the use of deliberate actions . . . to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks.”8 An attempt to shut down an urban transportation system by disrupting the computer programs that govern its operations would be such a cyber attack. By contrast, cyber exploitation “is an intelligence-gathering activity rather than a destructive activity.”9 Its aim is to secure unauthorized access to confidential information, while allowing the computer system on which that information resides to run normally. Cyber exploitation is more like espionage than warfare. Yet, as the NRC notes, “[c]yber attack and cyber exploitation are often conflated in public discourse,” increasing the likelihood that policy discussions about cyber exploitation are distorted by the kinds of public anxiety stirred up by cyber attack scenarios.10

Policy making with regard to potential cyber attack from both an offensive and defensive posture is rife with the sorts of value questions on which informed citizens can make meaningful contributions. Not least among them, as this volume well documents, is the determination of appropriate responsibilities to be assigned to civilian and military authorities in responding to a cyber attack. Mark Young has sketched the ongoing evolution among federal entities, both military and civilian, of a series of operational relationships in cyber defense that he still regards as insufficiently mature to meet the current cyber threat.11 He identifies the debate about the Defense Department’s appropriate role in protecting civilian networks as one that should be discussed “openly and frequently.”12

#### China essentialism is a disad to them – we recognize war as just one possible outcome – they totalize Chinese decisionmaking

Andrew **Leonard** Senior Technology Writier @ Salon 8-21-**09** “Hu Jintao is no Kaiser Wilhelm” http://www.salon.com/tech/htww/2009/08/21/hu\_jintao\_is\_the\_new\_kaiser\_wilhelm/

I don't think Hu Jintao makes a good Kaiser Wilhelm and I think it is foolhardy to predict what will happen with the kind of thunderous certainty that is Ferguson's stock-in-trade. A superpower clash, whether economic or military, between the U.S. and China is in no one's interest. World War I, of course, wasn't ultimately in anyone's interest either, but Europe seems to have learned from its 20th century mistakes, at least so far, so maybe we can too. I'm with James Fallows; just to assert that a disastrous divorce is **inevitable** is positively dangerous because it ignores a **world of other possibilities**, and constricts our freedom to move. Even historians -- or especially historians -- recognize that world events are shaped in part by deep economic, demographic, and technical trends, but only in part. Real human beings make real decisions that have real effects. (Cf: LBJ in 1964, Bush-Cheney in 2001, JFK-Khrushchev in 1962, etc.) If we recognize that a collision with China is **possible,** but **only one of several possibilities**, then we act so as to reduce that possibility and increase the probability of **better outcomes**. If we think breakup is inevitable, as Ferguson is arguing, then the odds of a collision in fact occurring become higher than they would otherwise be. (Because each side interprets the other's moves in the darkest way and responds in kind.)

#### Securitizing cyber space is the only way to prevent large scale cyber war – the alt can’t solve fast enough or change US doctrine – vulnerability creates a unique need for it

Pickin 12 (Matthew, MA War Stuides – Kings College, “What is the securitization of cyberspace? Is it a problem?”, http://www.academia.edu/3100313/What\_is\_the\_securitization\_of\_cyberspace\_Is\_it\_a\_problem)

