# 1NC

## PTX

Obama singularly focused on the fiscal crisis—his political capital will resolve it before shutdown and default

Jonathan Allen, Politico, 9/19/13, GOP battles boost President Obama, dyn.politico.com/printstory.cfm?uuid=17961849-5BE5-43CA-B1BC-ED8A12A534EB

There’s a simple reason President Barack Obama is using his bully pulpit to focus the nation’s attention on the battle over the budget: In this fight, he’s watching Republicans take swings at each other.

And that GOP fight is a lifeline for an administration that had been scrambling to gain control its message after battling congressional Democrats on the potential use of military force in Syria and the possible nomination of Larry Summers to run the Federal Reserve.

If House Republicans and Obama can’t cut even a short-term deal for a continuing resolution, the government’s authority to spend money will run out on Oct. 1. Within weeks, the nation will default on its debt if an agreement isn’t reached to raise the federal debt limit.

For some Republicans, those deadlines represent a leverage point that can be used to force Obama to slash his health care law. For others, they’re a zero hour at which the party will implode if it doesn’t cut a deal.

**Meanwhile, “on the looming fiscal issues, Democrats** — both **liberal** and **conservative**, executive and congressional — **are virtually 100 percent united**,” said Sen. Charles Schumer (D-N.Y.).

Just a few days ago, all that Obama and his aides could talk about were Syria and Summers. Now, they’re bringing their party together and shining a white hot light on Republican disunity over whether to shut down the government and plunge the nation into default in a vain effort to stop Obamacare from going into effect.

The squabbling among Republicans has gotten so vicious that a Twitter hashtag — #GOPvsGOPugliness — has become a thick virtual data file for tracking the intraparty insults. Moderates, and even some conservatives, are slamming Texas Sen. Ted Cruz, a tea party favorite, for ramping up grassroots expectations that the GOP will shut down the government if it can’t win concessions from the president to “defund” his signature health care law.

“I didn’t go to Harvard or Princeton, but I can count,” Sen. Bob Corker (R-Tenn.) tweeted, subtly mocking Cruz’s Ivy League education. “The defunding box canyon is a tactic that will fail and weaken our position.”

While it is well-timed for the White House to interrupt a bad slide, Obama’s singular focus on the budget battle is hardly a last-minute shift. Instead, it is a return to the narrative arc that the White House was working to build before the Syria crisis intervened.

And it’s so important to the president’s strategy that White House officials didn’t consider postponing Monday’s rollout of the most partisan and high-stakes phase even when a shooter murdered a dozen people at Washington’s Navy Yard that morning.

The basic storyline, well under way over the summer, was to have the president point to parts of his agenda, including reducing the costs of college and housing, designed to strengthen the middle class; use them to make the case that he not only saved the country from economic disaster but is fighting to bolster the nation’s finances on both the macro and household level; and then argue that Republicans’ desire to lock in the sequester and leverage a debt-ceiling increase for Obamacare cuts would reverse progress made.

The president is on firm ground, White House officials say, because he stands with the public in believing that the government shouldn’t shut down and that the country should pay its bills.

The plan causes an inter-branch fight that derails Obama’s agenda

Douglas Kriner, Assistant Profess of Political Science at Boston University, 2010, After the Rubicon: Congress, Presidents, and the Politics of Waging War, p. 67-69

Raising or Lowering Political Costs by Affecting Presidential Political Capital

Shaping both real and anticipated public opinion are two important ways in which Congress can raise or lower the political costs of a military action for the president. However, focusing exclusively on opinion dynamics threatens to obscure the much broader political consequences of domestic reaction—particularly congressional opposition—to presidential foreign policies. At least since Richard Neustadt's seminal work Presidential Power, presidency scholars have warned that **costly political battles in one policy arena frequently have significant ramifications for presidential power in other realms**. Indeed, two of Neustadt's three "cases of command"—Truman's seizure of the steel mills and firing of General Douglas MacArthur—explicitly discussed the broader political consequences of stiff domestic resistance to presidential assertions of commander-in-chief powers. In both cases, Truman emerged victorious in the case at hand—yet, Neustadt argues, each victory cost Truman dearly in terms of his future power prospects and leeway in other policy areas, many of which were more important to the president than achieving unconditional victory over North Korea."

While congressional support leaves the president's reserve of political capital intact, congressional criticism saps energy from other initiatives on the home front by forcing the president to expend energy and effort defending his international agenda. **Political capital spent shoring up support for a president's foreign policies is capital that is unavailable for his future policy initiatives**. Moreover, any weakening in the president's political clout may have immediate ramifications for his reelection prospects, as well as indirect consequences for congressional races." Indeed, Democratic efforts to tie congressional Republican incumbents to President George W. Bush and his war policies paid immediate political dividends in the 2006 midterms, particularly in states, districts, and counties that had suffered the highest casualty rates in the Iraq War.6°

In addition to boding ill for the president's perceived political capital and reputation, such partisan losses in Congress only further imperil his programmatic agenda, both international and domestic. Scholars have long noted that President Lyndon Johnson's dream of a Great Society also perished in the rice paddies of Vietnam. Lacking both the requisite funds in a war-depleted treasury and the political capital needed to sustain his legislative vision, Johnson gradually let his domestic goals slip away as he hunkered down in an effort first to win and then to end the Vietnam War. In the same way, many of President Bush's **highest second-term domestic priorities**, such as Social Security and immigration reform, **failed** perhaps in large part **because the administration had to expend so much energy** and effort **waging a rear-guard action against congressional critics** of the war in Iraq.

When making their cost-benefit calculations, presidents surely consider these wider political costs of congressional opposition to their military policies. If **congressional opposition in the military arena stands to** derail other elements of his agenda, all else being equal, the president will be more likely to judge the benefits of military action insufficient to its costs than if Congress stood behind him in the international arena

That spills-over to government shutdown and US default—that kills the economy and US credibility

Norm Ornstein, resident scholar at the American Enterprise Institute, 9/1/13, Showdowns and Shutdowns, www.foreignpolicy.com/articles/2013/09/01/showdowns\_and\_shutdowns\_syria\_congress\_obama

Then there is the overload of business on the congressional agenda when the two houses return on Sept. 9 -with only nine legislative days scheduled for action in the month. We have serious confrontations ahead on spending bills and the debt limit, as the new fiscal year begins on Oct. 1 and the debt ceiling approaches just a week or two thereafter. Before the news that we would drop everything for an intense debate on whether to strike militarily in Syria, Congress-watchers were wondering how we could possibly deal with the intense bargaining required to avoid one or more government shutdowns and/or a real breach of the debt ceiling, **with** devastating consequences for American credibility **and the** international economy.

Beyond the deep policy and political divisions, Republican congressional leaders will likely use both a shutdown and the debt ceiling as hostages to force the president to cave on their demands for deeper spending cuts. **Avoiding this end-game bargaining will require** the unwavering attention of the same top leaders in the executive and legislative branches who will be deeply enmeshed in the Syria debate. The possibility -even probability -of disruptions caused by partial shutdowns could complicate any military actions. The possibility is also great that the rancor that will accompany the showdowns over fiscal policy will bleed over into the debate about America and Syria.

**US economic decline spills over to the world economy and triggers 15 unique scenarios for instability and global nuclear war –**

1) US Internal disorder 2) Trade Collapse 3) Destruction of Constitution 4) Heg collapse 5) Middle East War 6) Crime 7) Pacific Drawdown 8) Chinese Aggression 9) Chinese Instability (nuclear) 10) European Totalitarianism 11) UK instability 12) Russian Expansionism 13) German Remilitarization 14) Food Riots 15) Prolonged Global Warfare

**Duncan 12** – chief economist at Singapore-based Blackhorse Asset Management, former financial sector specialist at the World Bank and global head of investment strategy at ABN AMRO Asset Management, studied literature and economics at Vanderbilt University (1983) and international finance at Babson College (1986);(February 24, 2012, “The New Depression: The Breakdown of the Paper Money Economy,” http://www.amazon.com/The-New-Depression-Breakdown-ebook/dp/B007GZOYI6)JCP

The consequences of a New Great Depression would extend far beyond the realm of economics. Hungry people will fight to survive. Governments will use force to maintain internal order at home. This section considers the geopolitical repercussion of economic collapse, beginning with the United States.

