# Cyberwar – Coast

**Status quo unregulated policy means there are no common rules of engagement in cyberspace –causes militarization**

**Gjelten 13**, Tom, correspondent for NPR, “Pentagon Goes On The Offensive Against Cyberattacks” February 11, 2013, http://www.npr.org/2013/02/11/171677247/pentagon-goes-on-the-offensive-against-cyber-attacks

Those assurances are deceptive. Behind the scenes, U.S. commanders are committing vast resources and large numbers of military personnel to planning offensive cyberattacks and, in at least some cases, actually carrying them out. But the secrecy surrounding offensive cyberwar planning means there has been almost no public discussion or debate over the legal, ethical and practical issues raised by waging war in cyberspace. Offensive cyberattacks carried out by the United States could set precedents other countries would follow. The rules of engagement for cyberwar are not yet clearly defined. And the lack of regulation concerning the development of cyberweapons could lead to a proliferation of lethal attack tools — and even to the possibility that such weapons could fall into the hands of unfriendly states, criminal organizations and even terrorist groups. In some cases, offensive cyberattacks are being conducted within the parameters of conventional military operations. In Afghanistan, soldiers and Marines depend heavily on video and data links when they go into combat. As part of the process of "prepping the battlefield," commanders may want to launch pre-emptive attacks on the adversary's cybercapabilities in order to make sure their data networks do not get interrupted. Marine Lt. Gen. Richard Mills, in a rare acknowledgment that the military engages in offensive cyber operations, discussed just such a situation during a military conference in August 2012. "I can tell you that as a commander in Afghanistan in the year 2010, I was able to use my cyber operations against my adversary with great impact," Mills declared. "I was able to get inside his nets, infect his command and control, and in fact defend myself against his almost constant incursions to get inside my wire." Another reference to the military's use of cyberattacks as part of a traditional combat operation came in 2009, during a presentation at the Brookings Institution by Air Force Gen. Norton Schwartz. Now retired, Schwartz at the time was serving as Air Force chief of staff. He told his audience that his airmen were prepared to carry out cyberattacks on another country's radar and missile installations before launching airstrikes against that country. "Traditionally, we take down integrated air defenses via kinetic [physical] means," Schwartz said. "But if it were possible to interrupt radar systems or surface-to-air missile systems via cyber, that would be another very powerful tool in our tool kit." Schwartz hinted that the Air Force already had that capability, and in the nearly four years since he gave that speech, such a capability has certainly matured. Cyberattacks, however, are also being used independently of traditional or kinetic operations, according to Jason Healey, a former Air Force officer who now directs the Cyber Statecraft Initiative at the Atlantic Council. "It might happen that we will use them as an adjunct to kinetic," Healey says, "but it's quite clear that we're using [cyber] quite a bit more freely." The best example of an offensive cyberattack independent of a kinetic operation would be Stuxnet, the cyberweapon secretly used to damage nuclear installations in Iran. A U.S. official has privately confirmed to NPR what the New York Times reported last summer — that the United States had a role in developing Stuxnet. Because the operation has been shrouded in secrecy, however, there has been no public discussion about the pros and cons of using a cyberweapon in the way Stuxnet was used. Among the top concerns is that other countries, seeing Stuxnet apparently used by the United States and Israel, might conclude that they would also be justified in carrying out a cyberattack. The British author Misha Glenny, writing in the Financial Times, argued that the deployment of Stuxnet may be seen "as a starting gun; countries around the world can now argue that it is legitimate to use malware pre-emptively against their enemies." Another concern is that the malicious software code in Stuxnet, instructing computers to order Iranian centrifuges to spin out of control, could be modified and used against U.S. infrastructure assets. "Now that technology is out there," cautions Michigan Rep. Mike Rogers, the Republican chairman of the House Permanent Select Committee on Intelligence. "People are taking a look at it. We are just a few lines of code away from someone else getting closer to a very sophisticated piece of malware that they either wittingly or unwittingly unleash across the world [and cause] huge, huge damage." The absence of debate over the pros and cons of using cyberweapons is in sharp contrast to the discussion of nuclear weapons. The United States has adopted a "declaratory policy" regarding why it has nuclear weapons and when it would be justified to use them. There is nothing comparable for the cyberweapon arsenal. Rep. Rogers says such gaps in military doctrine and strategy indicate that developments on the cyberwar front are getting ahead of U.S. thinking about cyberwar. "The capabilities, I think, are keeping pace with technology," Rogers said in an interview with NPR. "It's the policy that I worry about. We have not fully rounded out what our [cyber] policies are." The advantages of using cyberweapons are clear. They are more precise than bombs or missiles, and because they damage data rather than physical installations, they are far less likely to hurt innocent civilians. But they are new weapons, and critics say their use should be given careful consideration. "If we are allowing ourselves to go on the offense without thinking about it, we're likely to militarize cyberspace," says the Atlantic Council's Jason Healey. "We will end up with a cyberspace where everyone is attacking everyone else. I don't believe we need to go on the offense just yet. The downside is higher than the government acknowledges."

#### **Clarity in the congressional language about what constitutes an act of war is key to reign in escalation of cyber conflict**

Rosenzweig 9,

(Paul, founder of Reid Branch Consulting, specializing in homeland security, senior advisor to the Chertoff Group, Carnegie Fellow at Northwestern, professor at National Defense University, Editorial board at the Journal of National Security Law & Policy, deputy assistant secretary for policy at the US Department of Homeland Security, "National Security Threatsin Cyberspace" merican Bar Association Standing Committee on Law andNational Security And National Strategy Forum, September 2009, [www.utexas.edu/law/journals/tlr/sources/Issue%2088.7/Jensen/fn137.Rosenwieg.pdf](http://www.utexas.edu/law/journals/tlr/sources/Issue%2088.7/Jensen/fn137.Rosenwieg.pdf))

Offensive dominance creates a great risk of cyber arms races. State and non-state actors are likely to view the prevalence of offensive cyber threats as a legitimate rationale for bolstering their own capabilities, both defensive and offensive, thus fueling an action-reaction dynamic of iterative arming. Experts believe that at least 20 nations are engaged in a cyber arms competition and possess the type of advanced capabilities needed to wage cyber war against the United States.121 As Michael Nacht, Former Assistant Secretary of Defense for Global Strategic Affairs, told us, “An arms race is already going on in cyberspace and it is very intense.”122 Conflict in cyberspace is uniquely predisposed to escalation given uncertainties about what constitutes an act of war and the growing number of state and non-state actors seeking offensive capabilities. Actors are more likely to misperceive or miscalculate actions in cyberspace, where there is no widely understood strategic language for signaling intent, capability and resolve.123 Uncertainty will encourage states to prepare for worst-case contingencies, a condition that could fuel escalation. Furthermore, “false flag” attacks, in which an actor purposefully makes an attack look like it came from a third party, could also ignite a conflict.124

#### Cyber conflicts lead to great power war – guarantees nuclear retaliation

Lawson ‘9 (Sean, Assistant professor in the Department of Communication at the University of Utah, Cross-Domain Response to Cyber Attacks and the Threat of Conflict, p. <http://www.seanlawson.net/?p=477>, June 13, 2009)