In analysing the problems of securitization, major issues have been raised. Threat inflation, surveillance, militarisation and the military-industrial complex are only some of the most prominent issues. There are benefits of securitization however, and at the very end of this analysis it will be explained why securitization is necessary for now. The main supporting arguments for securitization include, the future of cyber-attacks in conflicts, protecting critical infrastructure and cyber-crime. The 2010 National Intelligence Annual Threat Assessment stated that the United States was under a severe threat of cyber-attacks (Blair, 2010). Due to the amount of infrastructure connected to the internet in the United States targets for cyber-attacks are nearly unlimited, as a superpower the United States presents a valuable target. “As the world’s hegemonic power, the United States is also the main target state that dissident groups, terrorists, and rogue states wish to damage (Valeriano & Maness, 2011, p. 145).” Therefore, the United States must have some defence, or offensive capability in order to protect itself from future conflicts and attacks on critical infrastructure. In Foreign Affairs William J Lynn the former deputy secretary of defence wrote that the centrality of information technology in the United States makes it a prime target. He argued that extending advanced cyber-defences was crucial for the American economy, and also stated that failure of critical infrastructure would compromise national defence, “Our assessment is that cyber-attacks will be a significant component of future conflicts (Lynn, 2011).” Therefore in order to protect the United States, the government has been forced to securitize the issue. According to William J Lynn an attack could compromise national defence; therefore the issue is very high in the national security agenda. In the article, he also addresses the critics who argue that cyberspace is at risk of being militarized and states that US cyber strategy has been designed to prevent this from happening, “Far from militarizing cyberspace, U.S. cyber-strategy will make it more difficult for military actors to use cyberspace for hostile purposes (Lynn, 2011).” In securitizing cyberspace and creating advanced cyber-defences and cyber-weapons the United States is preparing for any future conflict or attack. If such an attack or conflict is a real existing threat then it is beneficial to prepare through securitization, otherwise the disadvantages clearly outweigh any advantage. The other main benefit of securitizing cyberspace would be tackling cyber-crime. According to the security company Sophos, in the first six months of 2010 it received 60,000 new malware samples every day. Apart from malware, cyber-crime covers many different areas such as financial, piracy, hacking and cyber-terrorism. These crimes are growing due to the constantly evolving communications system of social sharing of data, online data storage and social networking, “Although cybercrime has formed a hidden shadow and a kind of evil doppelganger to every step of the Internet’s long history from its very origins, its growth has suddenly become explosive in recent years by virtually any estimate (Deibert & Rohozinski, Contesting Cyberspace and the Coming Crisis of Authority, 2012, p. 28).” Both Deibert and Rohozinski argue that the rise is cyber-crime has become a big problem for states, in 2011 counterfeiting and copying cost the Asia-Pacific region almost $21 billion. Certainly cyber-space has become a rewarding way to commit crimes with little risk of prosecution, “Cybercrime has elicited so little prosecution from the world’s law enforcement agencies it makes one wonder a de facto decriminalization has occurred (Deibert & Rohozinski, Contesting Cyberspace and the Coming Crisis of Authority, 2012, p. 29).” Due to the trouble of cyber-crime, the only way of combating it effectively would be greater state regulation and intervention. With the whole of cyber-space effectively securitized by the United States due to the threat to national security by technological and social shifts, the government is asserting itself increasingly to counter these threats. Conclusion In analysing what was the securitization of cyberspace, the beginnings of the cyber-debate in the United States have been examined; this country was used due to reliance on information technology and the status as a superpower. The securitization model from the Copenhagen school of thought was used to understand how issues are non-politicized, politicized and eventually securitized. A different range of security bills have been examined with this model to understand what was needed for cyberspace to become a securitized issue. With the definition of securitization dependent on the terms of national security, the changing definition of this concept was also examined. Securitization has occurred due to an evolving history whereby the military have understood the potential of information technologies in warfare and where vulnerabilities have been recognised that could damage national security. In evaluating whether securitization of cyberspace is a problem, it is very clear that securitization is a growing concern with many complications. There are many issues including privacy, regulation, surveillance, internet regulation and the growing tension in the international system. However, because the United States is a superpower contesting with other cyber-heavyweights such as Iran, Russia and China the issue will not be de-securitized in the short term. With the discovery and use of cyber-weapons, many states are in the process of making their own for defensive and offensive purposes. The government of the United States will not de-securitize the issue of cyberspace while there are rival states and groups which prove a threat to the national security agenda. These problems will continue to exist until there is no defensive agenda and the issue is de-securitized, for now securitization is a necessary evil.