First, the U.S. government’s tax revenues would collapse with the depression. Second, because global trade would shrivel up, other countries would no longer help finance the U.S. budget deficit by buying government bonds because they would no longer have the money to do so. At present, the rest of the world has a $500 billion annual trade surplus with the United States. The central banks of the United States’ trading partners accumulate that surplus as foreign exchange reserves and invest most of those reserves into U.S. government bonds. An economic collapse would cause global trade to plummet and drastically reduce (if not eliminate altogether) the U.S. trade deficit. Therefore, this source of foreign funding for the U.S. budget deficit would dry up.

Consequently, the government would have to sharply curtail its spending, both at home and abroad. Domestically, social programs for the old, the sick, and the unemployed would have to be slashed. Government spending on education and infrastructure would also have to be curtailed. Much less government spending would result in a dramatic increase in poverty and, consequently, in crime. This would combine to produce a crisis of the current two-party political system. Astonishment, frustration, and anger at the economic breakdown would radicalize politics. New parties would form at both extremes of the political spectrum. Given the great and growing income inequality going into the crisis, the hungry have-nots would substantially outnumber the remaining wealthy. On the one hand, a hard swing to the left would be the outcome most likely to result from democratic elections. In that case, the tax rates on the top income brackets could be raised to 80 percent or more, a level last seen in 1963. On the other hand, the possibility of a right-wing putsch could not be ruled out. During the Great Depression, the U.S. military was tiny in comparison with what it became during World War II and during the decades of hot, cold, and terrorist wars that followed. **In this New Great Depression, it might be the military that ultimately determines how the country would be governed.**

The political battle over America’s future would be bitter, and quite possibly bloody. It cannot be guaranteed that the U.S. Constitution would survive.

Foreign affairs would also confront the United States with enormous challenges. During the Great Depression, the United States did not have a global empire. Now it does. The United States maintains hundreds of military bases across dozens of countries around the world. Added to this is a fleet of 11 aircraft carriers and 18 nuclear-armed submarines. The country spends more than $650 billion a year on its military. If the U.S. economy collapses into a New Great Depression, the United States could not afford to maintain its worldwide military presence or to continue in its role as global peacekeeper. Or, at least, it could not finance its military in the same way it does at present.

Therefore, either the United States would have to find an alternative funding method for its global military presence or else it would have to radically scale it back. Historically, empires were financed with plunder and territorial expropriation. The estates of the vanquished ruling classes were given to the conquering generals, while the rest of the population was forced to pay imperial taxes.

The U.S. model of empire has been unique. It has financed its global military presence by issuing government debt, thereby taxing future generations of Americans to pay for this generation’s global supremacy. That would no longer be possible if the economy collapsed. Cost–benefit analysis would quickly reveal that much of America’s global presence was simply no longer affordable. Many—or even most—of the outposts that did not pay for themselves would have to be abandoned. Priority would be given to those places that were of vital economic interests to the United States. The Middle East oil fields would be at the top of that list. The United States would have to maintain control over them whatever the price.

In this global depression scenario, the price of oil could collapse to $3 per barrel. Oil consumption would fall by half and there would be no speculators left to manipulate prices higher. Oil at that level would impoverish the oil-producing nations, with extremely destabilizing political consequences. Maintaining control over the Middle East oil fields would become much more difficult for the United States. It would require a much larger military presence than it does now. On the one hand, it might become necessary for the United States to reinstate the draft (which would possibly meet with violent resistance from draftees, as it did during the Vietnam War). On the other hand, America’s all-volunteer army might find it had more than enough volunteers with the national unemployment rate in excess of 20 percent. The army might have to be employed to keep order at home, given that mass unemployment would inevitably lead to a sharp spike in crime.

Only after the Middle East oil was secured would the country know how much more of its global military presence it could afford to maintain.

If international trade had broken down, would there be any reason for the United States to keep a military presence in Asia when there was no obvious way to finance that presence? In a global depression, the United States’ allies in Asia would most likely be unwilling or unable to finance America’s military bases there or to pay for the upkeep of the U.S. Pacific fleet. Nor would the United States have the strength to force them to pay for U.S. protection. Retreat from Asia might become unavoidable.

And Europe? What would a cost–benefit analysis conclude about the wisdom of the United States maintaining military bases there? What valued added does Europe provide to the United States? Necessity may mean Europe will have to defend itself.

**Should a New Great Depression put an end to the Pax Americana, the world would become a much more dangerous place.** When the Great Depression began, Japan was the rising industrial power in Asia. It invaded Manchuria in 1931 and conquered much of the rest of Asia in the early 1940s. Would China, Asia’s new rising power, behave the same way in the event of a new global economic collapse? Possibly. China is the only nuclear power in Asia east of India (other than North Korea, which is largely a Chinese satellite state).

However, in this disaster scenario, it is not certain that China would survive in its current configuration. Its economy would be in ruins. Most of its factories and banks would be closed. Unemployment could exceed 30 percent. There would most likely be starvation both in the cities and in the countryside. The Communist Party could lose its grip on power, in which case the country could break apart, as it has numerous times in the past. It was less than 100 years ago that China’s provinces, ruled by warlords, were at war with one another.

United or divided, **China’s nuclear arsenal would make it Asia’s undisputed superpower if the United States were to withdraw from the region**. From Korea and Japan in the North to New Zealand in the South to Burma in the West, all of Asia would be at China’s mercy. And hunger among China’s population of 1.3 billion people could necessitate territorial expansion into Southeast Asia. In fact, the central government might not be able to prevent mass migration southward, even if it wanted to.

In Europe, severe economic hardship would revive the centuries-old struggle between the left and the right. During the 1930s, the Fascists movement arose and imposed a police state on most of Western **Europe. In the East, the Soviet Union had become a communist police state even earlier. The far right and the far left of the political spectrum converge in totalitarianism**. It is difficult to judge whether Europe’s democratic institutions would hold up better this time that they did last time.

England had an empire during the Great Depression. Now it only has banks. In a severe worldwide depression, the country— or, at least London—could become ungovernable. Frustration over poverty and a lack of jobs would erupt into anti-immigration riots not only in the United Kingdom but also across most of Europe.

The extent to which Russia would menace its European neighbors is unclear. On the one hand, Russia would be impoverished by the collapse in oil prices and might be too preoccupied with internal unrest to threaten anyone. On the other hand, it could provoke a war with the goal of maintaining internal order through emergency wartime powers.

Germany is very nearly demilitarized today when compared with the late 1930s. Lacking a nuclear deterrent of its own, it could be subject to Russian intimidation. While Germany could appeal for protection from England and France, who do have nuclear capabilities, it is uncertain that would buy Germany enough time to remilitarize before it became a victim of Eastern aggression.

As for the rest of the world, its prospects in this disaster scenario can be summed up in only a couple of sentences. Global economic output could fall by as much as half, from $60 trillion to $30 trillion. Not all of the world’s seven billion people would survive in a $30 trillion global economy. Starvation would be widespread. **Food riots would provoke political upheaval and myriad big and small conflicts around the world**. It would be a humanitarian catastrophe so extreme as to be unimaginable for the current generation, who, at least in the industrialized world, has known only prosperity. **Nor would there be reason to hope that the New Great Depression would end quickly. The Great Depression was only ended by an even more calamitous global war that killed approximately 60 million people.**

## XO CP

The executive branch of the United States federal government should issue and enforce an executive order to <plan mandate>. The order should also establish a bipartisan independent executive branch commission to <x>, mandate transparency, and develop interagency cyber warfare doctrine via consultation with the Congress.

Self-restraint is durable and sends a credible signal

Eric Posner, The University of Chicago Law School Professor, and Adrian Vermeule, Harvard Law School Professor of Law, 2007, The Credible Executive, 74 U. Chi. L. Rev. 865

The Madisonian system of oversight has not totally failed. Sometimes legislators overcome the temptation to free ride; sometimes they invest in protecting the separation of powers or legislative prerogatives. Sometimes judges review exercises of executive discretion, even during emergencies. But often enough, legislators and judges have no real alternative to letting executive officials exercise discretion unchecked. The Madisonian system is a partial failure; compensating mechanisms must be adopted to fill the area of slack, the institutional gap between executive discretion and the oversight capacities of other institutions. Again, the magnitude of this gap is unclear, but plausibly it is quite large; we will assume that it is.

It is often assumed that this partial failure of the Madisonian system unshackles and therefore benefits ill-motivated executives. This is grievously incomplete. The failure of the Madisonian system harms the well-motivated executive as much as it benefits the ill-motivated one. Where Madisonian oversight fails, the well-motivated executive is a victim of his own power. Voters, legislators, and judges will be wary of granting further discretion to an executive whose motivations are uncertain and possibly nefarious. The partial failure of Madisonian oversight thus threatens a form of inefficiency, a kind of contracting failure that makes potentially everyone, including the voters, worse off.