At a time when it seems impossible to avoid the seemingly growing hysteria over the threat of cyber war,[1] network security expert Marcus Ranum delivered a refreshing talk recently, “The Problem with Cyber War,” that took a critical look at a number of the assumptions underlying contemporary cybersecurity discourse in the United States.  He addressed one issue in partiuclar that I would like to riff on here, the issue of conflict escalation–i.e. the possibility that offensive use of cyber attacks could escalate to the use of physical force.  As I will show, his concerns are entirely legitimate as current U.S. military cyber doctrine assumes the possibility of what I call “cross-domain responses” to cyberattacks. Backing Your Adversary (Mentally) into a Corner Based on the premise that completely blinding a potential adversary is a good indicator to that adversary that an attack is iminent, Ranum has argued that “The best thing that you could possibly do if you want to start World War III is launch a cyber attack. [...] When people talk about cyber war like it’s a practical thing, what they’re really doing is messing with the OK button for starting World War III.  We need to get them to sit the f-k down and shut the f-k up.” [2] He is making a point similar to one that I have made in the past: Taking away an adversary’s ability to make rational decisions could backfire. [3]  For example, Gregory Witol cautions that “attacking the decision maker’s ability to perform rational calculations may cause more problems than it hopes to resolveÃ¢â‚¬Â¦ Removing the capacity for rational action may result in completely unforeseen consequences, including longer and bloodier battles than may otherwise have been.” [4] Ã¯Â»Â¿Cross-Domain Response So, from a theoretical standpoint, I think his concerns are well founded.  But the current state of U.S. policy may be cause for even greater concern.  It’s not just worrisome that a hypothetical blinding attack via cyberspace could send a signal of imminent attack and therefore trigger an irrational response from the adversary.  What is also cause for concern is that current U.S. policy indicates that “kinetic attacks” (i.e. physical use of force) are seen as potentially legitimate responses to cyber attacks.  Most worrisome is that current U.S. policy implies that a nuclear response is possible, something that policy makers have not denied in recent press reports. The reason, in part, is that the U.S. defense community has increasingly come to see cyberspace as a “domain of warfare” equivalent to air, land, sea, and space.  The definition of cyberspace as its own domain of warfare helps in its own right to blur the online/offline, physical-space/cyberspace boundary.  But thinking logically about the potential consequences of this framing leads to some disconcerting conclusions. If cyberspace is a domain of warfare, then it becomes possible to define “cyber attacks” (whatever those may be said to entail) as acts of war.  But what happens if the U.S. is attacked in any of the other domains?  It retaliates.  But it usually does not respond only within the domain in which it was attacked.  Rather, responses are typically “cross-domain responses”–i.e. a massive bombing on U.S. soil or vital U.S. interests abroad (e.g. think 9/11 or Pearl Harbor) might lead to air strikes against the attacker.  Even more likely given a U.S. military “way of warfare” that emphasizes multidimensional, “joint” operations is a massive conventional (i.e. non-nuclear) response against the attacker in all domains (air, land, sea, space), simultaneously. The possibility of “kinetic action” in response to cyber attack, or as part of offensive U.S. cyber operations, is part of the current (2006) National Military Strategy for Cyberspace Operations [5]: (U) Kinetic Actions. DOD will conduct kinetic missions to preserve freedom of action and strategic advantage in cyberspace. Kinetic actions can be either offensive or defensive and used in conjunction with other mission areas to achieve optimal military effects. Of course, the possibility that a cyber attack on the U.S. could lead to a U.S. nuclear reply constitutes possibly the ultimate in “cross-domain response.”  And while this may seem far fetched, it has not been ruled out by U.S. defense policy makers and is, in fact, implied in current U.S. defense policy documents.  From the National Military Strategy of the United States (2004): “The term WMD/E relates to a broad range of adversary capabilities that pose potentially devastating impacts.  WMD/E includes chemical, biological, radiological, nuclear, and enhanced high explosive weapons as well as other, more asymmetrical ‘weapons’.   They may rely more on disruptive impact than destructive kinetic effects.  For example, cyber attacks on US commercial information systems or attacks against transportation networks may have a greater economic or psychological effect than a relatively small release of a lethal agent.” [6] The authors of a 2009 National Academies of Science report on cyberwarfare respond to this by saying, “Coupled with the declaratory policy on nuclear weapons described earlier, this statement implies that the United States will regard certain kinds of cyberattacks against the United States as being in the same category as nuclear, biological, and chemical weapons, and thus that a nuclear response to certain kinds of cyberattacks (namely, cyberattacks with devastating impacts) may be possible.  It also sets a relevant scale–a cyberattack that has an impact larger than that associated with a relatively small release of a lethal agent is regarded with the same or greater seriousness.” [7]

**That causes nuclear miscalculation with Russia and China**

**Clark and Andreasen 13** (Richard A. Clarke, the chairman of Good Harbor Security Risk Management, was special adviser to the president for cybersecurity in the George W. Bush administration. Steve Andreasen, a consultant to the Nuclear Threat Initiative, was the National Security Council’s staff director for defense policy and arms control from 1993 to 2001, “Cyberwar’s threat does not justify a new policy of nuclear deterrence” June 14, 2013, <http://articles.washingtonpost.com/2013-06-14/opinions/39977598_1_nuclear-weapons-cyber-attack-cyberattacks>, KB)

President Obama is expected to unveil a new nuclear policy initiative this week in Berlin. Whether he can make good on his first-term commitments to end outdated Cold War nuclear policies may depend on a firm presidential directive to the Pentagon rejecting any new missions for nuclear weapons — in particular, their use in response to cyberattacks.¶ The Pentagon’s Defense Science Board concluded this year that **China and Russia could develop capabilities to launch an “existential cyber attack” against the United States** — that is, **an attack causing sufficient damage that our government would lose control of the country.** “**While the manifestation of a nuclear and cyber attack are** very **different**,” the board concluded, “in the end, **the existential impact to the United States is the same.”**¶ Because it will be impossible to fully defend our systems against existential cyberthreats, the board argued, the United States must be prepared to threaten the use of nuclear weapons to deter cyberattacks. In other words: I’ll see your cyberwar and raise you a nuclear response.¶ Some would argue that Obama made clear in his 2010 Nuclear Posture Reviewthat the United States has adopted the objective of making deterrence of nuclear attacks the “sole purpose” of our nuclear weapons. Well, the board effectively reviewed the fine print and concluded that the Nuclear Posture Review was “essentially silent” on the relationship between U.S. nuclear weapons and cyberthreats, so connecting the two “is not precluded in the stated policy.”¶ As the board noted, cyberattacks can occur very quickly and without warning, requiring rapid decision-making by those responsible for protecting our country. **Integrating the nuclear threat into the equation means making clear to any potential adversary that the United States** is prepared to use nuclear weapons **very early in response to a major cyberattack — and is maintaining nuclear forces on “prompt launch” status to do so.**¶ **Russia and China would** certainly take note — and presumably **follow suit**. Moreover, **if the United States, Russia and China adopted policies threatening an early nuclear response to cyber­attacks, more countries would surely take the same approach.**¶ It’s hard to see how this cyber-nuclear action-reaction dynamic would improve U.S. or global security. It’s more likely to lead to a new focus by Pentagon planners on generating an expanding list of cyber-related targets and the operational deployment of nuclear forces to strike those targets in minutes.¶ Against that backdrop, maintaining momentum toward reducing the role of nuclear weapons in the United States’ national security strategy (and that of other nations) — a general policy course pursued by the past five presidents — would become far more difficult. **Further reductions in nuclear forces and changes in “hair-trigger” postures, designed to lessen the risk of an accidental or unauthorized nuclear launch, would** also probably **stall**.¶ Fortunately, Obama has both the authority and the opportunity to make clear that he meant what he said when he laid out his nuclear policy in Prague in 2009. For decades, presidential decision directives have made clear the purpose of nuclear weapons in U.S. national security strategy and provided broad guidance for military planners who prepare the operations and targeting plans for our nuclear forces. An update to existing presidential guidance is one of the homework items tasked by the 2010 Nuclear Posture Review.¶ Cyberthreats are very real, and **there is** much we ne**ed to do to defend our military and critical civilian infrastructure against** what former defense secretary Leon E. Panetta referred to as **a “cyber Pearl Harbor”** — including enhancing the ability to take action, when directed by the president, against those who would attack us. We also need more diplomacy such as that practiced by Obama with his Chinese counterpart, Xi Jinping, at their recent summit. Multinational cooperation centers could ultimately lead to shared approaches to cybersecurity, including agreements related to limiting cyberwar.