#### Perm solves—a catch all security possibly makes action impossible and matters worse – we must combine cyber policy with the alternative strategically – conceptualizing security in terms of intention is a viable vision for change

Anderson 12 (NICHOLAS D. ANDERSON Georgetown University M.A., Security Studies, 2012, ““Re re defining” International Security”, The Josef Korbel Journal of Advanced International Studies Summer 2012, Volume 4, PDF, http://www.du.edu/korbel/jais/journal/volume4/volume4\_anderson.pdf, NICHOLAS D. ANDERSON Georgetown University M.A., Security Studies, 2012, ““Re re defining” International Security”, The Josef Korbel Journal of Advanced International Studies Summer 2012, Volume 4, PDF, http://www.du.edu/korbel/jais/journal/volume4/volume4\_anderson.pdf, KENTUCKY)

First, too expansive a definition for security would make comparing similar policies essentially impossible, and distinguishing between different policy options inherently difficult (Baldwin 1997, 6). Take, for instance, the types of discussions surrounding counterinsurgency versus counterterrorism policies for the war in Afghanistan, with counterinsurgency being more people centered and counterterrorism being more threat centered. It is important to note that both are centrally concerned with security . But security for whom? And security fro m what? This is where a catch all security concept becomes problematic, for those advocating different positions will, in effect, be arguing for the same thing. And those making these ominous, life and death decisions will be left without the requisite clarity to make prudent, rational, and at times moral, judgments. Secondly, the human security concept has a bearing on bureaucratic questionsconcerning areas and responsibilities . Should we expect, for instance, the Department of Defense to be putting together clim ate change legislation proposals or running HIV/AIDS relief centers? Conversely, would it be wise to have the State Department, USAID, or the U.S. Geological Survey conducting operational planning? This isn’t to say that there shouldn’t be cross departmental collaboration and exchange, for today’s most complex security problems are often too much to handle for any one department alone. But these different agencies are designed, funded, and staffed according to different criteria and for different purposes. While more holistic approaches are undoubtedly necessary, a more clearly circumscribed security concept will help ensure that agency overlap won’t lead to detrimental results. Third, unlike academics, policymakers are tasked with the difficult requirement of allocating resources. Considering these requirements, if everything is a security threat, it is difficult to set priorities or single out areas of particular concern (Koblentz 2010, 108; Paris 2001, 92). If we conceive of such disparate issues as defic it spending, illegal immigration, the H1N1 virus, and the receding Arctic ice cap as “vital” security threats, right alongside the rise of China in Asia, Iranian nuclear proliferation, and al Qaeda training camps, knowing what matters when will be next to impossible. Fourth, if what constitutes a security problem or security threat is too broad, problems will be subject to incompatible policy solutions that could undercut each other, or will be paralyzed by competing demands, relegating them to lowest common denominator compromises (Koblentz 2010, 108). At the best of times, as the bureaucratic politics literature points out, this “pulling and hauling” in inter and intra agency battle leads to less than optimal outcomes, generally far from what would be decided upon according to more rational calculation (Allison 1969). If the meaning of what is being battled over lacks consensus, and the means to solve such problems come from every different direction, matters will be made far worse. Finally and perhaps most importantly, it is worth pointing out that security threats are used to justify the suspension of civil liberties, waging war, and legitimizing the reallocation of vast resources. In many cases , this is a necessary cost for maintaining security and part of the burden we must bear as citizens and members of democratic societies. And yet, even in the healthiest of democracies, we would be ill advised to provide the government an exponentially expanding list of “vital” security threats to protect against (B aldwin 1997, 8; Caldwell and Williams, Jr., 2006, 12). One can easily see how this is a potential first step on the road toward an Orwellian world much like that described in 1984: Oce ania being at war with Eurasia, and having always been at war with Euras ia (Orwell 2004). “Re redefinition”: Bringing Intent Back In How then, are we to define international security and what should be categorized as international security threats ? Arguably, the most intelligent way of narrowing the definition of internatio nal security is to accept the