Our central question, then, is what the well-motivated executive can do to solve or at least ameliorate the problem. The solution is for the executive to complement his (well-motivated) first-order policy goals with second-order mechanisms for demonstrating credibility to other actors. We thus do not address the different question of what voters, legislators, judges, and other actors should do about an executive who is ill motivated and known to be so. That project involves shoring up or replacing the Madisonian system to block executive dictatorship. Our project is the converse of this, and involves finding new mechanisms to help the well-motivated executive credibly distinguish himself as such.

IV. Executive Signaling: Law and Mechanisms

We suggest that the executive's credibility problem can be solved by second-order mechanisms of executive signaling. In the general case, well-motivated executives send credible signals by taking actions that are more costly for ill-motivated actors than for well-motivated ones, thus distinguishing themselves from their ill-motivated mimics. Among the specific mechanisms we discuss, an important subset involves executive self-binding, whereby executives commit themselves to a course of action that would impose higher costs on ill-motivated actors. Commitments themselves have value as signals of benign motivations.

This departs from the usual approach in legal scholarship. Legal theory has often discussed self-binding by "government" or government officials. In constitutional theory, it is often suggested that constitutions represent an attempt by "the people" to bind "themselves" against their own future decisionmaking pathologies, or relatedly, that constitutional prohibitions represent mechanisms by which governments commit themselves not to expropriate investments or to exploit their populations. n72 Whether or not this picture is coherent, n73 it is not the question we examine here, although some of the relevant considerations are similar. n74 We are not concerned with binding the president so that he cannot abuse his powers, but with how he might bind himself or take other actions that enhance his credibility, so that he can generate support from the public and other members of the government. [\*895]

Furthermore, our question is subconstitutional: it is whether a well-motivated executive, acting within an established set of constitutional and statutory rules, can use signaling mechanisms to generate public trust. Accordingly, we proceed by assuming that no constitutional amendments or new statutes will be enacted. Within these constraints, what can a well-motivated executive do to bootstrap himself to credibility? The problem for the well-motivated executive is to credibly signal his benign motivations. In general, the solution is to engage in actions that are less costly for good types than for bad types.

We begin with some relevant law, then examine a set of possible mechanisms -emphasizing both the conditions under which they might succeed and the conditions under which they might not -and conclude by examining the costs of credibility.

A. A Preliminary Note on Law and Self-Binding

Many of our mechanisms are unproblematic from a legal perspective, as they involve presidential actions that are clearly lawful. But a few raise legal questions; in particular, those that involve self-binding. n75 Can a president bind himself to respect particular first-order policies? With qualifications, the answer is yes, at least to the same extent that a legislature can. Formally, a duly promulgated executive rule or order binds even the executive unless and until it is validly abrogated, thereby establishing a new legal status quo. n76 The legal authority to establish a new status quo allows a president to create inertia or political constraints that will affect his own future choices. In a practical sense, presidents, like legislatures, have great de facto power to adopt policies that shape the legal landscape for the future. A president might commit himself to a long-term project of defense procurement or infrastructure or foreign policy, narrowing his own future choices and generating new political coalitions that will act to defend the new rules or policies.

More schematically, we may speak of formal and informal means of self-binding:

1. The president might use formal means to bind himself. This is possible in the sense that an executive order, if otherwise valid, legally binds the president while it is in effect and may be enforced by the courts. It is not possible in the sense that the president can always repeal the executive order if he can bear the political and reputational costs of doing so.

2. The president might use informal means to bind himself. This is not only possible but frequent and important. Issuing an executive rule providing for the appointment of special prosecutors, as Nixon did, is not a formal self-binding. n77 However, there may be large political costs to repealing the order. This effect does not depend on the courts' willingness to enforce the order, even against Nixon himself. Court enforcement makes the order legally binding while it is in place, but only political and reputational enforcement can protect it from repeal. Just as a dessert addict might announce to his friends that he is going on a no-dessert diet in order to raise the reputational costs of backsliding and thus commit himself, so, too, the executive's issuance of a self-binding order can trigger reputational costs. In such cases, repeal of an executive order may be seen as a breach of faith even if no other institution ever enforces it.

Interagency development of cyber warfare doctrine solves the case – the U.S. is a leader, and the CP incorporates international partners

Mark Young, Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence, 2010, National Cyber Doctrine: The Missing Link in the Application of American Cyber Power, http://jnslp.com/2010/09/29/national-cyber-doctrine-the-missing-link-in-the-application-of-american-cyber-power/

In the development of doctrine**,** foreign partners arealmostas important as the intelligence community in offering particular knowledge, expertise, and intelligence capabilities. **It is unlikely that any future crisis will be met solely by the U**nited **S**tates. **Foreign countries and the U**nited **S**tates are **together on battlefield** of Iraq and Afghanistan, **and they will be in cyber space as well.**

Joint Publication 3-13 states:

**Allies and coalition partners recognize various** [information operations] **concepts and some have thorough and sophisticated doctrine**, procedures, and capabilities for **planning and conducting IO.** The multinational force commander (**MNFC**) **is responsible to resolve potential conflicts between each nation’s IO programs** and the IO objectives and programs of the multinational force. . . . It is vital to integrate allies and coalition partners into IO planning as early as possible so that an integrated and achievable IO strategy can be developed early in the planning process.73

**Foreign partners are critical to the success of U.S. military operations** in all the domains. A new cyber doctrine will clarify the U.S. policy in cyberspace for all allies.

IV. OTHER CONSIDERATIONS

**The most significant policy issues facing any cyberpower projection is the applicability of the Law of War** (LOW). The legal questions must be examined and resolved in detail.74 **The relationship between the laws of war and cyber operations will evolve, but a baseline policy position must involve the entire U.S. government.**

Scrutiny should focus on the definitions of “armed attack,” as well as “distinction” and “proportionality” as applied to cyber operations.75 The U.N. Charter provides guidance for responses to armed attacks. The proper classification of cyber activity as an armed attack is much more difficult than the drafters of the U.N. Charter ever envisioned. These issues are ripe for debate and could be addressed in drafting the guiding principles for a national cyber doctrine.

There is a presumption that the rules of engagement in cyber doctrine “will follow the [L]aw of Armed Conflict, meaning a response taken after receiving an electronic or cyber attack will be scaled in proportion to the attack received, and distinctions will be maintained between combatants and civilians.”76 This presumption may be significant because adversaries using cyber attacks may not distinguish between civilian and military targets. “Security experts warn that all U.S. federal agencies should now be aware that in cyberspace some malicious actors consider that no boundaries exist between military and civilian targets.”77

**The law frequently lags behind technology, but the consequences of adversarial actions against the U**nited **S**tates **and the responses of** the **Cyber Command illustrate the importance of establishing legitimate legal bases for defensive and offensive cyber operations**. “**The potentially nonlethal nature of cyber weapons may cloud the assessment of an attack’s legality, leading to more frequent violations of the principle of distinction** in this new form of warfare than in conventional warfare.”78

**For these reasons, legal experts in the national security sector must engage in the development of the new cyber doctrine.** Now is the time for the UnitedStatesto demonstrate its leadership in establishing the proper doctrine for a governmental approach in accordance with the civil and military principles that have led to U.S. freedom of action.

CONCLUSION

**The U.S. Cyber Command was established** to defend DoD networks against cyber attacks and to develop offensive cyber capabilities. The creation of this command is a legitimate response to the growing capabilities of nations such as China and Russia as well as non-state actors such as al Qaeda and Hamas. The command was established **without an adequate cyber doctrine** to guide the application of joint forces in protecting U.S. freedom of action in cyberspace. **Only by adopting a comprehensive government approach can the U**nited **S**tates **bring its full intellectual might to bear** on the challenging domain of cyberspace.

The joint doctrine development process will allow interagency elements to resolvemanyissues that currently complicate the U.S. approach to cyberpower. The joint doctrine must distinguish computer network operations from their current framework and embrace cyberspace as a war fighting domain. The process will allow debate and resolution of issues such as the training required for a cyber force, the proper classification of U.S. cyber capabilities, the authorities under which computer network attacks may be executed**,** and **actions in cyberspace that** implicate the laws of war**. This new doctrine will enhance U.S. national security by normalizing cyberspace as a domain through which the U**nited **S**tates **can express national values and protect national interests**.

