# 2AC

### T

#### Restrict and regulate are synonymous

Paust ’08 (Mike & Teresa Baker Law Center Professor, University of Houston)

Jordan 14 U.C. Davis J. Int'l L. & Pol'y 205

The primacy of customary international law is also evident in an opinion by Justice Chase in 1800. In Bas v. Tingy, Justice Chase recognized that "if a general war is declared [by Congress], its extent and operations are only restricted and regulated by the jus belli, forming a part of the law of nations ... ." n47 Therefore, the law of nations (and, in particular, the law of war) necessarily restricts and regulates congressional authorization of war's extent and operations. n48 In 1798, Albert Gallatin had recognized similarly: "By virtue of ... [the war power], Congress could ... [act], provided it be according to the laws of nations and to treaties." n49 And in 1804, counsel had argued before the Supreme Court that "as far as Congress have thought proper to legislate us into a state of war, the law of nations in war is to apply." n50 The restrictive role of the laws of war [\*221] apparently formed the basis for Justice Story's statement in 1814 that conduct under a relevant act of Congress "was absorbed in the more general operation of the law of war" and was permissible "under the jus gentium" or law of nations. n51 Although there was no clash between the act and the laws of war, the laws of war recognizably had a higher, "more general" absorbing effect.

#### Counter-interp: Statutory restrictions are legislative limits

Law dictionary No Date

http://thelawdictionary.org/statutory-restriction/

STATUTORY RESTRICTION?

Limits or controls that have been place on activities by its ruling legislation

#### Neg interp impossible: Congress CANNOT prohibit

Colella ‘88

Frank SPRING, 1988 54 Brooklyn L. Rev. 131

Because the subsequent versions of the amendment sought to deny the executive any latitude in supporting the Contras, they seem to be examples of congressional overreaching. Congress may regulate aspects of "foreign covert action," but it cannot totally bar the president from carrying them out. n151 One commentator incisively observes, "[C]ongress cannot deny the President the capacity to function effectively in this area any more than it could deny the courts the capacity to carry out their independent constitutional duties." n152 The restrictions contained in later versions of the amendments n153 make it apparent that Congress prevented effective execution of the president's policy objectives.

### Brecher CP

C. The counterplans covert action ensures unilateralism – prevents coalitions and fuels suspicion and cyberwar

**Rishikof 11**, Chair of the ABA Standing Committee on Law and National Security. Former professor of law and chair

(PROJECTING FORCE IN THE 21ST CENTURY - LEGITIMACY AND THE RULE OF LAWDepartment of National Security Strategy, National War Collegwww.rutgerslawreview.com/wp-content/uploads/archive/vol63/Issue4/Mustin-Rishikof\_Article\_PDF.pdf)

**Covert action** also **enables unilateral action. The stealthy nature of covert action means that the Executive would be discouraged from seeking international cooperation**. Any international support would likely be limited to notifying host nations of the presence of troops, and those notifications, as a tactical matter, would likely be last minute and very directive in nature. **This type of unilateral action** contrasts the cooperative intent for international law, and, in the words of one legal scholar, ―[u]nilateral action- covert or overt - **generates particularly high emotions, because many view it as a litmus test for one‘s commitment to international law. Excessive use of covert action might be deemed** by some nations **as a rebuke of international law or evidence of a hubristic foreign policy**. ///**The** continued and constant **use of this instrument** when lethality is the goal **raises issues of international legitimacy.**

#### 2. Perm do both — only the perm solves legitimacy — their author

Brecher 12 (Aaron P., , JD candidate at Michigan Law, Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations, [www.michiganlawreview.org/assets/pdfs/111/3/Brecher.pdf](http://www.michiganlawreview.org/assets/pdfs/111/3/Brecher.pdf))

It has become axiomatic of American constitutional doctrine that **presidential decisions gain greater** constitutional **legitimacy** **when** they are **carried out with Congress’s approval**. Though the president has tremendous freedom to act autonomously when conducting foreign affairs, the concerted action of both elected branches strengthens the presumption that the presidential policy is lawful. It is unclear, however, what the respective powers of either branch are when the president and Congress actively oppose one another, or when the president acts in the face of congressional silence.84 In the exercise of constitutional war powers, it seems clear that the president can order the responsive use of force, but becomes less so when faced with the question of whether the president may initiate an armed conflict. **Congress is** probably **empowered to place substantive limits on the scope of hostilities and the initiation of conflicts.**

#### 4. Links to politics – congress wants to be involved

Sasso 2012

(Brandon Sasso, December 21, 2012, “House Republicans urge Obama not to issue cybersecurity order,” The Hill, http://thehill.com/blogs/hillicon-valley/technology/274391-house-republicans-urge-obama-not-to-issue-cybersecurity-order)

A group of 46 House Republicans, led by Reps. Marsha Blackburn (Tenn.) and Steve Scalise (La.), sent President Obama a letter on Friday urging him not to issue an executive order on cybersecurity.¶ "Instead of preempting Congress' will and pushing a top-down regulatory framework, your administration should engage Congress in an open and constructive manner to help address the serious cybersecurity challenges facing our country," the lawmakers wrote. ¶ The White House is currently drafting an executive order that would encourage operators of critical infrastructure, such as banks and electric grids, to meet cybersecurity standards. ¶ The administration says the order, which could come as early as January, is necessary to protect vital systems from hackers.¶ The White House began working on the order after Senate Republicans blocked the Democrats' preferred cybersecurity bill.¶ But in their letter, the House Republicans urged the administration to continue working with Congress.

#### 5. Covert designation fuels suspicion and can’t solve cyber war — also removes international pressure from Chinese hacking

**Wright 11**, Executive director of studies at The Chicago Council on Global Affairs

(Thomas, 6/26, America has double standards in fighting cyberwar, [www.ft.com/cms/s/0/c8002f6a-a01b-11e0-a115-00144feabdc0.html#axzz1QYnW3i1w](http://www.ft.com/cms/s/0/c8002f6a-a01b-11e0-a115-00144feabdc0.html#axzz1QYnW3i1w))

While it has several advantages, **treating American cyber-destruction as a covert operation will severely undermine the new cyber-strategy. Suspicion that the US uses cyber­weapons whenever convenient will hamper its attempts to press other states to be transparent about their intentions**. **In particular, it takes the pressure off China, widely believed to be the leading state source of cyberattacks. It may also dissuade the US from developing the technology to trace the source of an attack.**

Nuclear war

**Sirota, Best-Selling Author, 11**, David Sirota is a best-selling author of the new book "Back to Our Future: How the 1980s Explain the World We Live In Now.", The Terrorist Threat We’re Ignoring, http://www.salon.com/news/david\_sirota/2011/07/11/trade\_terrorism