wide variety of possible threatened agents, but to restrict allowable threats to those with international implications that include the fundamental aspect of human agency or intent. This circumscription of the concept will hel p avoid many of the critical theoretical and policy problems outlined above. Furthermore, it is important to distinguish between tangible international security problems and what might be termed “ latent security problems.” Adherents to the human security p aradigm may argue that this distinction is not worth making, but it is important to recognize that nearly anything can have international security implications if the causal chain is drawn long enough. A useful rule of thumb is the more deliberate an inter national threat, the more justifiably it can be classified as a security issue (Caldwell and Williams, Jr., 2006, 11). Under this definition then, many of the modern era’s purported rising “nontraditional threats” (Mathews 1997, 51) do not necessarily me rit classification as international security problems. Rather than being vital security issues in and of themselves, those that exclude the important aspect of human agency are better classified as “latent . ” Climate change in the developing world, for inst ance, promises to bring food and water shortages, catastrophic natural disasters, deadly disease, mass human migration, and resource competition (Podesta and Ogden 2007 2008, 116). And yet, while it certainly poses an international threat, it does not meri t classification as a vital security threat in itself, because of the absence of intent. Deadly infectious diseases such as HIV/AIDS or the Avian flu are another such example. While they are clearly important problems posing potentially grave threats to individuals around the globe, classifying them as threats to international security will only cloud the necessary clarity needed to think and act intelligently in dealing with these problems (McInnes and Rushton 2010, 225). A great number of other examples that are often raised, such as poverty, economic recession, drug abuse, declining natural resources, and rapid urbanization and population growth, simply are what they are , and are not definitively vital issues of international security. While each has the potential to lead to serious international problems, even security problems, they are simply too many steps removed from posing a direct security threat to states, governments, militaries, communities, and individuals in the international system. A number of today’s oft cited threats to international security, on the other hand, are rightly categorized as such. The traditional issues of interstate conflict, military threats, arms races, nuclear deterrence, and contestation of the commons obviously continue to fit the definition. Some of the more recent threats , too, such as nuclear proliferation among “rogue” and weak states (Litwak 2007), increased international piracy, expanding organized crime rings, and international terrorism (Byman 2008; Cronin 2006; Rob erts 2005) all include human agency and have international implications, therefore befit ting the classification as international security problems. Even many emerging threats can be considered as such . Cyber threats, for instance, fit this classification if they are carried out with the intent to threaten the state, its military, or its people (Diebert and Rohozinski 2010). For example, Chinese hackers stealing trade secrets is not an international security issue, whereas cyber penetration of classified intelligence files or online terrorist recruitment and funding are. Biosecurity threats, too, can be justifiably classified as international security problems, but only if they include the fundamental issue of intent. Bio warfare, bio terrorism, maliciou s dual use biological research, and bio crime with violent intent or consequences are all obvious threats to international security. Laboratory accidents, pandemic and epidemic diseases, and agricultural blights, on the other hand, are not (Koblentz 2008, 111). 7 Admittedly, the lines are not nearly as clear as they have been made out to be here. Issues like military accidents, inadvertent missile launches, and abandoned mine fields fit within a grey area between tangible and potential international security problems. But these problems , among many others, can still be traced back to the key concept of intent. Militaries, missiles, and landmines are created and maintained with the intent of deterring, threatening, or even harming governments, militaries, co mmunities, and individuals, and although the harms they may happen to commit may not be intentional on given occasions, they still carry with them this important aspect of intentionality. And so an accidental nuclear weapon detonation should certainly be considered a true international security problem, but nuclear reactor accidents, even meltdowns, no matter how threatening, should not.