**Even absent US first strike, presidential discretion causes Russia and China to use nuclear first strike**

**Rothschild 13**, Matthew, the editor of The Progressive magazine, “The Dangers of Obama’s Cyber War Power Grab,” February 4th, http://progressive.org/dangers-of-obama-cyber-war-power-grab

According to The New York Times, the Obama Administration has concluded that the President has the authority to launch preemptive cyberattacks. This is a very dangerous**,** and very undemocratic power grab**.** There are no checks or balances when the President, alone, decides when to engage in an act of war. And this new aggressive stance will lead to a cyber arms race. The United States has evidently already used cyber weapons against Iran, and so many other countries will assume that cyber warfare is an acceptable tool and will try to use it themselves. Most troubling, U.S. cybersupremacy—and that is Pentagon doctrine—will also raise fears among nuclear powers like Russia, China, and North Korea that the United States may use a cyberattack as the opening move in a nuclear attack. For if the United States can knock out the command and control structure of an enemy’s nuclear arsenal, it can then launch an all-out nuclear attack on that enemy with impunity. This would make such nuclear powers more ready to launch their nuclear weapons preemptively for fear that they would be rendered useless. So we’ve just moved a little closer to midnight. Now, I don’t think Obama would use cyberwafare as a first strike in a nuclear war. But our adversaries may not be so sure, either about Obama or his successors. They, too, worry about the temptations of a President.

**US-Russia cyber conflict escalates**

Cimbala 12, Stephen J, Professor of Political Science at Penn State, “Chasing its Tail” 2012 www.au.af.mil/au/ssq/2012/summer/cimbala.pdf

Related to this possibility, Russia’s war against Georgia in August 2008 demonstrated how cyber war and information operations might be used in support of conventional military operations. The Russian cyber campaign reportedly attacked some 38 Georgian and Western websites upon the outbreak of war, including ranking Georgian government oices and the US and British embassies in Georgia, and appeared to be centrally directed and coordinated with the tempo of force operations. 26 Instead of a single integrated operational plan (SIOP), however lexible, for ighting a nuclear war if deterrence failed, planners would have to devise a matrix of plans linking information strike with kinetic options. How complicated this might be is probably beyond the power of mere mortals to demonstrate with any proiciency—much is speculative as to the two-way complexity of combined cyber and nuclear or conventional kinetic attacks. On the other hand, analysts and planners must do what they can in the face of questions and demands for performance that will not go away. A simpliied approach to one aspect of a cyber-soaked SIOP might be illustrated as follows. Let us assume that both the United States and Russia were required to carry out second-strike retaliation after having absorbed both cyber and kinetic first strikes. To measure the impact of such strikes, we estimate that the cyber component directly or indirectly neutralizes as many surviving and retaliating weapons as does the kinetic portion. The second-strike surviving forces would therefore be in a position equivalent to that of a third striker in a series of exchanges without information weapons. In effect, they would be fighting World War III-b. he additive efects of both cyber and kinetic strikes are summarized in igures 5 and 6 repre­ senting the 1,000- and 500-weapon prewar deployment limit (without defenses), respectively. Figures 5 and 6 show that, in a hypothetical but not necessarily unrealistic exercise of cyber-kinetic nuclear strike plans, the United States and Russia could still retain sufficient numbers of weapons to create historically un­ precedented and socially unacceptable damage in retaliation. Cyber attacks on command-control, communications, and warning systems might lead to ragged retaliations and strikes more dependent upon the most survivable launch platforms such as submarines and mobile missiles. Alternatively, two expectations about such a scenario would be mistaken. First, information operations cannot make any nuclear war between states with large arsenals into a surgical operation or an exercise in “soft” power. Second, a state’s cyber and kinetic strategies need to be carefully coordinated as to their political and military objectives, not only up to the brink of war but even beyond that threshold. Otherwise, the objectives of escalation control and conflict termination will be impossible to realize for either state when its op­ posite number is brain dead as well as partly but not completely disarmed. Faced with exigent threats, states with cyber capabilities will be tempted to employ them to good effect. For example, imagine a replay of the Cuban missile crisis between a future Russia and the United States, with Rus­ sia having deployed nuclear-capable missiles and/or warheads into South Ossetia. Or, to lip the example, hypothesize a NATO missile defense installation deployed to protect Tbilisi or Kiev, supported by short- and medium-range ballistic missiles as a trip wire. One can expect that cyber operations of the information-technical type (attacking enemy systems and networks) as well as the information-psychological variety (inluenc­ ing public opinion among foreign and domestic audiences, including elites and general publics) will commend themselves to peacetime and crisis political leaders and their military advisors.

**Extinction**

Corcoran 9 (PhD, Senior Fellow @ Global Security, Frmr. Strategic Analyst at the US Army War College where he chaired studies for the Office of the Deputy Chief of Operations and member of the National Advisory Board for the Alsos Digital Library for Nuclear Issues, we win the qualification game, 4/21, http://sitrep.globalsecurity.org/articles/090421301-strategic-nuclear-targets.htm)

That brings us to Russia, our former main adversary, now a competitive partner and still a potential future adversary, particularly as relations have gradually soured in recent years. Russia is the only other nation with a formidable arsenal of some three thousand strategic weapons. Our opposing arsenals were built up in the period when Mutually Assured Destruction (MAD) was the underlying strategic concept -- each side deterred from striking the other by the prospect of assured retaliatory destruction. The situation became even madder as both sides worked to develop a capability to destroy the other's strike force with a crippling first strike. This resulted in further large increases in the sizes of the arsenals, as well as early warning systems and hair-trigger launch-on-warning alert procedures. The final result was an overall system in which each side could destroy the other in a matter of minutes. And it also raised another chilling specter, Nuclear Winter, in which the atmospheric dust raised from a major nuclear exchange would block sunlight for an extended period and essentially destroy human civilization globally. The collapse of the Soviet Union collapsed this threat, but did not eliminate it. US and Russian nuclear forces remained frozen in adversarial positions. The May 2002 Moscow Treaty began to address this legacy and is leading to a reduction in strategic nuclear forces down to levels of about two thousand on each side by 2012. These levels are still sufficient to destroy not only both nations but also human civilization. It is hard to even construct scenarios where the use of even a few strategic nuclear weapons does not risk a total escalation. Strikes on Russian warning facilities or strike forces would almost certainly bring a wave of retaliatory strikes. Strikes on hardened command centers would be of questionable effectiveness and also risk total escalation. In addition, successful elimination of Russian leaders could greatly complicate any efforts to stop escalation short of a total nuclear exchange.