All of these threats are, indeed, scary -- and the last one, which sounds like something out of "Saw" movie, is especially creepy. But the fear of individual terrorist acts has diverted attention from a more systemic threat that is taking the implant idea to a much bigger platform. I'm talking about the threat of terrorists or foreign governments exploiting our economy's penchant for job outsourcing/offshoring. How? By using our corresponding reliance on imports to secretly stitch security-compromising technology into our society's central IT nervous system. Sounds far-fetched, right? Sounds like some fringe theory bizarrely melding liberal political complaints about bad trade policies with tinfoil-hat paranoia, right? Yeah, that's what I thought, until last week when -- in an announcement largely ignored by the Washington press corps -- the Department of Homeland Security made a stunning disclosure at a congressional hearing. As the business trade publication Fast Company [reports](http://www.fastcompany.com/1765855/dhs-someones-spiking-our-imported-tech-with-attack-tools) (emphasis added): A top Department of Homeland Security (DHS) official has admitted on the record that electronics sold in the U.S. are being preloaded with spyware, malware, and security-compromising components by unknown foreign parties. In testimony before the House Oversight and Government Reform Committee, acting deputy undersecretary of the DHS National Protection and Programs Directorate Greg Schaffer told Rep. Jason Chaffetz (R-UT) that both Homeland Security and the White House have been aware of the threat for quite some time. When asked by Rep. Chaffetz whether Schaffer was aware of any foreign-manufactured software or hardware components that had been purposely embedded with security risks, the DHS representative stated that "I am aware of instances where that has happened," after some hesitation. This supply chain security issue essentially means that, somewhere along the line, technology being marketed in the United States was either compromised or purposely designed to enable cyberattacks. The process by which this happens is fairly straightforward -- and its connection to our tariff-free trade policies that encourage outsourcing is obvious. First, an American company or governmental agency orders a piece of computer hardware or software from a tech company. Then, because the "free" trade era has economically incentivized those companies to move their production to low-wage countries, much of that order is actually fulfilled at foreign facilities where security and quality standards may be, ahem, lacking. If this still sounds far-fetched, remember that in the offshoring/outsourcing epoch, one of the major exporters of computer hardware -- and increasingly, software -- is China. That is, the country whose government has been at the forefront of aggressively researching, developing and implementing covert technologies that turn computers into stealth weapons of the police state. There is, for example, China's Great Firewall, which prevents computers from accessing content the government deems unacceptable. There's also the [Green Dam initiative](http://online.wsj.com/article/SB124638689078074805.html), which aimed to preload spying and censorship software on PCs. These, of course, are just the cyber-sabotage projects we know about, suggesting that there are far more being engineered by the Chinese regime. And this says nothing of the additional possibility of stateless terrorist groups infiltrating the high-tech supply chain to invisibly weave vulnerabilities into our IT infrastructure. If you think the biggest ramifications of this threat are merely Angry Birds malfunctions, suddenly shitty pictures from Hipstamatic and yet longer wait times when you fire up Microsoft Word -- think again. In an information age that sees [missiles remotely fired via keystrokes](http://news.cnet.com/8301-11386_3-10064231-76.html) and data mined for intelligence gathering, supply chain vulnerabilities in high-tech products are a genuine national security problem. Indeed, they are at least as big a threat to national security as the old concerns about how, say, offshoring steel production could compromises our strength by limiting our ability to unilaterally build tanks and warships. By creating a trade policy that helps offshore high-tech production, we may be inadvertently importing spying or terrorist instruments and then embedding those instruments into our computer-dependent society at large. What might this mean in practice? As the U.S.-China Economic and Security Review Commission [reported](http://www.nextgov.com/nextgov/ng_20110707_5612.php?oref=topstory) a few months ago, it could be "kill switches" implanted in Pentagon systems that **control our arsenal**. It could be new "War Games"-esque back doors that allow Chinese military hackers to punch in their own preprogrammed "Joshua" password and [again](http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html) breach computer networks deep within our national security apparatus.

#### 6. Congressional involvement makes the plan popular — the CP links to politics

Corcoran 11 --- Professor of Law and Director at University of New Hampshire School of Law (March 2011, Erin M., University of New Hampshire Law Review, “Obama's Failed Attempt to Close Gitmo: Why Executive Orders Can't Bring About Systemic Change,” 9 U.N.H. L. Rev. 207))

Finally, this example highlights that issuing unilateral executive orders, and then asking Congress to fund those decisions, is much less effective than having Congress help create the framework for significant policy changes. Congress is an independent branch of government regardless of whether the members' party affiliation is the same as the President's. Since members of the House are elected every two years, they are particularly sensitive to the idiosyncratic whims of the constituents in their district. For the President, it is often easier to support sweeping change on a policy level. Although Senators are elected every six years, they are still bound to protect parochial concerns of their constituents. Congress members go home every weekend to their respective districts and must explain their votes, decisions, and legislative priorities to the voters often at supermarkets, churches, and bingo halls.¶ Often times, when members of Congress can control the message or create the narrative addressing the problem, they can show their [\*235] constituents how their votes are in line with constituent priorities and concerns. In contrast, when Congress is told to do what the President wants and fund a controversial proposal, the members are in less control of the message and less invested in the outcome.¶Furthermore, in the Senate, particularly in the Appropriations Committee, members work across the aisle. Until recently, appropriators tended to vote as a block regardless of party affiliation, protecting their funding prerogatives and funding for their home districts. For example, the Senate Supplemental Appropriations mark included funding to close Guantanamo Bay. Yet, during the Senate floor debate about closing Guantanamo Bay, ultimately it was the Chair of the Appropriations Committee who filed the amendment on the floor to strip funding out of the supplemental bill. n150 The Chair's action provided cover to other appropriators to vote in support of stripping the funding. Since the Chair authored the amendment, there was no longer any obligation to support the appropriations bill as it was marked up out of committee. Generally, appropriators vote together to protect funding when other senators attempt to strip funding out of appropriations bills or move funds from one account to fund a priority not accommodated by the appropriators. Since these members value collegiality, compromise, and consultation, it is no surprise that Obama's efforts to fund Guantanamo Bay closure was thwarted. If the Senate had been charged with crafting legislation, the members would have been committed to making sure they had the votes to pass it.¶ Overall, if the Obama Administration wants to close Guantanamo Bay, it must get Congress to lead the charge. This is going to be extremely difficult now with a Republican House of Representatives and Democrat Senate that holds the majority by the narrowest of margins. At this point, it seems as if the Administration has abandoned its campaign to close Guantanamo Bay. The only silver lining is that the Administration hopefully has learned important lessons on what works and what is a non-starter and can use this knowledge when advancing the President's future controversial policy changes.

#### Future presidents roll back

Harvard Law Review 12, "Developments in the Law: Presidential Authority," Vol. 125:2057, www.harvardlawreview.org/media/pdf/vol125\_devo.pdf

The recent history of signing statements demonstrates how public opinion can effectively check presidential expansions of power by inducing executive self-binding. It remains to be seen, however, if this more restrained view of signing statements can remain intact, for **it relies on the promises of one branch — indeed of one person — to enforce and maintain the separation of powers**. To be sure, President Obama’s guidelines for the use of signing statements contain all the hallmarks of good executive branch policy: transparency, accountability, and fidelity to constitutional limitations. Yet, in practice, this apparent constraint (however well intentioned) may amount to little more than voluntary self-restraint. 146 Without a formal institutional check, it is unclear what mechanism will prevent the next President (or President Obama himself) from reverting to the allegedly abusive Bush-era practices. 147 Only time, and perhaps public opinion, will tell.

### Immigration DA

#### Won’t pass – GOP divisions

Page, 10/30/13 (Clarence, “GOP divided by immigration debate,” http://www.chicagotribune.com/news/columnists/ct-oped-1030-page-20131030,0,5264648.column, bgm)

Not everybody shares his optimism. Immigration has long divided House Republicans and the rest of the Grand Old Party. The party's dilemma is a sign of changing times and demographics: how to polish its brand and expand its reach without losing its conservative base. Pragmatic moderates in the GOP leadership want to fix our broken immigration system to spur economic growth and broaden the party's ethnic diversity after last November's presidential election loss. The only specific policy recommendation in the national party's post-election "autopsy" called for the passage of comprehensive immigration reform. But conservatives oppose anything that resembles "amnesty," including the "pathway" to legalization and ultimately citizenship that Gutierrez and other Democrats want for the nation's estimated 11 million undocumented workers. Conservatives would rather emphasize border enforcement, even though more than half of the undocumented are estimated not to have entered over the border but to have overstayed their visas.

#### Shutdown and debt ceiling poisoned the well

Nowicki and Kelly, 10/29/13 (Dan and Erin, “Fleeting hopes for immigration reform,” http://www.azcentral.com/news/politics/articles/20131029fleeting-hopes-immigration-reform.html, bgm)

The developments come as time runs short on supporters’ goal of action on immigration reform before the end of the year. The prognosis for bipartisan cooperation is grim if work on the issue slides into 2014, a congressional midterm-election year. Reform supporters are keeping their optimism in check. Feelings in Washington are still raw following the standoff between House Speaker John Boehner, R-Ohio, and his House GOP caucus and President Barack Obama over the federal government shutdown and debt ceiling. And many Republicans are not in the mood to hand the president a victory on the top domestic priority of his second term. A number of hard-line House Republicans, estimated at 20 to 40 members of Boehner’s GOP conference, have made it clear that they have no interest in voting for what they consider to be “amnesty” for undocumented immigrants.