#### Prefer specificity—empirical validity is a sufficient justification for action

Owen 2 (David, Reader of Political Theory at the Univ. of Southampton, Millennium, Vol 31, No 3)

Commenting on the ‘philosophical turn’ in IR, Wæver remarks that ‘[a] frenzy for words like “epistemology” and “ontology” often signals this philosophical turn’, although he goes on to comment that these terms are often used loosely.4 However, loosely deployed or not, it is clear that debates concerning ontology and epistemology play a central role in the contemporary IR theory wars. In one respect, this is unsurprising since it is a characteristic feature of the social sciences that periods of disciplinary disorientation involve recourse to reflection on the philosophical commitments of different theoretical approaches, and there is no doubt that such reflection can play a valuable role in making explicit the commitments that characterise (and help individuate) diverse theoretical positions. Yet, such a philosophical turn is not without its dangers and I will briefly mention three before turning to consider a confusion that has, I will suggest, helped to promote the IR theory wars by motivating this philosophical turn. The first danger with the philosophical turn is that it has an inbuilt tendency to prioritise issues of ontology and epistemology over explanatory and/or interpretive power as if the latter two were merely a simple function of the former. But while the explanatory and/or interpretive power of a theoretical account is not wholly independent of its ontological and/or epistemological commitments (otherwise criticism of these features would not be a criticism that had any value), it is by no means clear that it is, in contrast, wholly dependent on these philosophical commitments. Thus, for example, one need not be sympathetic to rational choice theory to recognise that it can provide powerful accounts of certain kinds of problems, such as the tragedy of the commons in which dilemmas of collective action are foregrounded. It may, of course, be the case that the advocates of rational choice theory cannot give a good account of why this type of theory is powerful in accounting for this class of problems (i.e., how it is that the relevant actors come to exhibit features in these circumstances that approximate the assumptions of rational choice theory) and, if this is the case, it is a philosophical weakness—but this does not undermine the point that, for a certain class of problems, rational choice theory may provide the best account available to us. In other words, while the critical judgement of theoretical accounts in terms of their ontological and/or epistemological sophistication is one kind of critical judgement, it is not the only or even necessarily the most important kind. The second danger run by the philosophical turn is that because prioritisation of ontology and epistemology promotes theory-construction from philosophical first principles, it cultivates a theory-driven rather than problem-driven approach to IR. Paraphrasing Ian Shapiro, the point can be put like this: since it is the case that there is always a plurality of possible true descriptions of a given action, event or phenomenon, the challenge is to decide which is the most apt in terms of getting a perspicuous grip on the action, event or phenomenon in question given the purposes of the inquiry; yet, from this standpoint, ‘theory-driven work is part of a reductionist program’ in that it ‘dictates always opting for the description that calls for the explanation that flows from the preferred model or theory’.5 The justification offered for this strategy rests on the mistaken belief that it is necessary for social science because general explanations are required to characterise the classes of phenomena studied in similar terms. However, as Shapiro points out, this is to misunderstand the enterprise of science since ‘whether there are general explanations for classes of phenomena is a question for social-scientific inquiry, not to be prejudged before conducting that inquiry’.6 Moreover, this strategy easily slips into the promotion of the pursuit of generality over that of empirical validity. The third danger is that the preceding two combine to encourage the formation of a particular image of disciplinary debate in IR—what might be called (only slightly tongue in cheek) ‘the Highlander view’—namely, an image of warring theoretical approaches with each, despite occasional temporary tactical alliances, dedicated to the strategic achievement of sovereignty over the disciplinary field. It encourages this view because the turn to, and prioritisation of, ontology and epistemology stimulates the idea that there can only be one theoretical approach which gets things right, namely, the theoretical approach that gets its ontology and epistemology right. This image feeds back into IR exacerbating the first and second dangers, and so a potentially vicious circle arises.

#### Realism is inevitable in the context of cyberwar

Kallberg and Thuraisingham 13 [Jan, PhD from the University of Texas at Dallas, and Bhavani, University of Texas at Dallas, March, “From Cyber Terrorism to State Actors’ Covert Cyber Operations,” http://works.bepress.com/jan\_kallberg/12/]

Cyber is already by definitions and doctrine a war-fighting domain even if only few states are able to do any offensive cyber operations, but the strategic abilities will grow in the next decade. There are several reasons why cyber weapons are inviting. In an era of austerity the countries seek alternative to traditional military policy options, better suited for future conflicts and also reduces the collateral damage that kinetic operations creates. The pursuit of cyber abilities also drills down to pure financial numbers(Kallberg and Lowther 2012). Militaries are expensive and require a standing force to ensure ability and deterrence. If the force is a professional army it will cost to recruit, train, provide salary and benefits for, and last require veterans’ pension for forty years after service. In modern state reasoning, cyber warfare is a cheaper option for both covert operations and to engage and destabilize an adversary (Kallberg and Lowther 2012). States act in their own self-interest; therefore it is questionable if a regulated cyberspace is in the long-term interest of the major powers, as a restrictive use of cyberspace would undermine their dominant status. Earlier efforts to create a uniform approach towards IT-security on a global scale have shown marginal progress. One example is the global standard for security certification of hardware, “Common Criteria”, that has be hindered by the lack of unrestricted trust between nations (Kallberg 2012a). If any international effort fails to create a uniform approach to securing the Internet domain we can assume by logic that major actors prefer the anarchy before order because there is a perceived opportunity and potential future gain for these powers.