A public doctrine ensures transparency – it demystifies our cyber policy

Mark Young, Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence, 2010, National Cyber Doctrine: The Missing Link in the Application of American Cyber Power, http://jnslp.com/2010/09/29/national-cyber-doctrine-the-missing-link-in-the-application-of-american-cyber-power/

A new cyber doctrine will provide guidance on the application of cyberpower in response to a physical attack or as part of a computer network attack **initiated by the U.S. government.** Under the existing doctrine, a computer network attack “is not integrated with overall [warfare] planning because of the highly compartmented classification that cyber activities receive.”51 **A major objective of assembling an interagency team to establish a national cyber doctrine is to improve the integration of** cyber defense and **offense into joint interagency operational planning. Operations in cyberspace must be “synchronized and coordinated with other operation**s, just as land and air operations . . . must be synchronized and coordinated.”52 **With their current classification, network attack capabilities are misunderstood and not widely employed**.

A national cyber doctrine should be unclassified to the maximum extent possible. As with other doctrines, a classified annex may be necessary to delineate sensitive capabilities, operations, or relationships. While it is foolish to disclose all the elements of U.S. cyberpower, the foundational principles that govern the applications of cyberpower should be widely disseminated. The development of this doctrine would de-mystify the domain for the national security community and the American people. **Federal agencies should participate in the debate to establish this doctrine and help institutionalize its principles across the entire government**. This debate can inform the decision on what information must remain classified and what does not need to be classified.

Although the doctrine should include as much unclassified detail as possible, the national cyber doctrine may require a classified annex to document U.S. offensive computer network capabilities. Other unclassified doctrines do not disclose specifications of weapons systems but do include a classified annex for a variety of purposes. Cyber weapons should be viewed as having little distinction from traditional weapons or techniques available to the U.S. Government. “Cyber weapons simply provide the operational planner with another option, in addition to the air-delivered, laser-guided bomb and the Special Operations force with demolition charges.”53 Given the nature of cyberwarfare, it is more important that details of specific weapons or techniques remain classified. As noted in a recent study, “As a general rule, [computer network] tricks exhaust themselves to the extent . . . that their existence and thus the need to protect against their recurrence is obvious and . . . that counters to their recurrence are straightforward to implement.”54

This issue of overclassification must be addressed if U.S. national security organizations are to benefit from cyberpower. According to Andrew Krepinevich, the “cyberwarfare competition is so shrouded in secrecy that it is difficult to determine the United States’ level of vulnerability, let alone options for addressing it.”55 The development of a national cyber doctrine would clarify the nation’s capabilities to those who are responsible for projecting U.S. power. The highly classified nature of computer network operations capabilities has prevented computer networks from being fully integrated into traditional war fighting exercises conducted by combatant commands. “[A]n unclassified and authoritative statement of current joint doctrine for the use of computer network attack is unavailable” and is still evolving.56

**The national security sector needs to debate cyberpower publicly**, rather than just hold classified conversations.57 **An open debate about the application of power and the circumstances that warrant** a doctrinal response would clarify and further develop the general understanding of not only the capabilities but also the limitations of network operations

## Restriction PIC

CP Text: The United States federal government should require the President of the United States to consult with congress prior to the use of offensive cyber operations except in the instance of wmd terror or aggressive offense cyber operations by other countries

## War Powers DA

Executive war power primacy now—the plan flips that

Eric Posner, 9/3/13, Obama Is Only Making His War Powers Mightier, www.slate.com/articles/news\_and\_politics/view\_from\_chicago/2013/09/obama\_going\_to\_congress\_on\_syria\_he\_s\_actually\_strengthening\_the\_war\_powers.html

President Obama’s surprise announcement that he will ask Congress for approval of a military attack on Syria is being hailed as a vindication of the rule of law and a revival of the central role of Congress in war-making, even by critics. But all of this is wrong. Far from breaking new legal ground, President **Obama has reaffirmed the primacy of the executive** in matters of war and peace. The war powers of the presidency remain as mighty as ever. It would have been different if the president had announced that only Congress can authorize the use of military force, as dictated by the Constitution, which gives Congress alone the power to declare war. **That would have been** worthy of notice, **a reversal of the ascendance of executive power over Congress**. But the president said no such thing. He said: “I believe I have the authority to carry out this military action without specific congressional authorization.” Secretary of State John Kerry confirmed that the president “has the right to do that”—launch a military strike—“no matter what Congress does.” Thus, the president believes that the law gives him the option to seek a congressional yes or to act on his own. He does not believe that he is bound to do the first. He has merely stated the law as countless other presidents and their lawyers have described it before him. The president’s announcement should be understood as a political move, not a legal one. His motive is both self-serving and easy to understand, and it has been all but acknowledged by the administration. If Congress now approves the war, it must share blame with the president if what happens next in Syria goes badly. If Congress rejects the war, it must share blame with the president if Bashar al-Assad gases more Syrian children. The big problem for Obama arises if Congress says no and he decides he must go ahead anyway, and then the war goes badly. He won’t have broken the law as he understands it, but he will look bad. He would be the first president ever to ask Congress for the power to make war and then to go to war after Congress said no. (In the past, presidents who expected dissent did not ask Congress for permission.) People who celebrate the president for humbly begging Congress for approval also apparently don’t realize that his understanding of the law—that it gives him the option to go to Congress—maximizes executive power vis-à-vis Congress. If the president were required to act alone, without Congress, then he would have to take the blame for failing to use force when he should and using force when he shouldn’t. If he were required to obtain congressional authorization, then Congress would be able to block him. But if he can have it either way, he can force Congress to share responsibility when he wants to and avoid it when he knows that it will stand in his way.

Plan destroys executive commander-in-chief supremacy—cyber capabilities are the key

Lorber ’13

Eric, J.D. Candidate, University of Pennsylvania Law School, Ph.D Candidate, Duke University Department of Political Science, “Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?,” 15 U. Pa. J. Const. L. 961

Yet a surprising amount of uncertainty exists as to which - if any - domestic laws constrain the use of OCOs and how they fit into the congressional-executive balance. As policymakers, scholars, and journalists have lamented, a coherent policy framework governing the use of OCOs does not exist and many questions remain unanswered. n8 Would an attack [\*963] using cyber weapons trigger the requirements of the War Powers Resolution? n9 Would OCOs be subject to reporting requirements under the Intelligence Authorization Act? n10 Conversely, do cyber operations grant the executive branch another tool with which it can prosecute attacks but avoid reporting and responding to congressional inquiries? These questions are largely unanswered both because the rise of OCOs is a relatively recent phenomenon and because much of the information about U.S. technical capability in this field is highly classified. n11 Yet addressing these questions is increasingly important for two reasons. First, as states such as China, Israel, Russia, and the United States use these weapons now and likely will do so more in future conflicts, determining the domestic legal strictures governing their use would provide policymakers and military planners a better sense of how to operate in cyberspace. n12 Second, the possible employment of these tools adds yet another wrinkle to the battle between the executive and legislative branches over war-making authority. n13 In particular, if neither the War Powers Resolution nor the Intelligence Authorization Act governs OCOs, the executive may be allowed to employ U.S. military power in a manner largely unchecked by congressional authority. n14 As a result, the employment of these tools [\*964] implicates - and perhaps problematically shifts - the balance between the executive's commander-in-chief power n15 and Congress's war-making authority. n16 This Comment provides an initial answer to the question of whether current U.S. law can effectively govern the Executive's use of OCOs. n17 It explores the interaction between this new tool and the current statutory limits on presidential war-making authority, with a particular focus on whether the two current federal laws meant to restrict executive power in this field - the War Powers Resolution n18 and the Intelligence Authorization Act n19 - apply to a wide range of potential offensive cyber operations undertaken by the executive branch. Beyond suggesting that neither the War Powers Resolution nor the Intelligence Authorization Act can effectively regulate most types of offensive cyber operations, this Comment suggests that while marginally problematic for a proper balance of war-making power between the executive and legislative branches, this lack of oversight does not fundamentally shift the current alignment. It does argue, however, that - given this lack of regulatory oversight - **the President now has another powerful war-making tool to use at his discretion**. Finally, the Comment suggests that this lack of limitation may be positive in some ways, as laying down clear legal markers before having a developed understanding of these capabilities may problematically limit their effective use.