#### Won’t pass and farm bill thumps

Galupo, 10/24/13 (Scott, “A to-do list for Republicans.” http://www.latimes.com/opinion/commentary/la-oe-galupo-republican-to-do-list-20131024,0,6408688.story#axzz2ikRNMTmg, bgm)

The first step is the most basic and most urgent: to prove to the country that Republicans are capable of governing. Obama would like very much to sign a comprehensive immigration bill into law. Republicans are split on the merits of a measure passed earlier this year by the Senate. At the risk of sounding willfully calculated, there is little urgency to bring this flawed bill to the finish line; the midterm electorate is older and whiter than in presidential years, and the odds that voters will punish Republicans for failing to resolve the legal status of undocumented immigrants seem remote. There is plenty of other important business to attend to, however. Topping the list is the so-called farm bill — a grab bag of agricultural support programs that hung fire last summer because of the tea party's insistence on steeper cuts to food stamps than Democrats could stomach. Since both sides agree that spending on food assistance should decline as the economy recovers, a deal on precisely how much shouldn't be impossible to reach.

#### Obama will pass immigration reform by XO

Mike Lillis, 2/16/2013 (staff writer, “Dems: Obama can act unilaterally on immigration reform,” <http://thehill.com/blogs/regwatch/administration/283583-dems-recognize-that-obama-can-act-unilaterally-on-immigration-reform>, Accessed 2/21/2013, rwg)

President Obama can – and will – take steps on immigration reform in the event Congress doesn't reach a comprehensive deal this year, according to several House Democratic leaders.¶ While the Democrats are hoping Congress will preclude any executive action by enacting reforms legislatively, they say the administration has the tools to move unilaterally if the bipartisan talks on Capitol Hill break down. Furthermore, they say, Obama stands poised to use them.¶ "I don't think the president will be hands off on immigration for any moment in time," Rep. Xavier Becerra (D-Calif.), the head of the House Democratic Caucus, told reporters this week. "He's ready to move forward if we're not."

#### The plan’s not perceived

Schmitt 13, **co-director of the Marilyn Ware Center for Security Studies at AEI** and the director of AEI's Program on American Citizenship. Mr. Schmitt is a former staff director of the Senate Select Committee on Intelligence. He was executive director of the President's Foreign Intelligence Advisory Board during President Ronald Reagan's second term. Mr. Schmitt's security work focuses on longer-term strategic issues that will affect America's security at home and its ability to lead abroad, while his work in the area of citizenship focuses on challenges to maintaining and sustaining a strong civic culture. His books include Of Men and Materiel: The Crisis in Military Resources (AEI Press, 2007), to which he was a contributing author and editor with Tom Donnelly; Silent Warfare: Understanding the World of Intelligence (Brassey’s, 2002), coauthored with Abram Shulsky and now in its third edition; and U.S. Intelligence at the Crossroads: Agendas for Reform (Brassey’s, 1995), a coedited volume to which he is a contributing author. His two most recent books, to which he is also editor and contributing author, are The Rise of China: Essays on the Future Competition (Encounter Books, May 2009) and Safety, Liberty and Islamist Terrorism: American and European Approaches to Domestic Counterterrorism (AEI Press, 2010), <http://www.aei-ideas.org/2011/12/authorization-for-cyber-attacks/>

**The press (and the White House) has been obsessed by the detention provision** in the recently agreed upon FY2012 **Defense Authorization bill, but one of the items that** slipped under the radar **is language authorizing the American military to engage in offensive operations in cyberspace.** Under Sec. 954,

#### **PC not key**

Hirsh, 2/16/2013 Feb. 16, 2013 (chief correspondent , political analyst) NATIONAL JOURNAL news.yahoo.com/no-thing-political-capital-201002390--politics.html;\_ylt=A2KJ3CRyFSBRwTEAoV3QtDMD

Meanwhile, the Republican members of the Senate’s so-called Gang of Eight are pushing hard for a new spirit of compromise on immigration reform, a sharp change after an election year in which the GOP standard-bearer declared he would make life so miserable for the 11 million illegal immigrants in the U.S. that they would “self-deport.” But this turnaround has very little to do with Obama’s personal influence—his political mandate, as it were. It has almost entirely to¶ do with just two numbers: 71 and 27. That’s 71 percent for Obama, 27 percent for Mitt Romney, the breakdown of the¶ Hispanic vote in the 2012 presidential election. Obama drove home his advantage by giving a speech on immigration reform¶ on Jan. 29 at a Hispanic-dominated high school in Nevada, a swing state he won by a surprising 8 percentage points in¶ November. But the movement on immigration has mainly come out of the Republican Party’s recent introspection, and the¶ realization by its more thoughtful members, such as Sen. Marco Rubio of Florida and Gov. Bobby Jindal of Louisiana, that¶ without such a shift the party may be facing demographic death in a country where the 2010 census showed, for the first¶ time, that white births have fallen into the minority. It’s got nothing to do with Obama’s political capital or, indeed, Obama¶ at all.

#### PC fails on CIR – Obama has zero relationship with House Republicans

Linda Feldmann, 10/16/2013 (staff writer, “Debt limit deal: Obama may have won, but victory is hardly lasting,” <http://www.csmonitor.com/USA/Politics/2013/1016/Debt-limit-deal-Obama-may-have-won-but-victory-is-hardly-lasting>, Accessed 10/16/2013, rwg)

And yet Obama is talking as if he can pick up with his domestic policy agenda without skipping a beat. On Tuesday, he told a Spanish-language TV station in Los Angeles that he plans to renew his push for comprehensive immigration reform.¶ Once the fiscal crisis has been resolved, he said, “the day after I’m going to be pushing to say, call a vote on immigration reform."¶ That hardly seems credible, given Obama’s barely existent relationship with congressional Republicans, says Steven Schier, a political scientist at Carleton College in Northfield, Minn.¶ “You have to build confidence through negotiations and ongoing relations over time,” he says. “I don’t see how this current crisis helped him build any relations that will move other legislative priorities forward.”

### Flex DA

#### 1. No Link – plan allows flexibility while still solving our internal links

**Clarke and Knake ‘12** (Richard (former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States) and Robert (Cybersecurity and homeland security expert at the Council on Foreign Relations), Cyber War: The Next Threat to National Security and What to Do About It, Harper Collins Books, 2012, RSR)

**Balancing our desire for military flexibility** **with the need to address the fact that cyber war could**¶ **damage the U.S. significantly, it may be possible to craft international constraints short of a complete ban.**¶ An international agreement that banned, under any circumstances, the use of cyber weapons is the most¶ extreme form of a ban. In the previous chapter, we looked briefly at the proposal of a no-first-use¶ agreement, which is a lesser option. **A no-first-use agreement could simply be a series of mutual**¶ **declarations**, or it could be a detailed international agreement. **The focus could be on keeping cyber**¶ **attacks from starting wars**, not on limiting their use once a conflict has started. We could apply the pledge¶ to all nations, or only to those nations that made a similar declaration or signed an agreement.¶ **Saying we won’t be the first ones to use cyber weapons may in fact have more than just diplomatic**¶ **appeal in the international arena**. **The existence of the pledge might make it less likely that another nation**¶ **would initiate cyber weapons use because to do so would violate an international norm that employing**¶ **cyber weapons crosses a line, is escalatory, and potentially destabilizing**. **The nation that goes first and**¶ **violates an agreement has added a degree of international opprobrium to its actions and created** in the¶ global community **a presumption of misconduct. International support for that nation’s** underlying **position**¶ in the conflict **might** thus **be undermined and the potential for international sanctions increased.**

#### 2. Congressional statue that clarifies the legal limit of Cyber-war is key to warfighting – generals think that executive planning causes battlefield incoherence

Dunlap 12 (Major General and Former Deputy Judge Advocate General , “Lawless Cyberwar? Not If You Want to Win”, www.americanbar.org/groups/public\_services/law\_national\_security/patriot\_debates2/the\_book\_online/ch9/ch9\_ess2.html-http://www.americanbar.org/groups/public\_services/law\_national\_security/patriot\_debates2/the\_book\_online/ch9/ch9\_ess2.html)