**China will cyberstrike in space**

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

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

**That causes extinction**

**Mitchell, et al 01** -Associate Professor of Communication and Director of Debate at the University of Pittsburgh (Dr. Gordon, ISIS Briefing on Ballistic Missile Defence, “Missile Defence:  Trans-Atlantic Diplomacy at a Crossroads”, No. 6 July, <http://www.isisuk.demon.co.uk/0811/isis/uk/bmd/no6.html>)

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

**Robust norms about the use of force prevent conflict escalation among great powers**

John Vasquez 9, Thomas B. Mackie Scholar of International Relations and Professor of Political Science at the University of Illinois at Urbana-Champaign, PhD in Poli Sci from Syracuse University, “Peace,” Chapter 8 in The War Puzzle Revisited, p 298-299, google books

Wallensteen’s examination of the characteristics of particularist periods provides significant additional evidence that the steps-to-war analysis is on the right track. Realist practices are associated with war, and peaceful systems are associated with an emphasis on other practices. Peaceful systems are exemplified by the use of practices like buffer states, compensation, and concerts of power that bring major states together to form a network of institutions that provide governance for the system. The creation of rules of the game that can handle certain kinds of issues – territorial and ideological questions – and/or keep them off the agenda seems to be a crucial variable in producing peace.¶ Additional evidence on the import of rules and norms is provided in a series of studies by Kegley and Raymond (1982, 1984, 1986, 1990) that are operationally more precise than Wallensteen’s (1984) analysis. Kegley and Raymond provide evidence that when states accept norms, the incidence of war and military confrontation is reduced. They find that peace is associated with periods in which alliance norms are considered binding and the unilateral abrogation of commitments and treaties illegitimate. The rules imposed by the global political culture in these periods result in fewer militarized disputes and wars between major states. In addition, the wars that occur are kept at lower levels of severity, magnitude, and duration (i.e. they are limited wars).¶ Kegley and Raymond attempt to measure the extent to which global cultural norms restrain major states by looking at whether international law and commentary on it sees treaties and alliances as binding. They note that there have been two traditions in international law – pacta sunt servanda, which maintains that agreements are binding, and clausa rebus sic stantibus, which says that treaties are signed “as matters stand” and that any change in circumstances since the treaty was signed permits a party to withdraw unilaterally. One of the advantages the Kegley-Raymond studies have over Wallensteen (1984) is that they are able to develop reliable measures of the extent to which in any given half-decade that tradition in international law emphasizes the rebus or pacta sunt servanda tradition. This indicator is important not only because it focuses in on the question of unilateral actions, but because it can serve as an indicator of how well the peace system is working. The pacta sunt servanda tradition implies a more constraining political system and robust institutional context which should provide an alternative to war.¶ Kegley and Raymond (1982: 586) find that in half-decades (from 1820 to 1914) when treaties are considered non-binding (rebus), wars between major states occur in every half-decade (100 percent), but when treaties are considered binding (pacta sunt servanda), wars between major states occur in only 50 percent of the half-decades. The Cramer’s V for this relationship is .66. When the sample is expanded to include all states in the central system, Cramer’s V is 0.44, indicating that global norms have more impact on preventing war between major states. Nevertheless, among central system states between 1820 and 1939, war occurred in 93 percent of the half-decades where the rebus tradition dominated and in only 60 percent of the half-decades where the pacta sunt sevanda tradition dominated.¶ In a subsequent analysis of militarized disputes from 1820 to 1914, Kegley and Raymond (1984: 207-11) find that there is a negative relationship between binding norms and the frequency and scope of disputes short of war. In periods when the global culture accepts the pacta sunt servanda tradition as the norm, the number of military disputes goes down and the number of major states involved in a dispute decreases. Although the relationship is of moderate strength, it is not eliminated by other variables, namely alliance flexibility. As Kegley and Raymond (1984: 213) point out, this means “that in periods when the opportunistic renunciation of commitments” is condoned, militarized disputes are more likely to occur and to spread. The finding that norms can reduce the frequency and scope of disputes is significant evidence that rules can permit actors to successfully control and manage disputes so that they are not contagious and they do not escalate to war. These findings are consistent with Wallensteen’s (1984) and suggest that one of the ways rules help prevent war is by reducing, limiting, and managing disputes short of war.

#### Clarity in the legal language about the WPR is key – only solid definitions prevent other countries from justifying cyber militarization

**Huston 11** <Warner. “we need rules for cyberwarfare before a president steals that power, too” October 10, 2011. http://www.conservativecrusader.com/articles/we-need-rules-for-cyberwarfare-before-a-president-steals-that-power-too>

A recent New York Times article revealed that the Pentagon briefly considered engaging in cyberwarfare at the outset of the actions in Libya, but decided against it for a variety of reasons. This reminds us all that as a nation we really need to discuss the use of cyberwarfare. The first question asked must be: should a president be able to simply order such an attack on his own hook?¶ The Times noted that one of the concerns about the use of cyberwarfare is how it would be justified under the War Powers Resolution of 1973?¶ One unresolved concern was whether ordering a cyberattack on Libya might create domestic legal restrictions on war-making by the executive branch without Congressional permission. One question was whether the War Powers Resolution -- which requires the executive to formally report to lawmakers when it has introduced forces into “hostilities” and sets a 60-day limit on such deployments if Congress does not authorize them to continue -- would be required for an attack purely in cyberspace.¶ One would think that the answer to this would be somewhat obvious -- though nothing seems obvious in Constitution-based discussions, sadly.¶ We know that the Founders vested in Congress the power to declare war not in the president. They wanted to avoid a repeat of the historical outrage of a King's untrammeled powers to declare wars without the consent of the people and their duly elected representatives.¶ Presidents have had certain restrictions for war-making ever since because the founders wanted to make sure that war was something duly considered not easily engaged.¶ This should hold as much for use of computer-based warfare as it does for any other type of military attack. Currently computer-based war, or cyberwarfare, presents a new field of military application and we have no legal precedent to govern its use.¶ Despite the last 200 years of presidents slowly stealing away power from Congress to initiate military actions, we should really think long and hard about allowing any president to unleash cyberwarfare at his discretion. In fact, we should set a precedent immediately to prevent any president from using cyberwarfare without the consent of Congress.¶ Why? Because cyberwarfare is a far, far different animal than use of conventional military forces and indiscriminate use of it would endanger our way of life in harsh and immediate terms if used against us. For that reason, we should be very careful when we use it against others. We should have solid legal definitions behind its use so as not to give enemies the excuse to resort to it quickly themselves.¶ You see, cyberwarfare is a relatively cheap war power, easier to implement, and requires far fewer in personnel and facilities than launching an invasion using conventional military forces. This is not to say that cyberwarfare is easy -- far from it. But it is cheaper and easier than deploying regular military forces.¶ So, we should casually resort to cyberwarfare no more easily than we would to using conventional forces. But if we do not set down specific and binding rules for its use we risk giving this power over to a president which could cause less considered use of this sort of warfare. That in turn, would give enemies an excuse to do the same. Further, remember that setting legally binding reasons for warfare is a long and proud American tradition, one that legitimizes our nation and one we should not casually toss aside simply under the assumption that enemies will not be as thoughtful as we.¶ We should lead the world in considered use of cyberwarfare and we should do so now. Any of those that felt we illicitly launched into the war on terror should no less worry about indiscriminate use of cyberwarfare. But illicit use or no, we should be deadly certain of what powers our president can have, when and how he can use them, and where the line should be drawn, even in cyberspace.