## 1AR

### 1AR Ableism

#### Rejecting their “call out” strategy is crucial to constructive activism—vote against them to facilitate productive dialogue about ableist language

Kinzel 11 — Lesley Kinzel, blogger and social justice writer, has written for *Newsweek* and *Marie Claire*, was named one of the Feminist Press’s “40 Feminists Under 40,” 2011 (“On our difficult language, and the calling-out of,” *Two Whole Cakes*—a blog about body politics, social justice activism, and pop-cultural criticism from a feminist perspective, March 30th, Available Online at http://blog.twowholecakes.com/2011/03/on-our-difficult-language-and-the-calling-out-of-same/, Accessed 03-02-2012)

We throw “that’s ableist” or “that’s racist” or “that’s fatphobic” around, I suspect, in the hope that such heavy judgement-bearing words will shock and embarrass the speaker out of using the offending language. And sometimes, it can work, at least in the short term, when we are merely thinking of our own self-preservation. But beyond that instant, this is not constructive activism. Using surprise, guilt, or humiliation as negative reinforcement to change behavior does nothing to instruct the person in question on why their behavior is causing problems; they stop simply because they don’t want to get in trouble. While the power shift this approach employs may feel awfully satisfying to those of us who have labored under some degree of oppression for much our lives—we get to dictate the terms of engagement, for once—merely shifting the power from one hand to another does nothing to change the destructive use of said power against us.

This practice of shaming people into behaving a certain way or using certain language does not truly address the underlying inclination; it does not unpack the thinking that allowed that speaker to feel entitled to say those things in the first place. Fear can be an effective motivator, but it’s not often a productive one, if our goal is broad and lasting cultural change. It is, after all, fear that motivates folks of all sizes to diet, that keeps queer folks in the closet, that makes women afraid to walk alone at night, that compels people of color to keep their heads down even in the face of overt discrimination and just get by. It is fear and shame that locks the systems that marginalize us in place, and as Audre Lorde has explained, in one of the most brilliant pieces of writing on social justice ever put to paper, there is little we can do while still holding on to the master’s tools.

Those of us who stand outside the circle of this society’s definition of acceptable women; those of us who have been forged in the crucibles of difference — those of us who are poor, who are lesbians, who are Black, who are older — know that survival is not an academic skill. It is learning how to stand alone, unpopular and sometimes reviled, and how to make common cause with those others identified as outside the structures in order to define and seek a world in which we can all flourish. It is learning how to take our differences and make them strengths. For the master’s tools will never dismantle the master’s house. They may allow us temporarily to beat him at his own game, but they will never enable us to bring about genuine change. And this fact is only threatening to those women who still define the master’s house as their only source of support.

Ideally, people should stop using certain language because they have developed an understanding of why that language is oppressive, and how their use of it contributes to inequality and marginalization, and not because they are afraid or ashamed of confusing social repercussions they do not understand. What we need is a commitment to giving people clear explanations—be they angry, or impassioned, or blunt—of why their words or behavior are problematic, or upsetting, or damaging. We need to resist relying on comfortable jargon to call people out, and to ditch the erroneous presumption that making someone feel stupid will encourage them to read more about a subject. It doesn’t work. Fear and shame don’t help people to understand how the language we use and the actions we undertake, even in our own small individual spheres, all conspire to create a social environment that oppresses us. Fear breeds resentment and, sometimes, hatred. These are not things we need more of. These are the things that put us here in the first place.

#### We are sincerely sorry—Apologies are effective and best

Latiff 01 (81 B.U.L. Rev. 289, p ln)