Military commanders have seen the no-legal-limits movie before and they do not like it. In the aftermath of 9/11, civilian lawyers moved in exactly that direction. Former Attorney General Alberto Gonzales, for example, rejected parts of the Geneva Conventions as “quaint.” He then aligned himself with other civilian government lawyers who seemed to believe that the president’s war-making power knew virtually no limits. The most egregious example of this mindset was their endorsement of interrogation techniques now widely labeled as torture.¶ The results of the no-legal-limits approach were disastrous. The ill-conceived civilian-sourced interrogation, detention and military tribunal policies, implemented over the persistent objections of America’s military lawyers, caused an international uproar that profoundly injured critical relations with indispensable allies. Even more damaging, they put the armed forces on the road to Abu Ghraib, a catastrophic explosion of criminality that produced what military leaders like then-U.S. Commander in Iraq Lt. Gen. Ricardo Sanchez labeled as a “clear defeat.”¶ Infused with illegalities, Abu Ghraib became the greatest reversal America has suffered since 9/11. In fact, in purely military terms, it continues to hobble counterterrorism efforts. Gen. David Petraeus observed that “Abu Ghraib and other situations like that are nonbiodegradable. They don't go away.” Petraeus told the New York Times, “The enemy continues to beat you with them like a stick.” In short, military commanders want to adhere to the law because they have hard experience with the consequences of failing to do so.¶ Why, then, are Mr. Baker and others so troubled? Actually, there are legitimate concerns about America’s cybercapabilities, but the attack on the issues is misdirected. Indeed, if Mr. Baker substitutes the word policymaker for lawyer and the word policy for law he might be closer to the truth in terms of today’s cyberwar challenges. To those with intimate knowledge of the intricacies of cyberwar, it is not the law, per se, that represents the most daunting issue; to them, it is policy.¶ For example, retired Air Force Gen. Michael Hayden, the former head of the National Security Agency and later director of the CIA, told Congress in October 2011 that America’s cyberdefenses were being undermined because cyberinformation was “horribly overclassified.” That issue is not sourced in lawyers but in policymakers who could solve the classification problem virtually overnight if they wanted.¶ That same month, Gen. Keith B. Alexander, commander of U.S. Cyber Command and current NSA director, said that rules of engagement were being developed that would “help to define conditions in which the military can go on the offensive against cyberthreats and what specific actions it can take.” Gen. Alexander readily acknowledges the applicability of the law of armed conflict, but suggests that challenges exist in discerning the facts and circumstances to apply to the law.¶ This gets to the “act of war” question Mr. Baker complains about. The law does provide a framework; it is up to decision-makers to discern the facts to apply to that framework. Hard to do? Absolutely. But frankly, such “fog of war” issues are not much different from those military commanders routinely confront in the other domains of conflict where difficult decisions frequently must be made on imperfect information.

#### 3. Massive alt causes to flex

Rozell 12

(Mark Rozell, Professor of Public Policy, George Mason University, “From Idealism to Power: The Presidency in the Age of Obama” 2012, <http://www.libertylawsite.org/book-review/from-idealism-to-power-the-presidency-in-the-age-of-obama/>, KB)

A substantial portion of Goldsmith’s book presents in detail his case that **various forces** outside of government, and some within, **are responsible for hamstringing the president** in unprecedented fashion: **Aggressive**, often intrusive, **journalism, that at times endangers national security; human rights and other advocacy groups**, some **domestic and** other **cross-national, teamed with big resources and talented, aggressive lawyers, using every legal category and technicality possible to complicate executive action**; **courts** thrust into the mix, **having to decide critical national security law controversies**, even when the judges themselves have little direct knowledge or expertise on the topics brought before them; **attorneys within the executive branch** itself **advising against actions** based on often narrow legal interpretations and with little understanding of the broader implications of tying down the president with legalisms.

#### 4. It’s impossible for the president to remain adequately flexible on cyber

Waxman ‘11

[Associate Professor, Columbia Law School; Adjunct Senior Fellow, Council on Foreign

Relations; Member of the Hoover Institution Task Force on National Security and Law. THE YALE JOURNAL OF INTERNATIONAL LAW 36:421. <http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf> ETB]

Such interpretive reorientation raises subsidiary doctrinal issues that¶ might not sit comfortably with extant U.S. legal positions about the resort to¶ force more generally. For example, in recent years the U.S. government has pushed an interpretation of anticipatory self-defense—the doctrinal notion that¶ a state may resort to self-defensive force in advance of an imminent attack,¶ rather than having to wait to suffer the first blow—that permits flexibility in¶ assessing the “imminence” of a threat so as to take account of the difficulty of¶ assessing when contemporary security threats are temporally immediate.72 If cyber-attacks with certain effects give rise to rights of self-defense, could an impending one give rise to such a right in advance as well? Moreover, how would a state even assess imminence in this context?73 Anticipatory selfdefense is especially difficult to evaluate in this context because even if hostile¶ cyber-attack capabilities and intentions are identified, there may be little or no¶ indication of their future timing. It may also be impossible to assess their likely consequences in advance, because modern society’s heavy reliance on¶ interconnected information systems means that the indirect secondary or¶ tertiary effects of cyber-attacks may be much more consequential than the¶ direct and immediate ones.

#### 5. No link – we only limit out LARGE SCALE, PRE\_EMPTIVE attacks – we can still respond quickly

#### 6. No impact to prez powers

Healy 11

Gene Healy is a vice president at the Cato Institute and the author of The Cult of the Presidency, The CATO Institute, June 2011, "Book Review: Hail to the Tyrant", http://www.cato.org/publications/commentary/book-review-hail-tyrant

Legal checks “have been relaxed largely because of the need for centralized, relatively efficient government under the complex conditions of a modern dynamic economy and a highly interrelated international order.” What’s more, the authors insist, America needs the legally unconstrained presidency both at home (given an increasingly complex economy) and abroad (given the shrinking of global distances).¶ These are disputed points, to say the least. If Friedrich Hayek was at all correct about the knowledge problem, then if anything increasing economic complexity argues for less central direction. Nor does the fact that we face “a highly interrelated international order” suggest that we’re more vulnerable than we were in 1789, as a tiny frontier republic surrounded by hostile tribes and great powers. Economic interdependence — and the rise of other modern industrial democracies — means that other players have a stake in protecting the global trading system.¶ Posner and Vermuele coin the term “tyrannophobia,” which stands for unjustified fear of executive abuse. That fear is written into the American genetic code: the authors call the Declaration of Independence “the ur-text of tyrannophobia in the United States.” As they see it, that’s a problem because “the risk that the public will fail to trust a well-motivated president is just as serious as the risk that it will trust an ill-motivated one.” They contend that our inherited skepticism toward power exacerbates biases that lead us to overestimate the dangers of unchecked presidential power. Our primate brains exaggerate highly visible risks that fill us with a sense of dread and loss of control, so we may decline to cede more power to the president even when more power is needed.¶ Fair enough in the abstract — but Posner and Vermuele fail to provide a single compelling example that might lead you to lament our allegedly atavistic “tyrannophobia.” And they seem oblivious to the fact that those same irrational biases drive the perceived need for emergency government at least as much as they do hostility towards it. Highly visible public events like the 9/11 attacks also instill dread and a perceived loss of control, even if all the available evidence shows that such incidents are vanishingly rare. The most recent year for which the U.S. State Department has data, 2009, saw just 25 U.S. noncombatants worldwide die from terrorist strikes. I know of no evidence suggesting that unchecked executive power is what stood between us and a much larger death toll.¶ Posner and Vermuele argue that only the executive unbound can address modernity’s myriad crises. But they spend little time exploring whether unconstrained power generates the very emergencies that the executive branch uses to justify its lack of constraint. Discussing George H.W. Bush’s difficulties convincing Congress and the public that the 1991 Gulf War’s risks were worth it, they comment, “in retrospect it might seem that he was clearly right.” Had that war been avoided, though, there would have been no mass presence of U.S. troops on Saudi soil — “Osama bin Laden’s principal recruiting device,” according to Paul Wolfowitz — and perhaps no 9/11.¶ Posner and Vermuele are slightly more perceptive when it comes to the home front, letting drop as an aside the observation that because of the easy-money policy that helped inflate the housing bubble, “the Fed is at least partly responsible for both the financial crisis of 2008-2009 and for its resolution.” Oh, well — I guess we’re even, then.¶ Sometimes, the authors are so enamored with the elegant economic models they construct that they can’t be bothered to check their work against observable reality. At one point, attempting to show that separation of powers is inefficient, they analogize the Madisonian scheme to “a market in which two firms must act in order to supply a good,” concluding that “the extra transaction costs of cooperation” make “the consumer (taxpayer) no better off and probably worse off than she would be under the unitary system.”¶ But the government-as-firm metaphor is daffy. In the Madisonian vision, inefficiency isn’t a bug, it’s a feature — a check on “the facility and excess of law-making … the diseases to which our governments are most liable,” per Federalist No. 62. If the “firm” in question also generates public “bads” like unnecessary federal programs and destructive foreign wars — and if the “consumer (taxpayer)” has no choice about whether to “consume” them — he might well favor constraints on production.¶ From Franklin Roosevelt onward, we’ve had something close to vertical integration under presidential command. Whatever benefits that system has brought, it’s imposed considerable costs — not least over 100,000 U.S. combat deaths in the resulting presidential wars. That system has also encouraged hubristic occupants of the Oval Office to burnish their legacies by engaging in “humanitarian war” — an “oxymoron,” according to Posner. In a sharply argued 2006 Washington Post op-ed, he noted that the Iraq War had killed tens of thousands of innocents and observed archly, “polls do not reveal the opinions of dead Iraqis.”