That goes nuclear

**Li ‘9**

Zheyao, J.D. candidate, Georgetown University Law Center, 2009; B.A., political science and history, Yale University, 2006. This paper is the culmination of work begun in the "Constitutional Interpretation in the Legislative and Executive Branches" seminar, led by Judge Brett Kavanaugh, “War Powers for the Fourth Generation: Constitutional Interpretation in the Age of Asymmetric Warfare,” 7 Geo. J.L. & Pub. Pol'y 373 2009 WAR POWERS IN THE FOURTH GENERATION OF WARFARE

A. The Emergence of Non-State Actors

Even as the quantity of nation-states in the world has increased dramatically since the end of World War II, the institution of the nation-state has been in decline over the past few decades. Much of this decline is the direct result of the waning of major interstate war, which primarily resulted from the introduction of nuclear weapons.122 The proliferation of nuclear weapons, and their immense capacity for absolute destruction, has ensured that conventional wars remain limited in scope and duration. Hence, "both the size of the armed forces and the quantity of weapons at their disposal has declined quite sharply" since 1945.123 At the same time, concurrent with the decline of the nation-state in the second half of the twentieth century, non-state actors have increasingly been willing and able to use force to advance their causes. In contrast to nation-states, who adhere to the Clausewitzian distinction between the ends of policy and the means of war to achieve those ends, non-state actors do not necessarily fight as a mere means of advancing any coherent policy. Rather, they see their fight as a life-and-death struggle, wherein the ordinary terminology of war as an instrument of policy breaks down because of this blending of means and ends.124 It is the existential nature of this struggle and the disappearance of the Clausewitzian distinction between war and policy that has given rise to a new generation of warfare. The concept of fourth-generational warfare was first articulated in an influential article in the Marine Corps Gazette in 1989, which has proven highly prescient. In describing what they saw as the modem trend toward a new phase of warfighting, the authors argued that: In broad terms, fourth generation warfare seems likely to be widely dispersed and largely undefined; the distinction between war and peace will be blurred to the vanishing point. It will be nonlinear, possibly to the point of having no definable battlefields or fronts. The distinction between "civilian" and "military" may disappear. Actions will occur concurrently throughout all participants' depth, including their society as a cultural, not just a physical, entity. Major military facilities, such as airfields, fixed communications sites, and large headquarters will become rarities because of their vulnerability; the same may be true of civilian equivalents, such as seats of government, power plants, and industrial sites (including knowledge as well as manufacturing industries). 125 It is precisely this blurring of peace and war and the demise of traditionally definable battlefields that provides the impetus for the formulation of a new. theory of war powers. As evidenced by Part M, supra, the constitutional allocation of war powers, and the Framers' commitment of the war power to two co-equal branches, was not designed to cope with the current international system, one that is characterized by the persistent machinations of international terrorist organizations, the rise of multilateral alliances, the emergence of rogue states, and the potentially wide proliferation of easily deployable weapons of mass destruction, nuclear and otherwise. B. The Framers' World vs. Today's World The Framers crafted the Constitution, and the people ratified it, in a time when everyone understood that the state controlled both the raising of armies and their use. Today, however, the threat of terrorism is bringing an end to the era of the nation-state's legal monopoly on violence, and the kind of war that existed before-based on a clear division between government, armed forces, and the people-is on the decline. 126 As states are caught between their decreasing ability to fight each other due to the existence of nuclear weapons and the increasing threat from non-state actors, it is clear that the Westphalian system of nation-states that informed the Framers' allocation of war powers is no longer the order of the day. 127 As seen in Part III, supra, the rise of the modem nation-state occurred as a result of its military effectiveness and ability to defend its citizens. If nation-states such as the United States are unable to adapt to the changing circumstances of fourth-generational warfare-that is, if they are unable to adequately defend against low-intensity conflict conducted by non-state actors-"then clearly [the modem state] does not have a future in front of it.' 128 The challenge in formulating a new theory of war powers for fourthgenerational warfare that remains legally justifiable lies in the difficulty of adapting to changed circumstances while remaining faithful to the constitutional text and the original meaning. 29 To that end, it is crucial to remember that the Framers crafted the Constitution in the context of the Westphalian system of nation-states. The three centuries following the Peace of Westphalia of 1648 witnessed an international system characterized by wars, which, "through the efforts of governments, assumed a more regular, interconnected character."' 130 That period saw the rise of an independent military class and the stabilization of military institutions. Consequently, "warfare became more regular, better organized, and more attuned to the purpose of war-that is, to its political objective."' 1 3' That era is now over. Today, the stability of the long-existing Westphalian international order has been greatly eroded in recent years with the advent of international terrorist organizations, which care nothing for the traditional norms of the laws of war. This new global environment exposes the limitations inherent in the interpretational methods of originalism and textualism and necessitates the adoption of a new method of constitutional interpretation. While one must always be aware of the text of the Constitution and the original understanding of that text, that very awareness identifies the extent to which fourth-generational warfare epitomizes a phenomenon unforeseen by the Framers, a problem the constitutional resolution of which must rely on the good judgment of the present generation. 13 Now, to adapt the constitutional warmarking scheme to the new international order characterized by fourth-generational warfare, one must understand the threat it is being adapted to confront. C. The Jihadist Threat The erosion of the Westphalian and Clausewitzian model of warfare and the blurring of the distinction between the means of warfare and the ends of policy, which is one characteristic of fourth-generational warfare, apply to al-Qaeda and other adherents of jihadist ideology who view the United States as an enemy. An excellent analysis of jihadist ideology and its implications for the rest of the world are presented by Professor Mary Habeck. 133 Professor Habeck identifies the centrality of the Qur'an, specifically a particular reading of the Qur'an and hadith (traditions about the life of Muhammad), to the jihadist terrorists. 134 The jihadis believe that the scope of the Qur'an is universal, and "that their interpretation of Islam is also intended for the entire world, which must be brought to recognize this fact peacefully if possible and through violence if not."' 135 Along these lines, the jihadis view the United States and her allies as among the greatest enemies of Islam: they believe "that every element of modern Western liberalism is flawed, wrong, and evil" because the basis of liberalism is secularism. 136 The jihadis emphasize the superiority of Islam to all other religions, and they believe that "God does not want differing belief systems to coexist."' 37 For this reason, jihadist groups such as al-Qaeda "recognize that the West will not submit without a fight and believe in fact that the Christians, Jews, and liberals have united against Islam in a war that will end in the complete destruction of the unbelievers.' 138 Thus, the adherents of this jihadist ideology, be it al-Qaeda or other groups, will continue to target the United States until she is destroyed. Their ideology demands it. 139 To effectively combat terrorist groups such as al-Qaeda, it is necessary to understand not only how they think, but also how they operate. Al-Qaeda is a transnational organization capable of simultaneously managing multiple operations all over the world."14 It is both centralized and decentralized: al-Qaeda is centralized in the sense that Osama bin Laden is the unquestioned leader, but it is decentralized in that its operations are carried out locally, by distinct cells."4 AI-Qaeda benefits immensely from this arrangement because it can exercise direct control over high-probability operations, while maintaining a distance from low-probability attacks, only taking the credit for those that succeed. The local terrorist cells benefit by gaining access to al-Qaeda's "worldwide network of assets, people, and expertise."' 42 Post-September 11 events have highlighted al-Qaeda's resilience. Even as the United States and her allies fought back, inflicting heavy casualties on al-Qaeda in Afghanistan and destroying dozens of cells worldwide, "al-Qaeda's networked nature allowed it to absorb the damage and remain a threat." 14 3 This is a far cry from earlier generations of warfare, where the decimation of the enemy's military forces would generally bring an end to the conflict. D. The Need for Rapid Reaction and Expanded Presidential War Power By now it should be clear just how different this conflict against the extremist terrorists is from the type of warfare that occupied the minds of the Framers at the time of the Founding. Rather than maintaining the geographical and political isolation desired by the Framers for the new country, today's United States is an international power targeted by individuals and groups that will not rest until seeing her demise. The Global War on Terrorism is not truly a war within the Framers' eighteenth-century conception of the term, and the normal constitutional provisions regulating the division of war powers between Congress and the President do not apply. Instead, this "war" is a struggle for survival and dominance against forces that threaten to destroy the United States and her allies, and the fourth-generational nature of the conflict, highlighted by an indiscernible distinction between wartime and peacetime, necessitates an evolution of America's traditional constitutional warmaking scheme. As first illustrated by the military strategist Colonel John Boyd, constitutional decision-making in the realm of war powers in the fourth generation should consider the implications of the OODA Loop: Observe, Orient, Decide, and Act. 44 In the era of fourth-generational warfare, quick reactions, proceeding through the OODA Loop rapidly, and disrupting the enemy's OODA loop are the keys to victory. "In order to win," Colonel Boyd suggested, "we should operate at a faster tempo or rhythm than our adversaries." 145 In the words of Professor Creveld, "[b]oth organizationally and in terms of the equipment at their disposal, the armed forces of the world will have to adjust themselves to this situation by changing their doctrine, doing away with much of their heavy equipment and becoming more like police."1 46 Unfortunately, the existing constitutional understanding, which diffuses war power between two branches of government, necessarily (by the Framers' design) slows down decision- making. In circumstances where war is undesirable (which is, admittedly, most of the time, especially against other nation-states), the deliberativeness of the existing decision-making process is a positive attribute. In America's current situation, however, in the midst of the conflict with al-Qaeda and other international terrorist organizations, the existing process of constitutional decision-making in warfare may prove a fatal hindrance to achieving the initiative necessary for victory. As a slow-acting, deliberative body, Congress does not have the ability to adequately deal with fast-emerging situations in fourth-generational warfare. Thus, in order to combat transnational threats such as al-Qaeda, the executive branch must have the ability to operate by taking offensive military action even without congressional authorization, because only the executive branch is capable of the swift decision-making and action necessary to prevail in fourth-generational conflicts against fourthgenerational opponents.