A coerced apology can mitigate anger even if it is perceived as insincere, and regardless of the offender's level of responsibility. Two studies support this assertion. In a study by psychologists Mark Bennett and Christopher Dewberry, subjects were asked to indicate how they would respond in a hypothetical situation in which they received an unconvincing apology for a moderately serious transgression. n159 Though Bennett and Dewberry drafted the apology to be disingenuous, all of the subjects nonetheless indicated that they would accept it. n160 In another, related study, Bennett and Deborah Earwaker sought to fill the gaps to Bennett and Dewberry's study by identifying the conditions under which an apology is accepted or rejected. n161 [\*312] The experimenters found that the degree to which the apology would dissipate anger had no relation to the offender's degree of responsibility for the offense —though it was significantly related to the severity of the offense. n162 In both the high and the low responsibility conditions, subjects indicated that an apology would substantially mitigate their anger. n163 Furthermore, though the degree of responsibility did have an effect on whether the subjects would ultimately accept the apology, the "likelihood that an apology [would] be rejected is remarkably small, even when there is considerable provocation." n164 Indeed, coerced or ordered apologies can be valuable in their capacity to mitigate anger and move the victim and community closer to the resolution of a crime. As part of the remedy for the arson of a church in Kentucky founded by freed slaves, the district judge in the case ordered the offenders (all white) to apologize to the church's current congregation. n165 Bill Sircy, one of the arsonists, bowed his head in front of the congregation and exclaimed, "We're sorry, but I know that's not enough." n166 The congregation responded, "Amen!" n167 After each of the four persons involved gave an apology, the congregation responded with a round of applause. One member remarked, "I think what they did was a fantastic gesture." n168 Additionally, a court-ordered or insincere apology can be effective as a shaming sanction. "Say your boss wrongfully accused you in front of the whole office. A fair reparation would require an apology —in front of the whole office. His questionable sincerity might be of secondary importance." n169 A punitive atmosphere surrounding an apology may force an exchange of shame and power between offender and victim, thus achieving what is at the heart of a successful apologetic ritual. n170 To be sure, several judges who have ordered apologies have done so in order to shame the offenders in front of their victims or their community. n171[\*313] Apology as a shaming sanction can have both retributive and deterrent value. First, a coerced apology can heal the community by "saying the right thing" in its expression of moral condemnation for the offender's conduct. Alternative sanctions, like community service, often fail to satisfy the public thirst for retribution because they fail to reaffirm the moral order. n172 On the other hand, as Professor David Karp argues, shaming sanctions, like apology, often satisfy this "retributive" thirst by communicating and enforcing normative, as opposed to legal, standards. n173 An apology as a shaming sanction communicates that the offense has not only a legal nature, but a moral and social nature as well. n174 The ordered apology requires the offender to demonstrate knowledge of the moral order that he transgressed, and culpability for having transgressed it. n175 Additionally, an ordered apology can deter future transgressions. n176 An ordered public apology can deter wrongdoing by 1) imposing some limitation on the offender's freedom, 2) creating an unpleasant emotional experience for the offender, and 3) harming the offender's social attachments and esteem. n177 For example, some offenders might feel that an apology is a sign of weakness, and others may just not want to admit that what they did was wrong. Thus, an ordered apology will force such offenders to swallow their pride and go through a potentially embarrassing, uncomfortable experience. Further, public apologies submit the offender to the judgment of the community. Some members of the community may not wish to associate with the offender again. Accordingly, the offender's social esteem and communal attachments may suffer. n178

### LOJ

#### VTL is inevitable

**Schwartz 2**, Lecturer in Philosophy of Medicine at the Department of General Practice at the University of Glasgow ‘02 (Lisa, , Medical Ethic: A case-based approach, Chapter 6: A Value to Life: Who Decides and How?, www.fleshandbones.com/readingroom/pdf/399.pdf)

The second assertion made by supporters of the quality of life as a criterion for decision— making is closely related to the first, but with an added dimension. This assertion suggests that the determination of the value of the quality of a given life is a subjective determi-nation to be made by the person experiencing that life. The important addition here is that the decision is a personal one that, ideally, ought not to be made externally by another person but internally by the individual involved. Katherine Lewis made this decision for herself based on a comparison between two stages of her life. So did James Brady. Without this element, decisions based on quality of life criteria lack salient information and the patients concerned cannot give informed consent. Patients must be given the opportunity to decide for themselves whether they think their lives are worth living or not. To ignore or overlook patients’ judgement in this matter is to violate their autonomy and their freedom to decide for themselves on the basis of relevant informa— tion about their future, and comparative con— sideration of their past. As the deontological position puts it so well, to do so is to violate the imperative that we must treat persons as rational and as ends in themselves.It is important to remember the subjectiv-ity assertion in this context, so as to empha-size that the judgement made about the value of a life ought to be made only by the person concerned and not by others.