#### 7. Mission failure is inevitable without Congressional deliberation

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

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

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

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

In addition, the case studies show that there is considerable evidence that the executive branch has had problems determining on war aims. President George H. W. Bush studiously avoided consulting Congress during the crucial period of decision in fall 1990 when it became possible to contemplate turning Operation Desert Shield into Desert Storm. This meant that he did not have to resolve on a unified set of war aims that would have been a necessary part of convincing Congress to authorize the war. Like Truman, Bush waited until it was too late to convince Congress and the public that the war had a point beyond forcing Iraq out of Kuwait. Thus the war had no substantial implications for policy and could not even help Bush remain in office. Not submitting the war to a timely congressional decision that Bush would have respected turned out not only to be counterproductive in terms of policy, but contrary to Bush’s political interests. Similarly, President George W. Bush failed to clarify what the war in Afghanistan was for beyond the removal of al Qaeda from Afghan territory. Partly as a consequence, the war became an endless struggle against the Taliban in both Afghanistan and Pakistan that is still ongoing as of 2012. It is striking that the executive, often represented by presidentialists as the branch that is most decisive and expert on matters of war, could consistently both fail to deliberate and fail to reach agreement on its goals in going to war. This suggests strongly that the pressures to shirk hard choices are too great to be overcome by one branch working alone. As I have argued throughout this article, the post-1945 constitutional order tended to derange the policy process inside the executive branch, producing not a set of swift successful decisions, but rather a series of policy disasters. The formulation of policy on Vietnam in the Johnson administration, for example, showed serious deficiencies that have not been taken into account by contemporary presidentialists. In essence, the advisers in the White House and the different departments in the executive branch found it impossible to move beyond the narrow orbit established by the president. Rather, the president and the idiosyncratic process he establishes tends to dominate the undoubted policymaking expertise of the different departments. The lack of planning for the aftermath of the Iraq War, with the president and policymakers in the White House falling prey to all sorts of false assumptions, showed that nothing had changed since Vietnam. I have also highlighted the costs of decisions for war on presidents. In doing so, I am not arguing that presidents who go to war suffer some sort of trauma. But there is good evidence that decisions for war are considerably different from other sorts of policy decisions. They can clearly impair presidential decision making, as was the case with Presidents Johnson and Nixon and probably both Bushes, father and son. There can be other, more subtle effects on policy. War can take up so much of the president’s time that other pressing concerns, including those related to foreign affairs, are crowded out. So President Johnson probably lost several chances to negotiate meaningful arms control agreements with the Soviet Union.217 This helped undermine the structure of détente in the 1970s by continuing the arms race. Preparing for and fighting the 1991 Gulf War so exhausted President Bush and his advisers that they had less capacity to make decisions with respect to the postwar environment in Iraq.218 This helped undermined the credibility of Bush’s decision not to depose Saddam Hussein. The 2003 Iraq War so consumed President George W. Bush and his advisers that they lost track of the situation in Afghanistan, leaving to President Obama the knotty task of sorting out the mess. As the discussion in this article has thus demonstrated, the defects of the post-1945 constitutional order are manifest. Experience has shown that the executive branch is incapable of handling the deliberation necessary for decisions for war on its own. Perhaps this is what we should expect, given the continued tidal pull of the original constitutional order. Yet it is still striking how consistently poor executive decision making for war has been in the post-1945 period. These defects create several distinct challenges for executive enthusiasts. For example, supporters of the presidentialist position often stress its unitary character. With a single person at the helm, the executive branch can act quickly to address foreign crises. We can now see more clearly that when the executive branch is not subject to oversight it is too easy either for presidents to dominate their advisers, thus suppressing valuable policy input (Johnson) or to so rearrange the White House policy process that an effective decisionmaking process becomes nearly impossible (Bush II). This supports the inference, which may come as a surprise to presidentialists, that a chief purpose of interbranch deliberation is to ensure that the executive branch is truly unitary and effective with respect to the all-important decision for war. Oversight also has the potential to counter the scenario in which the president totally dominates his advisers. Congressional hearings might give advisers a public forum in which they can finally get through to the president, although this is obviously a more difficult case. Without oversight, policy in the executive branch can be unsound or even deranged. One pathway to policy disaster, seen in Vietnam, is that the various departments responsible for war are never forced to agree on a unified set of goals and what means are necessary to achieve those goals. Without strong external compulsion it is too easy for the different parts of the executive branch to fall to quarreling amongst themselves without any ability to resolve their differences. When the State Department, Defense Department and the CIA fail to agree, the NSC process has been insufficient to create a consensus on a proposed course of policy. While it is reasonable to assume that the nation requires a unified foreign policy, nothing in the internal architecture of the executive branch that guarantees unity. Again, this can strike us as surprising, because the executive branch is a hierarchy and we expect presidents to have the ability to lead. Experience shows, however, that leadership is usually expressed either through domination involving the suppression of dissident views or by the president being unable or unwilling to manage the many different parts of the executive branch together with their often strong-willed department heads. Striking the appropriate balance has been difficult for presidents who are, after all, politicians, not experienced managers. Another pathway to disaster already mentioned is that it has proven difficult for the executive branch to determine war aims. Understandably the president and his advisers tend to respond to the exigencies of the moment, rather than concerning themselves with how a given military operation relates to the overall strategy of the U.S. in foreign affairs. The executive branch does not have any inherent ability to relate short-term responses to long-term goals. As we saw with the 1991 Gulf War, this inability to justify a war in terms of long-term goals can run contrary to the president’s own political interests. It is not necessary to assume anything about the policy knowledge of individual members of Congress or the quality of congressional hearings to appreciate that a world in which the executive branch is required to justify itself publicly provides a significant incentive for the president to insist on a unified approach to policy. It is plausible that repeated iterations of oversight would build up congressional expertise in foreign policy and thus begin a meaningful cycle of accountability where each branch could learn over time from experience. While there is a sense in which everyone accepts that oversight is a traditional function of Congress, it is noteworthy that there was no strong tradition of external review established in the early Cold War. The situation with respect to the CIA eventually became notorious, with a small group of senators handling oversight on a basis akin to a private club.219 But the situation with respect to foreign affairs in general was little better, with many hearings and exchanges held in executive session or off the books in private gatherings. While it is a mistake to think that the congressional leadership had no influence over the early Cold War administrations, the lack of public oversight meant that the proper incentives were never provided to executive branch agencies. As recounted by historian Robert Johnson, later in the Cold War the influence and prestige of the Senate Foreign Relations Committee waned in comparison with the growing power of the Armed Services Committee.220 This further undermined accountability and was emblematic of the dominant militarized approach to the Cold War. While the executive branch was retooled to a certain extent for Cold War duty after 1947, nothing was done to the structure of Congress. Members of Congress assumed that the existing committee structure would suffice. Eventually the costs of this approach became apparent, at least with respect to intelligence policy. Part of the intelligence reforms of the 1970s was to establish committees to oversee the intelligence community. The subsequent difficulties with implementing this oversight have been well analyzed by a number of scholars and presidential commissions, including the 9/11 Commission. Some of the ignored proposals of the 9/11 Commission had to do with changes to congressional oversight of intelligence.221 What oversight there is has been rendered less effective by the use of term limits for service on the intelligence committees and the fact that budgetary authority is located elsewhere.222 As Amy Zegart concluded in her study of Congress, the intelligence community and 9/11: It was no secret that this fragmented oversight system desperately needed fixing. Restructuring the Congress was recommended in seven of the twelve intelligence and terrorism studies between 1991 and 2001. Yet Congress never acted. In fact, Congress was the only government entity that failed to implement