Bioterror causes extinction

Mhyrvold ‘13

Nathan, Began college at age 14, BS and Masters from UCLA, Masters and PhD, Princeton “Strategic Terrorism: A Call to Action,” Working Draft, The Lawfare Research Paper Series

Research paper NO . 2 – 2013

As horrible as this would be, such a pandemic is by no means the worst attack one can imagine, for several reasons. First, most of the classic bioweapons are based on 1960s and 1970s technology because the 1972 treaty halted bioweapons development efforts in the United States and most other Western countries. Second, the Russians, although solidly committed to biological weapons long after the treaty deadline, were never on the cutting edge of biological research. Third and most important, the science and technology of molecular biology have made enormous advances, utterly transforming the field in the last few decades. High school biology students routinely perform molecular-biology manipulations that would have been impossible even for the best superpower-funded program back in the heyday of biological-weapons research. The biowarfare methods of the 1960s and 1970s are now as antiquated as the lumbering mainframe computers of that era. Tomorrow’s terrorists will have vastly more deadly bugs to choose from. Consider this sobering development: in 2001, Australian researchers working on mousepox, a nonlethal virus that infects mice (as chickenpox does in humans), accidentally discovered that a simple genetic modification transformed the virus.10, 11 Instead of producing mild symptoms, the new virus killed 60% of even those mice already immune to the naturally occurring strains of mousepox. The new virus, moreover, was unaffected by any existing vaccine or antiviral drug. A team of researchers at Saint Louis University led by Mark Buller picked up on that work and, by late 2003, found a way to improve on it: Buller’s variation on mousepox was 100% lethal, although his team of investigators also devised combination vaccine and antiviral therapies that were partially effective in protecting animals from the engineered strain.12, 13 Another saving grace is that the genetically altered virus is no longer contagious. Of course, it is quite possible that future tinkering with the virus will change that property, too. Strong reasons exist to believe that the genetic modifications Buller made to mousepox would work for other poxviruses and possibly for other classes of viruses as well. Might the same techniques allow chickenpox or another poxvirus that infects humans to be turned into a 100% lethal bioweapon, perhaps one that is resistant to any known antiviral therapy? I’ve asked this question of experts many times, and no one has yet replied that such a manipulation couldn’t be done. This case is just one example. Many more are pouring out of scientific journals and conferences every year. Just last year, the journal Nature published a controversial study done at the University of Wisconsin–Madison in which virologists enumerated the changes one would need to make to a highly lethal strain of bird flu to make it easily transmitted from one mammal to another.14 Biotechnology is advancing so rapidly that it is hard to keep track of all the new potential threats. Nor is it clear that anyone is even trying. In addition to lethality and drug resistance, many other parameters can be played with, given that the infectious power of an epidemic depends on many properties, including the length of the latency period during which a person is contagious but asymptomatic. Delaying the onset of serious symptoms allows each new case to spread to more people and thus makes the virus harder to stop. This dynamic is perhaps best illustrated by HIV , which is very difficult to transmit compared with smallpox and many other viruses. Intimate contact is needed, and even then, the infection rate is low. The balancing factor is that HIV can take years to progress to AIDS , which can then take many more years to kill the victim. What makes HIV so dangerous is that infected people have lots of opportunities to infect others. This property has allowed HIV to claim more than 30 million lives so far, and approximately 34 million people are now living with this virus and facing a highly uncertain future.15 A virus genetically engineered to infect its host quickly, to generate symptoms slowly—say, only after weeks or months—and to spread easily through the air or by casual contact would be vastly more devastating than HIV . It could silently penetrate the population to unleash its deadly effects suddenly. This type of epidemic would be almost impossible to combat because most of the infections would occur before the epidemic became obvious. A technologically sophisticated terrorist group could develop such a virus and kill a large part of humanity with it. Indeed, terrorists may not have to develop it themselves: some scientist may do so first and publish the details. Given the rate at which biologists are making discoveries about viruses and the immune system, at some point in the near future, someone may create artificial pathogens that could drive the human race to extinction. Indeed, a detailed species-elimination plan of this nature was openly proposed in a scientific journal. The ostensible purpose of that particular research was to suggest a way to extirpate the malaria mosquito, but similar techniques could be directed toward humans.16 When I’ve talked to molecular biologists about this method, they are quick to point out that it is slow and easily detectable and could be fought with biotech remedies. If you challenge them to come up with improvements to the suggested attack plan, however, they have plenty of ideas. Modern biotechnology will soon be capable, if it is not already, of bringing about the demise of the human race— or at least of killing a sufficient number of people to end high-tech civilization and set humanity back 1,000 years or more. That terrorist groups could achieve this level of technological sophistication may seem far-fetched, but keep in mind that it takes only a handful of individuals to accomplish these tasks. Never has lethal power of this potency been accessible to so few, so easily. Even more dramatically than nuclear proliferation, modern biological science has frighteningly undermined the correlation between the lethality of a weapon and its cost, a fundamentally stabilizing mechanism throughout history. Access to extremely lethal agents—lethal enough to exterminate Homo sapiens—will be available to anybody with a solid background in biology, terrorists included.

## Legalism

The affirmative re-inscribes the primacy of liberal legalism as a method of restraint—that paradoxically collapses resistance to Executive excesses.

**Margulies ‘11**

Joseph, Joseph Margulies is a Clinical Professor, Northwestern University School of Law. He was counsel of record for the petitioners in Rasul v. Bush and Munaf v. Geren. He now is counsel of record for Abu Zubaydah, for whose torture (termed harsh interrogation by some) Bush Administration officials John Yoo and Jay Bybee wrote authorizing legal opinions. Earlier versions of this paper were presented at workshops at the American Bar Foundation and the 2010 Law and Society Association Conference in Chicago., Hope Metcalf is a Lecturer, Yale Law School. Metcalf is co-counsel for the plaintiffs/petitioners in Padilla v. Rumsfeld, Padilla v. Yoo, Jeppesen v. Mohammed, and Maqaleh v. Obama. She has written numerous amicus briefs in support of petitioners in suits against the government arising out of counterterrorism policies, including in Munaf v. Geren and Boumediene v. Bush., “Terrorizing Academia,” http://www.swlaw.edu/pdfs/jle/jle603jmarguilies.pdf