#### Consequences matter – the tunnel vision of moral absolutism generates evil and political irrelevance

Issac 02 (Jeffery, Professor of Political Science at Indiana University, Dissent, Vol. 49 No. 2, Spring, 2002)

Politics, in large part, involves contests over the distribution and use of power. To accomplish anything in the political world one must attend to the means that are necessary to bring it about. And to develop such means is to develop, and to exercise, power. To say this is not to say that power is beyond morality. It is to say that power is not reducible to morality. As writers such as Niccolo Machiavelli, Max Weber, Reinhold Niebuhr, Hannah Arendt have taught, an unyielding concern with moral goodness undercuts political responsibility. The concern may be morally laudable, reflecting a kind of personal integrity, but it suffers from three fatal flaws: (1) It fails to see that the purity of one’s intentions does not ensure the achievement of what one intends. Abjuring violence or refusing to make common cause with morally comprised parties may seem like the right thing, but if such tactics entail impotence, then it is hard to view them as serving any moral good beyond the clean conscience of their supporters; (2) it fails to see that in a world of real violence and injustice, moral purity is not simply a form of powerlessness, it is often a form of complicity in injustice. This is why, from the standpoint of politics-as opposed to religion-pacifism is always a potentially immoral stand. In categorically repudiating violence, it refuses in principle to oppose certain violent injustices with any effect; and (3) it fails to see that politics is as much about unintended consequences as it is about intentions; it is the effects of action, rather than the motives of action, that is most significant. Just as the alignment with “good” may engender impotence, it is often the pursuit of “good” that generates evil. This is the lesson of communism in the twentieth century: it is not enough that one’s goals be sincere or idealistic; it is equally important, always, to ask about the effects of pursuing these goals and to judge these effects in pragmatic and historically contextualized ways. Moral absolutism inhibits this judgment. It alienates those who are not true believers. It promotes arrogance. And it undermines political effectiveness.

#### War outweighs structural violence—their impact can’t turn ours

**Boulding 90** (Kenneth E., Conflict: Readings in Management and Resolution, Ed: John Burton, pg. 40-41)

I must confess that when I first became involved with the peace research enterprise 25 years ago I had hopes that it might produce something like the Keynesian revolution in economics, which was the result of some rather simple ideas that had never really been thought out clearly before (though they had been anticipated by Malthus and others), coupled with a substantial improvement in the information system with the development of national income statistics which reinforced this new theoretical framework. As a result, we have had in a single generation a very massive change in what might be called the "conventional wisdom" of economic policy, and even though this conventional wisdom is not wholly wise, there is a world of difference between Herbert Hoover and his total failure to deal with the Great Depression, simply because of everybody's ignorance, and the moderately skillful handling of the depression which followed the change in oil prices in 1-974, which, compared with the period 1929 to 1932, was little more than a bad cold compared with a galloping pneumonia. In the international system, however, there has been only glacial change in the conventional wisdom. There has been some improvement.Kissinger was an improvement on John Foster Dulles. We have had the beginnings of detente, and at least the possibility on the horizon of stable peace between the United States and the Soviet Union, indeed in the whole temperate zone-even though the tropics still remain uneasy and beset with arms races, wars, and revolutions which we cannot really afford. Nor can we pretend that peace around the temperate zone is stable enough so that we do not have to worry about it. The qualitative arms race goes on and could easily take us over the cliff. The record of peace research in the last generation, therefore, is one of very partial success. It has created a discipline and that is something of long-run consequence, most certainly for the good. It has made very little dent on the conventional wisdom of the policy makers anywhere in the world. It has not been able to prevent an arms race, any more, I suppose we might say, than the Keynesian economics has been able to prevent inflation. But whereas inflation is an inconvenience, the arms race may well be another catastrophe. Where, then, do we go from here? Can we see new horizons for peace and conflict research to get it out of the doldrums in which it has been now for almost ten years? The challenge is surely great enough. It still remains true that war, the breakdown of Galtung's "negative peace," remains the greatest clear and present danger to the human race, a danger to human survival far greater than poverty, or injustice, or oppression, desirable and necessary as it is to eliminate these things.