a single recommendation for reform during the decade—a record worse than either the CIA’s or the FBI’s.223 One purpose of the interbranch cycle of accountability is to test the executive branch’s claims with respect to war and foreign affairs. Of all the shibboleths of the Cold War, none have arguably done more harm than the idea that the executive branch’s undoubted expertise with respect to diplomacy is relevant to the expertise necessary for planning and running a war. The experience of presidential administrations in the post-1945 period is clear – there is no such thing as a civilian “expert” in making the policy choices and decisions necessary for war. Even if we accept the reasonable point that military leaders are expert in planning and running military operations, this sort of expertise is built up over many years of service and such experience was not available to any post-1945 president except Eisenhower. Consider that the substantial expertise FDR had acquired with respect to foreign policy by the time he was elected to a third term in 1940 is barred to any contemporary president by the 22nd Amendment. Further, cabinet officials and advisers are rarely drawn from a pool of those expert in war. As we drew away from the World War II generation, the Secretaries of State and Defense have usually been different sorts of careerists or politicians. While there is nothing inherently wrong with this, none of them were experts in making war decisions.224 In fact, there have been too few major wars for any civilian adviser to acquire the sort of experience necessary before true expertise is possible. At the same time, the major wars since 1945 show that effective consultation with Congress is pragmatically possible. Because American armies have been fighting far from home in the post-World War II period, considerable time has been required to transport them to the theatre of conflict and assemble the necessary enormous amount of supply material. Aside from true crises such as the 1962 Cuban missile crisis, there has always been plenty of time for interbranch deliberation over the decision to go to war. This has not always been highlighted by presidents. In Korea, many weeks were required before the Inchon landing and break-out from the Pusan perimeter became possible. In Vietnam, it took two years, until 1967, for General Westmoreland to assemble the supply chain necessary to support the kind of military operations he envisioned in 1965.225 The build-up time required to simply provide an effective defense for Saudi Arabia (Operation Desert Shield) in the Gulf War was seventeen weeks. More weeks were required to attain an offensive capability. Months were required after 9/11 before there were sufficient regular armed forces in Afghanistan and the same was true for the Iraq War. The fact of a crisis or apparent emergency that arguably requires a military response does not necessarily mean that there is little time for proper interbranch deliberation. The war powers debate should occur on the terrain of a realistic appraisal of presidential success in making decisions for war and the possible contributions a true interbranch dialogue could make to effective decisionmaking. Such an appraisal is not found in recent works by executive enthusiasts. Eric Posner and Adrian Vermeule, for example, have recently provided a provocative theoretical grounding for executive enthusiasm. 226 They present a tightly woven argument that challenges what they describe as the “Madisonian” understanding of separation of powers. Their target, which they call “liberal legalism,” is the idea that the executive can be constrained primarily through legal means, including the constitutional law promulgated by judges as well as statutes passed by Congress.227 While their argument is wide-ranging, extending to administrative law and “global liberal legalism,” my comments here are directed at the parts of their argument most nearly relevant to war and foreign affairs. There is arguably a subtle bias in the Posner and Vermeule analysis. They criticize the eighteenth-century “Madisonian” view of how an executive should be constrained. But why constrain the executive at all? Here Posner and Vermeule confine themselves to critiquing what might be called an eighteenth-century view of the dangers posed by the executive – chiefly the threat to civil liberties and the possibility, which they rightly discount, that the American term-limited president might turn into a tyrant.228 But they do not consider reasons for caution about the executive branch connected with our twentieth-century experience with war and foreign affairs. They believe one fatal problem with liberal legalism is that Congress can never catch up with emergencies. The nature of emergencies is that rules cannot be created in advance to handle them. By contrast, the executive is well suited to handling fast-changing situations – “in emergencies, only the executive can supply new policies and real-world action with sufficient speed to manage events.”229 While this is superficially plausible, it will have a strange ring to anyone who lived through Hurricane Katrina in 2005. Of course, this does not mean Congress somehow would have done better. Posner and Vermeule’s analysis is relentlessly comparative. The fact that the executive inevitably makes mistakes and fails sometimes does not show that liberal legalism is a workable alternative. What Posner and Vermeule do not consider is the enormous influence, amply demonstrated by the narrative I have presented, of the original constitutional order. Because Posner and Vermeule do not consider how constitutional orders work, they miss the significance of the original constitutional design. My argument has concerned war and foreign affairs. But it supports the general inference that the original design made it difficult for either branch to make good policy on its own. Sound policy with respect to war requires the branches to cooperate. While political parties have made such cooperation more difficult, parties are an example of how constitutional change tends to add to, rather than completely replacing, the original constitutional order.230 The discussion in this article has shown that policymaking in the executive branch becomes deranged without the oversight and input of the legislature. Posner and Vermeule have no way to account for this because they assume that executive branch is generally competent not only to execute the law but to make policy on its own. Strangely, they do not consider the generally poor record of the executive branch in war making in the post-1945 period. This period is littered not simply with mistakes, but with policy catastrophes that undermined the stability of the government as a whole. It is also noteworthy that Posner and Vermeule focus on the executive branch without managing to say much about the person of the president or how the president runs the White House. The post-World War II experience showed that the president was incapable of managing the tasks of war without the substantial support of Congress. Briefly summarized, the biggest problem with the arguments of executive enthusiasts is that they reflect pre-Vietnam understandings of how the executive branch makes decisions in foreign policy. It is as if the substantial and closely documented historical scholarship on the Vietnam War has made no impression on legal scholars who study presidential power. These scholars continue to treat the executive branch as if it were a black box full of the “best and the brightest” – knowledgeable experts willing to make hard choices and swift, yet measured and effective decisions.231 History shows differently. Conclusion War is a unique kind of policy. Even “limited” wars tend to subordinate the rest of the nation’s foreign policy to their requirements rather than the reverse. This has meant that in starting any major military conflict, the president is almost literally betting the ranch. All the more reason to ensure that there is sufficient deliberation before going forward. In the restrained phrasing of political scientist James Kurth, the U.S. would have been better off had “an authentic democratic process” been used to approve wars since 1945.232 The question for the future is whether such a process is possible. Pg. 31-37

### Security K

D. Debate about the repercussions of cyber preemption is good- key to generating literature on dangers of cyber war, which checks its use

**Magnuson ‘9**

[Stew, National Defense Magazine. <http://www.nationaldefensemagazine.org/archive/2009/June/Pages/USPlanstoDestroyEnemyComputerNetworksQuestioned.aspx> ETB]

¶ Retired Adm. William **Owen**, **former vice chairman of the Joint Chiefs of Staff,** said he **sees little evidence that there is a government-wide understanding of the repercussions of launching an attack on enemy computers. And that goes for the military as well.**¶¶ “My guess is that most of **the generals and admirals don’t really understand** **what** the hell **we’re** **playing with here** and we need to find a way to get some focused attention” on this topic, he told National Defense.¶ ¶ Owen is the co-author of a National Research Council report, “Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber-Attack Capabilities.”¶ ¶ The study — two-and-a-half years in the making — concludes that **policies and regulations for carrying out computer attacks are “ill-formed, undeveloped and highly uncertain,”** said Kenneth Dam, a former deputy secretary of state who also contributed to the report.¶ ¶ The authors could not identify any single authority in the government responsible for coordinating cyber-attacks or promulgating policy — if there is any policy at all. Further, there are no congressional committees designated to oversee the government’s efforts. ¶ ¶ In short, if the United States government goes on the offense in cyberspace, there may be a lack of accountability, the report concluded.¶ ¶ Secrecy has impeded widespread debate about the nature and implications of cyber-attack, the authors asserted. Much of the defense community’s efforts in this realm are top secret.¶ ¶ “It’s not so much secrecy, it’s actual silence. It just isn’t discussed,” Dam said at a press briefing. **There needs to be a public debate about the repercussions of launching cyber-attacks**, the report said. **In the early days of nuclear weapons, there was a great deal of literature coming out of think tanks, universities and other institutions about when and how to use atomic bombs. That just isn’t happening in this new kind of warfare**, Dam added.