In an observation more often repeated than defended, we are told that the attacks of September 11 “changed everything.” Whatever merit there is in this notion, it is certainly true that 9/11—and in particular the legal response set in motion by the administration of President George W. Bush—left its mark on the academy. Nine years after 9/11, it is time to step back and assess these developments and to offer thoughts on their meaning. In Part II of this essay, we analyze the post-9/11 scholarship produced by this “emergency” framing. We argue that legal scholars writing in the aftermath of 9/11 generally fell into one of three groups: unilateralists, interventionists, and proceduralists. Unilateralists argued in favor of tilting the allocation of government power toward the executive because the state’s interest in survival is superior to any individual liberty interest, and because the executive is best able to understand and address threats to the state. Interventionists, by contrast, argued in favor of restraining the executive (principally through the judiciary) precisely to prevent the erosion of civil liberties. Proceduralists took a middle road, informed by what they perceived as a central lesson of American history.1 Because at least some overreaction by the state is an inevitable feature of a national crisis, the most one can reasonably hope for is to build in structural and procedural protections to preserve the essential U.S. constitutional framework, and, perhaps, to minimize the damage done to American legal and moral traditions. Despite profound differences between and within these groups, legal scholars in all three camps (as well as litigants and clinicians, including the authors) shared a common perspective—viz., that repressive legal policies adopted by wartime governments are temporary departures from hypothesized peacetime norms. In this narrative, metaphors of bewilderment, wandering, and confusion predominate. The country “loses its bearings” and “goes astray.” Bad things happen until at last the nation “finds itself” or “comes to its senses,” recovers its “values,” and fixes the problem. Internment ends, habeas is restored, prisoners are pardoned, repression passes. In a show of regret, we change direction, “get back on course,” and vow it will never happen again. Until the next time, when it does. This view, popularized in treatments like All the Laws but One, by the late Chief Justice Rehnquist,2 or the more thoughtful and thorough discussion in Perilous Times by Chicago’s Geoffrey Stone,3 quickly became the dominant narrative in American society and the legal academy. **This narrative also figured heavily in the many challenges to Bush-era policies,** including by the authors. The narrative permitted litigators and legal scholars to draw upon what elsewhere has been referred to as America’s “civic religion”4 and to cast the courts in the role of hero-judges5 **whom we hoped would restore legal order.**6 But by framing the Bush Administration’s response as the latest in a series of regrettable but temporary deviations from a hypothesized liberal norm, the legal academy ignored the more persistent, and decidedly illiberal, authoritarian tendency in American thought to demonize communal “others” during moments of perceived threat. Viewed in this light, what the dominant narrative identified as a brief departure caused by a military crisis is more accurately seen as part of a recurring process of intense stigmatization tied to periods of social upheaval, of which war and its accompanying repressions are simply representative (and particularly acute) illustrations. It is worth recalling, for instance, that the heyday of the Ku Klux Klan in this country, when the organization could claim upwards of 3 million members, was the early-1920s, and that the period of greatest Klan expansion began in the summer of 1920, almost immediately after the nation had “recovered” from the Red Scare of 1919–20.7 Klan activity during this period, unlike its earlier and later iterations, focused mainly on the scourge of the immigrant Jew and Catholic, and flowed effortlessly from the anti-alien, anti-radical hysteria of the Red Scare. Yet this period is almost entirely unaccounted for in the dominant post-9/11 narrative of deviation and redemption, which in most versions glides seamlessly from the madness of the Red Scare to the internment of the Japanese during World War II.8 And because we were studying the elephant with the wrong end of the telescope, we came to a flawed understanding of the beast. In Part IV, we argue that the interventionists and unilateralists came to an incomplete understanding by focusing almost exclusively on what Stuart Scheingold called “the myth of rights”—the belief that if we can identify, elaborate, and secure judicial recognition of the legal “right,” **political structures and policies will adapt their behavior to the requirements of the law** and change will follow more or less automatically.9 Scholars struggled to define the relationship between law and security primarily through exploration of structural10 and procedural questions, and, to a lesser extent, to substantive rights. And they examined the almost limitless number of subsidiary questions clustered within these issues. Questions about the right to habeas review, for instance, generated a great deal of scholarship about the handful of World War II-era cases that the Bush Administration relied upon, including most prominently Johnson v. Eisentrager and Ex Parte Quirin. 11 Regardless of political viewpoint, a common notion among most unilateralist and interventionist scholars was that when law legitimized or delegitimized a particular policy, **this would have a direct and observable effect on actual behavior**. The premise of this scholarship, in other words, was that policies “struck down” by the courts, or credibly condemned as lawless by the academy, would inevitably be changed—and that this should be the focus of reform efforts. Even when disagreement existed about the substance of rights or even which branch should decide their parameters, it reflected shared acceptance of the primacy of law, often to the exclusion of underlying social or political dynamics. Eric Posner and Adrian Vermeule, for instance, may have thought, unlike the great majority of their colleagues, that the torture memo was “standard fare.”12 But their position nonetheless accepted the notion that if the prisoners had a legal right to be treated otherwise, then the torture memo authorized illegal behavior and must be given no effect.13 Recent developments, however, cast doubt on two grounding ideas of interventionist and unilateralist scholarship—viz., that post-9/11 policies were best explained as responses to a national crisis (and therefore limited in time and scope), and that the problem was essentially legal (and therefore responsive to condemnation by the judiciary and legal academy). One might have reasonably predicted that in the wake of a string of Supreme Court decisions limiting executive power, apparently widespread and bipartisan support for the closure of Guantánamo during the 2008 presidential campaign, and the election of President Barack Obama, which itself heralded a series of executive orders that attempted to dismantle many Bush-era policies, the nation would be “returning” to a period of respect for individual rights and the rule of law. Yet the period following Obama’s election has been marked by an increasingly retributive and venomous narrative surrounding Islam and national security. **Precisely when the dominant narrative would have predicted change** and redemption, we have seen retreat and retrenchment. This conundrum is not adequately addressed by dominant strands of post-9/11 legal scholarship. In retrospect, it is surprising that much post-9/11 scholarship appears to have set aside critical lessons from previous decades as to the relationship among law, society and politics.14 Many scholars have long argued in other contexts that rights—or at least the experience of rights—are subject to political and social constraints, particularly for groups subject to historic marginalization. Rather than self-executing, rights are better viewed as contingent political resources, capable of mobilizing public sentiment and generating social expectations.15 From that view, a victory in Rasul or Boumediene no more guaranteed that prisoners at Guantánamo would enjoy the right to habeas corpus than a victory in Brown v. Board16 guaranteed that schools in the South would be desegregated.17 Rasul and Boumediene, therefore, should be seen as part (and probably only a small part) of a varied and complex collection of events, including the fiasco in Iraq, the scandal at the Abu Ghraib prison, and the use of warrantless wiretaps, as well as seemingly unrelated episodes like the official response to Hurricane Katrina. These and other events during the Bush years merged to give rise to a powerful social narrative critiquing an administration committed to lawlessness, content with incompetence, and engaged in behavior that was contrary to perceived “American values.”18 Yet the very success of this narrative, culminating in the election of Barack Obama in 2008, produced quiescence on the Left, even as it stimulated massive opposition on the Right. The result has been the emergence of a counter-narrative about national security that has produced a vigorous social backlash such that most of the Bush-era policies will continue largely unchanged, at least for the foreseeable future.19 Just as we see a widening gap between judicial recognition of rights in the abstract and the observation of those rights as a matter of fact, there appears to be an emerging dominance of proceduralist approaches, which take as a given that rights dissolve under political pressure, and, thus, are best protected by basic procedural measures. But that stance falls short in its seeming readiness to trade away rights in the face of political tension. First, it accepts the tropes du jour surrounding radical Islam—namely, that it is a unique, and uniquely apocalyptic, threat to U.S. security. In this, proceduralists do not pay adequate heed to the lessons of American history and sociology. And second, it endorses too easily the idea that procedural and structural protections will protect against substantive injustice in the face of popular and/or political demands for an outcome-determinative system that cannot tolerate acquittals. Procedures only provide protection, however, if there is sufficient political support for the underlying right. Since the premise of the proceduralist scholarship is that such support does not exist, it is folly to expect the political branches to create meaningful and robust protections. In short, a witch hunt does not become less a mockery of justice when the accused is given the right to confront witnesses. And a separate system (especially when designed for demonized “others,” such as Muslims) cannot, by definition, be equal. In the end, we urge a fuller embrace of what Scheingold called “the politics of rights,” which recognizes the contingent character of rights in American society. We agree with Mari Matsuda, who observed more than two decades ago that rights are a necessary but not sufficient resource for marginalized people with little political capital.20 To be effective, therefore, we must look beyond the courts and grapple with the hard work of long-term change with, through and, perhaps, in spite of law. These are by no means new dilemmas, but the post-9/11 context raises difficult and perplexing questions that deserve study and careful thought as our nation settles into what appears to be a permanent emergency.

Legalism underpins the violence of empire and creates the conditions of possibility for liberal violence.