#### Perception is key – failure to signal restraint erodes US credibility and causes conflict escalation

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.

# WPR Credibility - Coast

#### Application of the War Powers Resolution is key to its credibility – prevents executive adventurism

Dycus ’10 (Stephen Dycus, 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, National Security Law Section, Association of American Law Schools. Professor Dycus 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, “Congress’s Role in Cyber Warfare”, Pg 157, September 29, 2010)

Before an attack can be launched, of course, Congress must have supplied the President with personnel and weapons. Moreover, Congress may regulate the President’s actions as Commander in Chief, except when the nation comes under sudden attack or the President exercises her tactical powers (and perhaps even then). In the Supreme Court’s 1800 decision in Bas v. Tingy, Justice Paterson, one of the Framers, echoed the other Justices in declaring that “[a]s far as congress authorized and tolerated the war on our part, so far may we proceed in hostile operations.” Four years later, in Little v. Barreme, the Court reiterated that the President must not exceed limits set forth in Congress’s authorization of hostilities. Since then, no court has ruled otherwise. In the intervening two centuries, Congress has adopted a number of measures to control the initiation or conduct of warfare. At the end of the Vietnam War, for example, Congress passed the War Powers Resolution (WPR), which requires the President to report to Congress within 48 hours the introduction of U.S. armed forces into hostilities or imminent hostilities, and to withdraw those forces within 60 days if Congress does not expressly 18 approve of their continued deployment. Lambasted by some as an unconstitutional encroachment on presidential powers, the WPR has been followed (or at least lip service has been paid to it) by each President since the Nixon administration, and Congress has repeatedly referred to the 20 WPR approvingly in subsequent legislation. If Congress now fails to enact guidelines for cyber warfare, it might be perceived as inviting “measures on independent presidential responsibility.” Chief Justice Marshall suggested in Little v. Barreme that if Congress had remained silent, the President might have been free to conduct the Quasi-War with France as he saw fit. But the national interest in electronic warfare, just as in that early maritime conflict, is so great that the planning and conduct of such a war should not be left entirely to the Executive. And because a cyber war might be fought under circumstances that make it impossible for Congress to play a meaningful contemporaneous role, Congress ought to get out in front of events now in order to be able to participate in the formulation of national policy.

#### Cyber operations are key – not applying the WPR allows Obama to continue to avoid congressional checks by using an overly restrictive definition of hostilities

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.

Letting Stuxnet and PPD20 by with a free pass greenlights future unchecked executive lashout

Walker 8/2/13 (Richard, Pen Name for New York News Producer, American free Press, “OBAMA EXPANDS WAR POWERS; CAN UNLEASH CYBERWAR ANY TIME <http://americanfreepress.net/?p=11966#sthash.GqeI03l8.dpuf>)

The very moment United States President Barack Obama authorized the “dropping” of an electronic bomb on Iran’s nuclear industry he crossed a line into a new kind of warfare that could have global consequences today and far into the future. The weapon used against Iran was built with the cooperation of Israel and was named Stuxnet. It was a “worm” that infected the computers running Iran’s nuclear industry. German systems control expert, Ralph Langer, who told the world about Stuxnet, remarked Stuxnet represented a dangerous capability and that its code could be used by hackers and others. In other words, Obama had unleashed a weapon that could be re-engineered by anyone to attack computer networks controlling American infrastructure.

Perhaps the most significant aspect of the Stuxnet attack was it demonstrated how Obama had given to himself new powers to launch a cyberwar against any country without Congressional approval. Unlike conventional war in which soldiers are sent to the front and bombs are dropped from the skies, cyberweapons silently and stealthily attack information systems, as well as financial and power centers. We do not know how many times Obama has used his new Cyber Command unit to attack nations other than Iran.

Obama’s Presidential Policy Directive 20, known as PPD 20, which he signed in October 2012, was a stark example of a power grab to accord to him special powers to launch a cyber war at a moment of his choosing. The Guardian newspaper, which first revealed the existence of the directive, claimed it sought a larger target list for cyber attacks and contemplated the use of cyber weapons within the U.S. if the president gave the green light and only in an emergency. But what kind of emergency remains unclear, as does the list of nations he might target in the future.

#### WPR credibility creates the perception of restrained force that lends legitimacy to US military force and international coalitions

Frye, 2002 Alton, President Senior Fellow Emeritus, “Applying the War Powers Resolution to the War on Terrorism”, April 17, <http://www.cfr.org/terrorism/applying-war-powers-resolution-war-terrorism/p4514>

4. CONSENSUS IS ESSENTIAL TO NATIONAL COHESION The case for active, continuing congressional engagement on the many issues of high policy presented by an open-ended campaign against terrorism does not rest on an instinct for institutional self-aggrandizement. It is grounded in the critical need to forge and maintain America’s social cohesion as a nation caught up in war. War, especially prolonged war, always poses the risk of depleting that cohesion, so vital to domestic harmony and international effectiveness. Members of Congress should also realize how essential their involvement is to the morale and cohesion of the military men and women sent to do violence on our behalf. One of our most distinguished and thoughtful military leaders, former Army Chief of Staff, General Edward Meyer, emphasized that point some months ago. In a letter to Congressman Thomas Campbell, who was then seeking a definitive judicial ruling on the constitutional balance of war powers, General Meyer wrote, “I believe it is essential that when American servicemen [servicepeople] are sent into combat that they have the support of their fellow Americans. The War Powers Act causes the people’s representatives (the Congress) to take a position, and not leave the troops dangling on threads of definition and interpretation.” The parallel, policy-centered procedures outlined here would serve that same need. Congress’s stand on how our nation uses the mighty arsenal at its disposal also bears crucially on America’s standing in the world. Even among our closest allies, American power elicits mixed emotions: awe and fear, respect and anxiety. That should surprise no one. Military and economic capabilities of the magnitude America possesses cannot fail to cause alarm in other countries, however benign our intentions. That alarm is heightened to the degree that American force appears to be too easily deployed. In the eyes of others, no less than of our own citizens, American military action may be seen as most legitimate when it is demonstrably subject to democratic governance. This insight is akin to Justice Jackson’s memorable formulation that the President’s power is at its maximum only when he acts “pursuant to an explicit or implied authorization of Congress.” Marshaling international coalitions to wage the war on terrorism will depend importantly on giving our allies confidence that American power is guided and restrained by a disciplined relationship between Congress and President. Absent attentive, persistent congressional involvement, public diplomacy in the war on terrorism could lose much of the credibility that arises from the perception of America as a model of representative government. There is thus an enduring necessity to balance executive potency in military endeavors with the legislative review that provides democratic legitimacy. The challenge is not to enchain the presidency but to harness both branches to common purpose. On that insight the War Powers Resolution was founded, and in that insight may be found the germ of other innovations to guarantee that Congress will play its proper constitutional role in the war on terrorism.