#### 3. Cyber operates in a realist framework

Dawson ‘13

[Ashley Dawson, M.A. Candidate in Policy Sci @ University of British Columbia. “Addressing Cyber Warfare: Bolstering Deterrence through developing norms.” Master’s Thesis. Etb]

RDT is centered around two central strategies with the goal of dissuading an ¶ adversary from undertaking an action that it has not already started through fear of the ¶ consequences: deterrence by punishment or MAD, a strategy that centres on a credible ¶ threat of offensive retaliation, and deterrence by denial, a defensive strategy in which a¶ potential aggressor is convinced that the offensive and defensive balance is such that an ¶ offensive attack cannot succeed and therefore should be avoided. Moreover, according to ¶ Achen and Snidal, two key components are crucial for the success of RDT: the credibility of the deterrence capabilities, and the rational actor assumption of decisions ¶ rely on a cost-benefit analysis.28 In other words, cyber deterrence is pursued by rational ¶ actors undertaking a cost benefit analysis before making logical decisions,29 where states¶ only engage in conflicts when they expect to win or from which they expect to at least ¶ yield a net gain. Therefore the proliferation of any cyber-technology that lowers a¶ weaker state’s estimation of the power/capabilities gap between it and a stronger ¶ adversary can thus be expected to make war more likely.

#### 4. IR theory proves cyberwar is probable- multiple mechanisms

Junio ‘13

[Timothy J. Junio (Tim)is a doctoral candidate of political science at the¶ University of Pennsylvania and a predoctoral fellow at the Center for¶ International Security and Cooperation (CISAC) at Stanford University.¶ He also develops new cyber capabilities at the Defense Advanced¶ Research Projects Agency (DARPA). How Probable is Cyber War? Bringing¶ IR Theory Back In to the Cyber Conflict Debate, Journal of Strategic Studies, 36:1,¶ 125-133. ETB]

Two recent articles in the pages of this journal contribute to an¶ important debate about how information technology (IT) inﬂuences¶ international politics.1¶ Thomas Rid and Adam Liff argue that cyber¶ ‘war’ has never happened and probably will not happen. A fundamental¶ problem with these articles is that Rid and Liff do not commit to a¶ theoretical framework regarding the causes of war. Doing so yields an¶ opposite conclusion: international relations theory identiﬁes many¶ mechanisms that may cause violent escalation with cyber weapons.¶ This brief response article explains why cyber war is sufﬁciently¶ probable to merit serious attention from scholars and practitioners,¶ and proposes a theoretical research agenda. First, domestic political¶ factors – such as states’ command and control over cyber operations –¶ must be problematized. The principal-agent approach demonstrates¶ how variation in incentives and preferences may make militaries more¶ likely to favor cyber attack than other kinds of bureaucracies. This¶ matters in societies with poor civilian control over the military. Second,¶ the unique material qualities of IT must be evaluated alongside¶ traditional mechanisms that cause war. For instance, the attribution¶ problem and computational complexity in modeling cyber operations¶ may increase the odds of inadvertent cyber war by causing states to¶ retaliate against the wrong targets or miscalculate the potential costs¶ and gains of attacking.

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

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

In evaluating whether securitization of cyberspace is a problem, it is very clear that securitization is a growing concern with many complications. There are many issues including privacy, regulation, surveillance, internet regulation and the growing tension in the international system. However, because the United States is a superpower contesting with other cyber-heavyweights such as Iran, Russia and China the issue will not be de-securitized in the short term. With the discovery and use of cyber-weapons, many states are in the process of making their own for defensive and offensive purposes. The government of the United States will not de-securitize the issue of cyberspace while there are rival states and groups which prove a threat to the national security agenda. These problems will continue to exist until there is no defensive agenda and the issue is de-securitized, for now securitization is a necessary evil.

#### 7. Their engagement in solely theory of cyberwar will never create change – only the permutation can resolve that.

Eriksson and Giacomello ‘6

[Johan Eriksson and Giampiero Giacomello. International Political Science Review 27.3 (Jul., 2006), pp. 221-244. “The Information Revolution, Security, and International Relations: (IR) Relevant Theory?” ETB]

The foregoing analysis has shown that there are two interrelated problems in ¶ past efforts at understanding security in the digital age. First, theory and practice ¶ on this matter are so distant that they hardly ever inform each other. Second, ¶ existing IR theories are plagued by an entrenched dualism, implying great difficulties for theoretical adaptation and application in analyses of the complexities of the emerging new digital world. ¶ One possible way of overcoming these problems is by adopting a more "prag ¶ matic" approach.'9 While there are several strands of pragmatist philosophy, ¶ pragmatism generally advocates bridge building between theory and practice, ¶ methodological pluralism, contingent generalizations, and theoretical comple ¶ mentarities and tolerance rather than entrenched opposition (Bauer and Brighi, ¶ 2002: iii). This seems to be exactly what is needed to bridge the gap between ¶ theory and practice, and to help overcome the dualistic conflicts in academic IR. ¶ There is thus no reason why the scholar trying to understand digital-age security ¶ cannot draw simultaneously on insights from a diverse range of IR theories, ¶ unfortunately often depicted as contending or incompatible, and on insights from ¶ the policy-oriented literature. ¶ The critical reader might wonder whether "pragmatist" is another word for ¶ "empiricist" or, more cynically worded, for "not smart enough for theory" ¶ (Lewontin, 1992). Indeed, pragmatism is more of an orientation, or ethos, than a ¶ theory. This is, however, a necessary first step to overcoming the chasm between ¶ theory and practice, and while a particular theory is not proffered, a fruitful ¶ starting point for the development of theory on security in the digital age is ¶ provided. With such a pragmatic approach applied to case studies and compar ¶ ative analyses, it is possible to build a foundation upon which further theory ¶ building can be done, with an emphasis on middle-range theory and on ¶ conditional rather than universal generalizations.

**8. Cyber threats are real – cyberspace is organized transnationally, not governed centrally, constantly changes, and is difficult to regulate**

**Deibert and Rohozinski 2010**

(Ronald J, professor of Political Science and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto, and Rafal, Canadian expert and practitioner active in the fields of information security, cyber warfare, and the globalization of armed violence at the University of Toronto, 2010, International Studies Association, “Risking Security: Policies and Paradoxes of Cyberspace Security,” International Political Sociology, vol. 4, p. 15-16, BS)