**That prevents European conflict, destabilizing transition wars, Asian war, and great power conflict**

Brooks, Ikenberry, and Wohlforth ’13 (Stephen, Associate Professor of Government at Dartmouth College, John Ikenberry is the Albert G. Milbank Professor of Politics and International Affairs at Princeton University in the Department of Politics and the Woodrow Wilson School of Public and International Affairs, William C. Wohlforth is the Daniel Webster Professor in the Department of Government at Dartmouth College “Don’t Come Home America: The Case Against Retrenchment,” International Security, Vol. 37, No. 3 (Winter 2012/13), pp. 7–51)

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

**Hegemonic strategy inevitable – the aff is key to one that promotes alliances instead of war**

**Calleo 10**, Director – European Studies Program and Professor @ SAIS, (David P, “American Decline Revisited,” *Survival*, 52:4, 215 – 227)

The history of the past two decades suggests that adjusting to a plural world is not easy for the United States. As its economic strength is increasingly challenged by relative decline, it clings all the more to its peerless military prowess. As the wars in Iraq and Afghanistan have shown, that overwhelming military power, evolved over the Cold War, is less and less effective. In many respects, America's geopolitical imagination seems frozen in the posture of the Cold War. The lingering pretension to be the dominant power everywhere has encouraged the United States to hazard two unpromising land wars, plus a diffuse and interminable struggle against 'terrorism'. Paying for these wars and the pretensions behind them confirms the United States in a new version of Cold War finance. Once more, unmanageable fiscal problems poison the currency, an old pathology that firmly reinstates the nation on its path to decline. It was the hegemonic Cold War role, after all, that put the United States so out of balance with the rest of the world economy. In its hegemonic Cold War position, the United States found it necessary to run very large deficits and was able to finance them simply by creating and exporting more and more dollars. The consequence is today's restless mass of accumulated global money. Hence, whereas the value of all global financial assets in 1980 was just over 100% of global output, by 2008, even after the worst of the financial implosion, that figure had exploded to just under 300%.25 Much of this is no doubt tied up in the massive but relatively inert holdings of the Chinese and Japanese. But thanks to today's instantaneous electronic transfers, huge sums can be marshalled and deployed on very short notice. It is this excess of volatile money that arguably fuels the world's great recurring bubbles. It can create the semblance of vast real wealth for a time, but can also (with little notice) sow chaos in markets, wipe out savings and dry up credit for real investment. What constitutes a morbid overstretch in the American political economy thus ends up as a threat to the world economy in general. To lead itself and the world into a more secure future the United States must put aside its old, unmeasured geopolitical ambitions paid for by unlimited cheap credit. Instead, the United States needs a more balanced view of its role in history. But America's post-Soviet pundits have, unfortunately, proved more skilful at perpetuating outmoded dreams of past glory than at promoting the more modest visions appropriate to a plural future. One can always hope that newer generations of Americans will find it easier to adjust to pluralist reality. The last administration, however, was not very encouraging in this regard. III What about Barack Obama? So far, his economic policy has shown itself probably more intelligent and certainly more articulate than his predecessor's. His thinking is less hobbled by simple-minded doctrines. It accepts government's inescapable role in regulating markets and providing a durable framework for orderly governance and societal fellowship. To be sure, the Obama administration, following in the path of the Bush administration, has carried short-term counter-cyclical stimulation to a previously unimagined level. Perhaps so radical an expansion of credit is unavoidable under present circumstances. The administration is caught between the need to rebalance by scaling back and the fear that restraint applied now will trigger a severe depression. Obama's chief aide, Rahm Emanuel, is famous for observing: 'Rule one: Never allow a crisis to go to waste. They are opportunities to do big things.'26 So far, Obama's administration has made use of its crisis to promote an unprecedented expansion of welfare spending.27 Much of the spending is doubtless good in itself and certainly serves the administration's strong counter-cyclical purposes. But at some point the need to pass from expansion to stabilisation will presumably be inescapable. Budget cuts will have to be found somewhere, and demographic trends suggest that drastic reductions in civilian welfare spending are unlikely. Elementary prudence might suggest that today's financial crisis is an ideal occasion for America's long-overdue retreat from geopolitical overstretch, a time for bringing America's geopolitical pretensions into harmony with its diminishing foreign possibilities and expanding domestic needs. The opportunities for geopolitical saving appear significant. According to the Congressional Budget Office (CBO), current military plans will require an average military budget of $652bn (in 2010 dollars) each year through 2028. The estimate optimistically assumes only 30,000 troops will be engaged abroad after 2013. As the CBO observes, these projections exceed the peak budgets of the Reagan administration's military build-up of the mid-1980s (about $500bn annually in 2010 dollars). This presumes a military budget consuming 3.5% of GDP through 2020.28 Comparable figures for other nations are troubling: 2.28% for the United Kingdom, 2.35% for France, 2.41% for Russia and 1.36% for China.29 Thus, while the financial crisis has certainly made Americans fear for their economic future, it does not yet seem to have resulted in a more modest view of the country's place in the world, or a more prudent approach to military spending. Instead, an addiction to hegemonic status continues to blight the prospects for sound fiscal policy. Financing the inevitable deficits inexorably turns the dollar into an imperial instrument that threatens the world with inflation.

**The aff’s key – congressional silence makes court enforcement impossible**

**Corn 13**, Geoff, Presidential Research Professor of Law at South Texas College of Law in Houston, “Syria Insta-Symposium: Geoff Corn–The President, Congress, Syria: What If?” 9/07, http://opiniojuris.org/2013/09/07/syria-insta-symposium-geoff-corn-president-congress-syria/

Based on the President’s assertion that he is vested with authority to initiate an attack on Syria without congressional authorization, he might have initiated the attack based on this asserted inherent Article II power, without seeking authorization and with Congress never voting on a proposed AUMF. Had he done so, he would have been on relatively solid constitutional turf. Invoking Justice Jackson’s seminal Youngstown methodology for assessing the legality of exercises of executive power in relation to national security objectives, the absence of express congressional opposition following his overt assertion of inherent power and intent to initiate the attack would indicate congressional acquiescence at worst. The availability of existing funding for the operation would bolster his position, and if, as in the case of the air war against Serbia, Congress were to authorize supplemental funding, it would indicate implied congressional support. It is also important to bear in mind that initiating action without first seeking and in the absence of an up or down congressional vote on an authorization to do so would also provide a high degree of confidence that any judicial challenge by congressional opponents would fail to clear the legislative standing hurdle. With no vote to argue their role was “completely nullified” by the President’s action, such plaintiffs would be unable to satisfy the requirements of Raines v. Byrd. And, as Judge Green suggested in Dellums v. Bush, the failure to take an affirmative stand against the operation would undermine any assertion of a “constitutional loggerhead” between the two political branches, an ostensible predicate for establishing a ripe dispute. Opponents of unilateral presidential action could, of course, invoke the War Powers Resolution. According to this law, a President may order forces into hostilities only pursuant to a declaration of war, express statutory authorization, or an attack on the United States or its armed forces. The absence of express statutory authorization coupled with the undeniable fact that the action was not in response to an attack on the United States or its armed forces would therefore seem to prohibit presidential action even if Congress is silent. However, no President has ever accepted the constitutionality of this “exclusive list” of constitutional justifications for using force, and for good reason. The WPR essentially forbids presidents from relying on other evidence of congressional support for war making initiatives, such enactment of supplemental appropriations and implementing treaty obligations. It also dictates to Congress an exclusive method for manifesting support for hostilities (express authorization), a method that is inconsistent with both pre and post WPR congressional practice. But even if this express authorization requirement of the WPR is constitutional in theory, in reality it is of little value to legislators who oppose a presidential war making initiative unless they can also muster sufficient support to enact a statutory prohibition for such action. This is because the doctrines of legislative standing and ripeness have in large measure nullified the efficacy of this provision. Enforcement to stop a presidential war making initiative would require affirmative congressional action prohibiting the operation. If Congress is able to muster the will to take such affirmative action, the WPR becomes functionally superfluous, because an express statutory prohibition against an operation would provide an independent basis for challenging the President. In short, the consequence of the standing and ripeness doctrines have almost completely nullified the “prohibition by silence” objective of the WPR (with the possible narrow exception of a service-member lawsuit against complying with a deployment order, which would ostensibly overcome any ripeness barrier, and rely on the WPR itself to provide standing).

**Congress enforcing WPR restrictions is key – solves groupthink**

**Healy 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. Thanks to Jason Thelen of the Atlantic Council for his contributions, ”Cyber Confliict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain,” February

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. The War Powers Resolution 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.’ 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: [Any 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, 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 ¡s no detailed indication in Koh’s testimony of what weight ¡s to be accorded to each of the factors he enumerates, the overriding emphasis is on physical risk to US personnel. As Koh himself said, uwe ¡n 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.7 As 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.

**Congressional involvement is key to prevent mistakes – executive decisions are inevitably flawed**

Ahmad Chehab 12, Georgetown University Law Center, “RETRIEVING THE ROLE OF ACCOUNTABILITY IN THE TARGETED KILLINGS CONTEXT: A PROPOSAL FOR JUDICIAL REVIEW,” March 30 2012, available at https://docs.google.com/file/d/0B91bSAyxkYQWbktoTDRSWGJzNmc/edit?usp=sharing

The practical, pragmatic justification for the COAACC derives largely from considering social psychological findings regarding the skewed potential associated with limiting unchecked decision-making in a group of individuals. As an initial point, psychologists have long pointed out how individuals frequently fall prey to cognitive illusions that produce systematic errors in judgment.137 People simply do not make decisions by choosing the optimal outcome from available alternatives, but instead employ shortcuts (i.e., heuristics) for convenience.138 Cognitive biases like groupthink can hamper effective policy deliberations and formulations.139 Groupthink largely arises when a group of decision-makers seek conformity and agreement, thereby avoiding alternative points of view that are critical of the consensus position.140 This theory suggests that some groups—particularly those characterized by a strong leader, considerable internal cohesion, internal loyalty, overconfidence, and a shared world view or value system—suffer from a deterioration in their capacity to engage in critical analysis.141 Many factors can affect such judgment, including a lack of crucial information, insufficient timing for decision-making, poor judgment, pure luck, and/or unexpected actions by adversaries.142 Moreover, decision-makers inevitably tend to become influenced by irrelevant information,143 seek out data and assessments that confirm their beliefs and personal hypotheses notwithstanding contradictory evidence,144 and “[i]rrationally avoid choices that represent extremes when a decision involves a trade-off between two incommensurable values.”145 Self-serving biases can also hamper judgment given as it has been shown to induce well-intentioned people to rationalize virtually any behavior, judgment or action after the fact.146 The confirmation and overconfidence bias, both conceptually related to groupthink, also result in large part from neglecting to consider contradictory evidence coupled with an irrational persistence in pursuing ideological positions divorced from concern of alternative viewpoints.147¶ Professor Cass Sunstein has described situations in which groupthink produced poor results precisely because consensus resulted from the failure to consider alternative sources of information.148 The failures of past presidents to consider alternative sources of information, critically question risk assessments, ensure neutral-free ideological sentiment among those deliberating,149 and/or generally ensure properly deliberated national security policy has produced prominent and devastating blunders,150 including the Iraq War of 2003,151 the Bay of Pigs debacle in the 1960’s,152 and the controversial decision to wage war against Vietnam.153¶ Professor Sunstein also has described the related phenomenon of “group polarization,” which includes the tendency to push group members toward a “more extreme position.”154 Given that both groupthink and group polarization can lead to erroneous and ideologically tainted policy positions, the notion of giving the President unchecked authority in determining who is eligible for assassination can only serve to increase the likelihood for committing significant errors.155 The reality is that psychological mistakes, organizational ineptitude, lack of structural coherence and other associated deficiencies are inevitable features in Executive Branch decision-making.¶ D. THE NEED FOR ACCOUNTABILITY CHECKS¶ To check the vices of groupthink and shortcomings of human judgment, the psychology literature emphasizes a focus on accountability mechanisms in which a better reasoned decision-making process can flourish.156 By serving as a constraint on behavior, “accountability functions as a critical norm-enforcement mechanism—the social psychological link between individual decision makers on the one hand and social systems on the other.”157 Such institutional review can channel recognition for the need by government decision-makers to be more self-critical in policy targeted killing designations, more willing to consider alternative points of view, and more willing to anticipate possible objections.158 Findings have also shown that ex ante awareness can lead to more reasoned judgment while also preventing tendentious and ideological inclinations (and political motivations incentivized and exploited by popular hysteria and fear).159¶ Requiring accounting in a formalized way prior to engaging in a targeted killing—by providing, for example, in camera review, limited declassification of information, explaining threat assessments outside the immediate circle of policy advisors, and securing meaningful judicial review via a COAACC-like tribunal—can promote a more reliable and informed deliberation in the executive branch. With process-based judicial review, the COAACC could effectively reorient the decision to target individuals abroad by examining key procedural aspects—particularly assessing the reliability of the “terrorist” designation—and can further incentivize national security policy-makers to engage in more carefully reasoned choices and evaluate available alternatives than when subject to little to no review.

**Key to solve war**

Jervis, 4(Robert, political science and international politics professor at Columbia University and a consultant to the CIA, The Record, 7/14, lexis)

But was that indeed what happened? "Groupthink" - identified in the early 1970s by the late Yale psychologist Irving Janis - refers to a process by which conformity grows out of deliberations in small groups. It can indeed be quite powerful. The way Janis explained it, groupthink operates when individuals work closely together over a sustained period. It isn't merely that members of the group come to think alike but that they come to overvalue the harmonious functioning of the group. In their eagerness to reach consensus, they become inhibited from questioning established assumptions or from raising questions that might disturb their colleagues and friends. A vicious circle begins as the group feels good about itself because it has discovered the truth, and this truth is accepted by each person because it is believed by the others. In this way, a group of intelligent individuals can confidently arrive at conclusions that are wildly removed from reality. Most social scientists agree that groupthink has contributed to many disastrous decisions in business, families, and foreign policy. President Kennedy and his top advisers, for instance, fell into a groupthink trap, believing that the landings of the Cuban exiles at the Bay of Pigs in April 1961 might overthrow Fidel Castro. Intense face-to-face meetings among the president's top foreign policy planners formed strong bonds that no one wanted to loosen. In hindsight, their plans were so badly flawed that it is hard to understand how such world-wise leaders could have endorsed them. But apparently each individual grew confident because the others were - each was reassured because the group was functioning so well and without discord; no one felt the need, or had the nerve, to insist they consider the possibility that the group was on the totally wrong track.

Richard Nixon's Watergate cover-up was in part maintained by the same dynamic. To many outsiders even at the time, it was obvious that the only way for Nixon to survive was to air the full truth early on. But the Nixon White House was a small group, closed-mouthed and predisposed to keeping everything secret.