Globalization is generating new security challenges. Modern societies confront a myriad of risks that threaten economic prosperity, undermine the safety and security of citizens, and cause signiﬁcant disruption to society and politics. These risks range from empowered and militant nonstate actors to technological and human-made processes, such as environmental degradation and global warming. **Risk mitigation has become a routine matter of good public policy. Cyberspace represents a special category of risk.**1 A term once found only in science ﬁction novels, cyberspace describes the human-made domain for action that exists as a consequence of an interconnected and interdependent global communications and computing infrastructure. **Cyberspace connects more than half of all humanity and is an indispensable component of political, social, economic, and military power worldwide. In strategic terms, cyberspace is accepted now as a domain equal to land, air, sea, and space. Predictably, in the post-9/11 era, cyberspace is the focus of security concerns as states weigh the risks and beneﬁts of omnipresent global connectivity. However, cyberspace presents special security challenges, for a variety of reasons. First, and most importantly, it is a communication network that is organized transnationally and not through the institutional structures of the state system. Although states and individuals may claim sovereignty or ownership over segments of cyberspace, particularly parts of its material infrastructure, or even opt out of it entirely, once in they are never fully in control. Cyberspace has emergent properties, in other words, that elude state control. Second, and closely related, cyberspace is operated as a mix of public and private networks. Governance of cyberspace, like its architecture, is distributed, and does not take place within a singular forum or point of control** (Dutton and Peltu 2007). Even the Internet Corporation for Assigned Names and Numbers (ICANN), that is most often associated with Internet governance issues, is only narrowly concerned with domain and routing management and not with the full panoply of cyberspace governance issues (Mueller 2002). **There are instead numerous sites of cyberspace governance, from spectrum allocation to copyright and intellectual property regulation to content ﬁltering and cyber-crime (among many others). Each of these sites involves numerous stakeholders, including governments, businesses, and civil society networks. In addition, private sector actors from multiple countries operate most of the core infrastructural components of cyberspace.** What James Der Derian (2003) calls ‘‘heteropolarity’’ perhaps best characterizes the state of cyberspace governance. **Third, unlike other domains, such as the sea, land, air, or space, cyberspace is a human-made domain in constant ﬂux based on the ingenuity and participation of users themselves. One of the core design features of cyberspace is the end-to-end principle, which allows for generative technologies to be introduced into cyberspace by end users as long as they conform to the basic protocols of interconnectivity** (Saltzer, Reed, and Clark 1984). **The latter introduces not only great variation and constant innovation, but also new and unforeseen security risks** (Zittrain 2007). **It also creates major problems for regulation, insofar as regulators are always chasing a moving target. In other words, cyberspace is a domain of constant transformation and a high degree of complexity. Fourth, cyberspace is comprised of both a material and a virtual realm—a space of things and ideas, structure and content.** Theorists and observers of cyberspace often focus on one of these elements to the exclusion or diminution of the other, but both are important and interdependent. Cyberspace is indeed a ‘‘consensual hallucination’’ as Gibson (1984) famously deﬁned it, but one that could not exist without the physical infrastructure that supports it. **Attempts to control and monitor the virtual realm of cyberspace often begin with interventions in the physical infrastructure, at key Internet chokepoints** (Deibert, Palfrey, Rohozinski, and Zittrain 2008). **However, these efforts are never entirely comprehensive; once released into cyberspace, the distributed properties of the network help ideas and information circulate, duplicate and proliferate. Even radical measures, such as disconnecting the Internet entirely as was done recently in Burma and Nepal, can only limit, but not entirely contain the ﬂow of ideas.**

**10. The alt results in more securitization and intervention**

Tara **McCormack, 2010**, is Lecturer in International Politics at the University of Leicester and has a PhD in International Relations from the University of Westminster. 2010, (Critique, Security and Power: The political limits to emancipatory approaches, page 127-129)

The following section will briefly raise some questions about the rejection of the old security framework as it has been taken up by the most powerful institutions and states. Here we can begin to see the political limits to critical and emancipatory frameworks. In an international system which is marked by great power inequalities between states, the **rejection of the** old narrow national interest-based **security framework** by major international institutions, and the adoption of ostensibly emancipatory policies and policy rhetoric, **has the consequence of problematising weak or unstable states and allowing international institutions or major states a more interventionary role, yet without establishing mechanisms by which the citizens of states being intervened in might have any control over the agents or agencies of their emancipation**. Whatever the problems associated with the pluralist security framework **there were at least formal and clear demarcations. This has the consequence of entrenching international power inequalities and allowing for a shift towards a hierarchical international order in which the citizens in weak or unstable states may arguably have even less freedom or power than before**. Radical critics of contemporary security policies, such as human security and humanitarian intervention, argue that we see an assertion of Western power and the creation of liberal subjectivities in the developing world. For example, see Mark Duffield’s important and insightful contribution to the ongoing debates about contemporary international security and development. Duffield attempts to provide a coherent empirical engagement with, and theoretical explanation of, these shifts. Whilst these shifts, away from a focus on state security, and the so-called merging of security and development are often portrayed as positive and progressive shifts that have come about because of the end of the Cold War, Duffield argues convincingly that these shifts are highly problematic and unprogressive. For example, the rejection of sovereignty as formal international equality and a presumption of nonintervention has eroded the division between the international and domestic spheres and led to an international environment in which Western NGOs and powerful states have a major role in the governance of third world states. Whilst for supporters of humanitarian intervention this is a good development, Duffield points out the depoliticising implications, drawing on examples in Mozambique and Afghanistan. Duffield also draws out the problems of the retreat from modernisation that is represented by sustainable development. The Western world has moved away from the development policies of the Cold War, which aimed to develop third world states industrially. Duffield describes this in terms of a new division of human life into uninsured and insured life. Whilst we in the West are ‘insured’ – that is we no longer have to be entirely self-reliant, we have welfare systems, a modern division of labour and so on – sustainable development aims to teach populations in poor states how to survive in the absence of any of this. **Third world populations must be taught to be self-reliant, they will remain uninsured. Self-reliance of course means the condemnation of millions to a barbarous life of inhuman bare survival.** Ironically, although sustainable development is celebrated by many on the left today, by leaving people to fend for themselves rather than developing a society wide system which can support people, sustainable development actually leads to a less human and humane system than that developed in modern capitalist states. Duffield also describes how many of these problematic shifts are embodied in the contemporary concept of human security. For Duffield, we can understand these shifts in terms of Foucauldian biopolitical framework, which can be understood as a regulatory power that seeks to support life through intervening in the biological, social and economic processes that constitute a human population (2007: 16). Sustainable development and human security are for Duffield technologies of security which aim to *create* self-managing and self-reliant subjectivities in the third world, which can then survive in a situation of serious underdevelopment (or being uninsured as Duffield terms it) without causing security problems for the developed world. For Duffield this is all driven by a neoliberal project which seeks to control and manage uninsured populations globally. Radical critic Costas Douzinas (2007) also criticises new forms of cosmopolitanism such as human rights and interventions for human rights as a triumph of American hegemony. Whilst we are in agreement with critics such as Douzinas and Duffield that **these new security frameworks cannot be empowering, and ultimately lead to more power for powerful states,** we need to understand why these frameworks have the effect that they do. We can understand that these frameworks have political limitations without having to look for a specific plan on the part of current powerful states. **In new security frameworks such as human security we can see the political limits of the framework proposed by critical and emancipatory theoretical approaches**.

#### 11. Lack of empirical ground isn’t sufficient reason to reject the aff- the 1ac contributes to a better understanding of cyber war even without data

**Liff ‘12**

[Adam P. Liff, Doctoral Candidate, Department of Politics,¶ Princeton University, USA. “Cyberwar: A New ‘Absolute Weapon’? The¶ Proliferation of Cyberwarfare Capabilities and Interstate War,” Journal of Strategic¶ Studies, 35:3, 401-428. ETB]

Theorizing about a kind of warfare that has not occurred necessitates¶ a major caveat: the chief contribution of this article is theoretical and its¶ conclusions should be treated as preliminary. It does not – and cannot –¶ provide empirical tests.5¶ It suggests and examines several hypotheses in¶ order to try to make what we know more intelligible and challenge¶ some of the more extreme claims about cyberwarfare. While the author¶ believes that the logic underpinning his analysis is sound, this article is¶ merely a ﬁrst cut at a complex and evolving issue. As manifest in the¶ major contributions to our understanding of nuclear weapons and¶ strategy by Brodie and his contemporaries a paucity of data is not a¶ sound rationale for neglecting a topic with possible major implications¶ for national security. The hope is that this article will serve as a¶ foundation for further scholarly work on the implications of the¶ proliferation of cyberwarfare capabilities for interactions between¶ states.

[continues in footnote]

5

The data that would be necessary for an empirical study either do not exist or are¶ highly classiﬁed. Governments, militaries, and private corporations have strong¶ incentives not to reveal information about attacks. Furthermore, as will become clear¶ in the ‘deﬁning cyberwarfare’ section below, there is no example of an event in the real¶ world that can indisputably be cited as an occurrence of cyberwarfare.