# Solvency

**Text: The United States Congress should increase restrictions on the war powers authority of the president of the United States by statutorily clarify that efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them fall under the introduction of hostilities under the War Powers Resolution.**

**The plan is key to reign in overly narrow interpretations of “hostilities” – congressional reporting under the War Powers Resolution effectively checks presidential power while maintaining flexibility**

**Healy 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. Thanks to Jason Thelen of the Atlantic Council for his contributions, ”Cyber Confliict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain,” February 2013.

Yet this narrow interpretation of “hostilities,” that requires¶ reporting only if action would put American troops at risk,¶ falls short. While the explanation of every administration has¶ been to submit WPR reports only for actions that put¶ American lives in danger, this definition seems divorced from¶ the text of the WPR that makes no mention of this¶ requirement. More fundamentally, while preventing¶ unnecessary American deaths is an essential part of the¶ justification for having curbs on the Executive’s power to¶ initiate hostilities, it is by no means the whole story. The¶ WPR’s text declares its purpose to “insure that the collective¶ judgment of both the Congress and the President will apply”¶ to the decision to introduce US armed forces.¶ Military force is the most drastic—not to mention the most¶ costly—manifestation of national power on the international¶ stage which must not be used recklessly or go un-checked¶ by other branches of government. Recognizing this, the¶ Framers of the Constitution made the president commanderin-¶ chief—but gave Congress the power to declare war. In an¶ age in which formal declarations of war are as out of fashion¶ as the imperial-collared diplomats who once delivered them,¶ the WPR’s language is deliberately drafted broadly in order to¶ give voice to this careful parceling of power instead of¶ unilateral action. When evaluated in the context of the WPR’s¶ policy and purpose, it is accordingly appropriate to take a¶ broader view of when “United States armed forces” are¶ “introduced into hostilities.”

If there were such a re-look on¶ this issue, hostilities in cyberspace should be treated no¶ differently from the domains or air, land, or sea.¶ It would be surprising—to say the least—if a campaign¶ designed, as cyber warfare can be, to degrade another¶ sovereign nation’s economy or debilitate its military itself¶ required no congressional imprimatur.¶ Yet this seems to be exactly the position of the DoD. In its¶ Section 934 report to Congress (discussed above) the DoD¶ seems to assert that since US personnel cannot be¶ introduced into hostilities in cyberspace then a purely cyber¶ campaign would never trigger the President’s requirement¶ under the WPR to report to Congress. No soldiers would be¶ endangered, so it is purely an Executive matter.¶ Other DoD writings clearly imply the opposite, and even the¶ Section 934 report itself discusses “hostile acts in¶ cyberspace.” What are “hostilities,” after all, if not a¶ succession of hostile acts? Elsewhere, the DoD has made¶ clear its intention to “treat cyberspace as an operational¶ domain … to ensure the ability to operate effectively in¶ cyberspace,”9 while the US Air Force’s mission is to “fly, fight,¶ and win in air, space, and cyberspace.” Of course armed¶ forces are introduced into cyberspace – why else does the¶ Pentagon’s own cyber strategy refers to cyber operations as¶ “intrusions” and “breaches”? It would make little sense to¶ prepare to operate or fight, let alone win, in a domain into¶ which one’s forces cannot be “introduced” for the purpose of¶ engaging in “hostilities.” True, American soldiers, sailors,¶ airmen and marines would be astoundingly unlikely to be¶ harmed in these hostile cyber actions, but have no doubt,¶ the DoD recognizes they would be engaged in hostile acts¶ in cyberspace.¶ In addition, our experience in cyber conflicts is still new and¶ they are likely to escalate in ways unanticipated to the DoD.¶ When these conflicts do escalate, they are far more likely to¶ blowback not against our military forces, but against the US¶ private sector, which owns and operates so much of¶ cyberspace. We may already be seeing just such blowback,¶ as the US finance sector has been the subject of a largescale¶ and prolonged cyber campaign, widely held to be¶ conducted by Iran. This counterattack is assumedly in¶ response not just to financial sanctions but also the Stuxnet¶ virus, launched by the US and Israel to disrupt the Iranian¶ nuclear program. Given the dominant role of the private¶ sector in cyberspace, and the vulnerability of the US private¶ sector, cyber hostilities should arguably receive more scrutiny¶ by both the political branches, not less.¶ 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.

#### Our definition of offensive cyber operations would best constrain presidential power – applies clarity and credibility to the WPR

Lorber 13 - J.D. Candidate, University of Pennsylvania Law School, Ph.D Candidate, Duke University Department of Political Science <Eric. January 13. “Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?” Pennsylvania Journal of Constitutional Law, Vol. 15, No. 3. LexisNexis.>

Cyberattacks are "efforts to alter, disrupt, or destroy computer systems or networks or the infor-mation or programs on them ... [,] encompassing activities that range in target (military versus civil-ian, public versus private), consequences (minor versus major, direct versus indirect), and duration (temporary versus long-term)." n83 While this definition provides broad [\*977] guidance as to what may constitute a cyberattack, for the purposes of applying existing legal structures, the definition must be conceptualized in a way that usefully fits into those preexisting regimes. Because of the complexity and great number of potential means of cyberattack, this Comment groups such attacks based on employment, i.e., the way in which they are utilized and their intended purposes. Such an approach provides greater clarity as to which U.S. domestic legal regime will likely govern their employment.

The following section proceeds by first discussing some of the technical details of cyberattacks and then moves into understanding how they have been - and likely will be - employed in future conflicts. Before moving to a discussion of what cyberattacks are, it is important to note what they are not. They are not cyberexploitation, that is, "the use of actions and operations ... to obtain information that would otherwise be kept confidential ... . Cyberexploitations are usually clandestine and con-ducted with the smallest possible intervention that still allows extraction of the information sought." n84 The core difference between attack and exploitation is in the cyber operation's purpose; cyberat-tacks are meant to be destructive whereas cyberexploitation acquires information nondestructively. n85 While the term offensive cyber operations usually encompasses both attack and exploitative ele-ments, here "OCO" refers only to attacks. At the most basic level, a cyberattack requires three elements: vulnerability; access; and pay-load. n87 A vulnerability is "an aspect of the system that can be used by the attacker to compromise" an adversary's network. n88 Given the increase in the number of complex systems employed by coun-tries in the past two decades, many cyber defense analysts and computer experts agree that it is in-creasingly difficult to foresee and prevent vulnerability exploitation before attacks. n89 Access refers to the ability to deliver the payload into the target system such that it exploits the vulnerability. In particular, access to a target depends on whether the attack can be launched via remote access (e.g., by hacking into a computer network via the internet) n90 or close access (e.g., attacking a system through [\*978] the "local installation of hardware" via covert operatives). n91 The payload describes "the things that can be done once a vulnerability has been exploited. For example, once a software agent (such as a virus) has entered a given computer, it can be programmed to do many things - re-producing and retransmitting itself, destroying files on the system, or altering files." n92 Cyberattacks generally target a system's integrity (i.e., the system's ability to operate normally), n93 ability to dis-cern proper authenticity (i.e., the system's ability to determine whether it should accept incoming data), n94 or its availability (i.e., whether users can properly access the system). n95 The resulting ef-fects can be wide-ranging, including destroying data on networks, generating bogus network traffic, covertly altering data on the network, and degrading or denying service on the network. n96