Dossa ‘99

Shiraz, Department of Political Science, St. Francis Xavier University, Antigonish, Nova Scotia, “Liberal Legalism: Law, Culture and Identity,” The European Legacy, Vol. 4, No. 3, pp. 73-87,1

No discipline in the rationalized arsenal of modernity is as rational, impartial, objective as the province of law and jurisprudence, in the eyes of its liberal enthusiasts. Law is the exemplary countenance of the conscious and calculated rationality of modern life, **it is the** emblematic face of liberal civilization. Law and legal rules symbolize the spirit of science, the march of human progress. As Max Weber, the reluctant liberal theorist of the ethic of rationalization, asserted: judicial formalism enables the legal system to operate like a technically **rational machine**. Thus it guarantees to individuals and groups within the system a relative of maximum of freedom, and greatly increases for them the possibility of predicting the legal consequences of their action. In this reading, law encapsulates the western capacity to bring order to nature and human beings, to turn the ebb and flow of life into a "rational machine" under the tutelage of "judicial formalism".19 Subjugation of the Other races in the colonial empires was motivated by power and rapacity, but it was justified and indeed rationalized, by an appeal to the civilizing influence of religion and law: western Christianity and liberal law. To the imperialist mind, "the civilizing mission of law" was fundamental, though Christianity had a part to play in this program.20 Liberal colonialists visualized law, civilization and progress as deeply connected and basic, they saw western law as neutral, universally relevant and desirable. The first claim was right in the liberal context, the second thoroughly false. In the liberal version, the mythic and irrational, emblems of thoughtlessness and fear, had ruled all life-forms in the past and still ruled the lives of the vast majority of humanity in the third world; in thrall to the majesty of the natural and the transcendent, primitive life flourished in the environment of traditionalism and lawlessness, hallmarks of the epoch of ignorance. By contrast, liberal ideology and modernity were abrasively unmythic, rational and controlled. Liberal order was informed by knowledge, science, a sense of historical progress, a continuously improving future. But this canonical, secular, bracing self-image, is tendentious and substantively illusory: it blithely scants the bloody genealogy and the extant historical record of liberal modernity, liberal politics, and particularly liberal law and its impact on the "lower races" (Hobson). In his Mythology of Modern Law, Fitzpatrick has shown that the enabling claims of liberalism, specifically of liberal law, are not only untenable but implicated in canvassing a racist justification of its colonial past and in eliding the racist basis of the structure of liberal jurisprudence.21 Liberal law is mythic in its presumption of its neutral, objective status. Specifically, the liberal legal story of its immaculate, analytically pure origin obscures and veils not just law's own ruthless, violent, even savage and disorderly trajectory, but also its constitutive association with imperialism and racism.22 In lieu of the transcendent, divine God of the "lower races", modern secular law postulated the gods of History, Science, Freedom. Liberal law was to be the instrument for realizing the promise of progress that the profane gods had decreed. Fitzpatrick's invasive surgical analysis lays bare the underlying logic of law's self-articulation in opposition to the values of cultural-racial Others, and its strategic, continuous reassertion of liberalism's superiority and the civilizational indispensability of liberal legalism. Liberal law's self-presentation presupposes a corrosive, debilitating, anarchic state of nature inhabited by the racial Others and lying in wait at the borders of the enlightened modern West. This mythological, savage Other, creature of raw, natural, unregulated fecundity and sexuality, justified the liberal conquest and control of the racially Other regions.23 Law's violence and resonant savagery on behalf of the West in its imperial razing of cultures and lands of the others, has been and still is, justified in terms of the necessary, beneficial spread of liberal civilization. Fitzpatrick's analysis parallels the impassioned deconstruction of this discourse of domination initiated by Edward Said's Orientalism, itself made possible by the pioneering analyses of writers like Aime Cesaire and Frantz Fanon. Fitzpatrick's argument is nevertheless instructive: his focus on law and its machinations unravels the one concrete province of imperial ideology that is centrally modern and critical in literally transforming and refashioning the human nature of racial Others. For liberal law carries on its back the payload of "progressive", pragmatic, **instrumental modernity**, its ideals of order and rule of law, its articulation of human rights and freedom, its ethic of procedural justice, its hostility to the sacred, to transcendence or spiritual complexity, its recasting of politics as the handmaiden of the nomos, its valorization of scientism and rationalization in all spheres of modern life. Liberal law is not synonymous with modernity tout court, but it is the exemplary voice of its rational spirit, **the custodian of its civilizational ambitions.** For the colonized Others, no non-liberal alternative is available: a non-western route to economic progress is inconceivable in liberal-legal discourse. For even the truly tenacious in the third world will never cease to be, in one sense or another, the outriders of modernity: their human condition condemns them to **playing perpetual catch-up**, eternally subservient to Western economic and technological superiority in a epoch of self-surpassing modernity.24 If the racially Other nations suffer exclusion globally, the racially other minorities inside the liberal loop enjoy the ambiguous benefits of inclusion. As legal immigrants or refugees, they are entitled to the full array of rights and privileges, as citizens (in Canada, France, U.K., U.S—Germany is the exception) they acquire civic and political rights as a matter of law. Formally, they are equal and equally deserving. In theory liberal law is inclusive, but concretely it is routinely **partial and invidious**. Inclusion is conditional: it depends on how robustly the new citizens wear and deploy their cultural difference. Two historical facts account for this phenomenon: liberal law's role in western imperialism and the Western claim of civilizational superiority that pervades the culture that sustains liberal legalism. Liberal law, as the other of the racially Other within its legal jurisdiction, differentiates and locates this other in the enemy camp of the culturally raw, irreducibly foreign, making him an unreliable ally or citizen. Law's suspicion of the others socialized in "lawless" cultures is instinctive and undeniable. Liberal law's constitutive bias is in a sense incidental: the real problem is racism or the racist basis of liberal ideology and culture.25 The internal racial other is not the juridical equal in the mind of liberal law but the juridically and humanly inferior Other, the perpetual foreigner.

The alternative is to vote negative to endorse political, rather than legal restrictions on Presidential war powers authority.

**Goldsmith ‘12**

Jack, Harvard Law School Professor, focus on national security law, presidential power, cybersecurity, and conflict of laws, Former Assistant Attorney General, Office of Legal Counsel, and Special Counsel to the Department of Defense, Hoover Institution Task Force on National Security and Law, March 2012, Power and Constraint, p. 205-209

DAVID BRIN is a science-fiction writer who in 1998 turned his imagination to a nonfiction book about privacy called The Transparent Society. Brin argued that individual privacy was on a path to extinction because government surveillance tools—tinier and tinier cameras and recorders, more robust electronic snooping, and bigger and bigger databases—were growing irreversibly more powerful. His solution to this attack on personal space was not to erect privacy walls, which he thought were futile, but rather to induce responsible government action by turning the surveillance devices on the government itself. A government that citizens can watch, Brin argued, is one subject to criticism and reprisals for its errors and abuses, and one that is more careful and responsible in the first place for fear of this backlash. A transparent government, in short, is an accountable one. "If neo-western civilization has one great trick in its repertoire, a technique more responsible than any other for its success, that trick is accountability," Brin argues, "[e]specially the knack—which no other culture ever mastered—of making accountability apply to the mighty."' Brin's notion of reciprocal transparency is in some ways the inverse of the penological design known as a "panopticon," made famous by the eighteenth-century English utilitarian philosopher Jeremy Bentham. Bentham's brother Samuel had designed a prison in Paris that allowed an "inspector" to monitor all of the inmates from a central location without the prisoners knowing whether or when they were being watched (and thus when they might be sanctioned for bad behavior). Bentham described the panopticon prison as a "new mode of obtaining power of mind over mind" because it allowed a single guard to control many prisoners merely by conveying that he might be watching.' The idea that a "watcher" could gain enormous social control over the "watched" through constant surveillance backed with threats of punishment has proved influential. Michel Foucault invoked Bentham's panopticon as a model for how modern societies and governments watch people in order to control them.' George Orwell invoked a similar idea three decades earlier with the panoptical telescreen in his novel 1984. More recently, Yale Law School professor Jack Balkin used the panopticon as a metaphor for what he calls the "National Surveillance State," in which governments "use surveillance, data collection, and data mining technologies not only to keep Americans safe from terrorist attacks but also to prevent ordinary crime and deliver social services." **The direction of the panopticon can be reversed, however, creating a "synopticon" in which many can watch one, including the government**.' The television is a synopticon that enables millions to watch the same governmental speech or hearing, though it is not a terribly robust one because the government can control the broadcast. Digital technology and the Internet combine to make a more powerful synopticon that allows many individuals to record and watch an official event or document in sometimes surprising ways. Video recorders placed in police stations and police cars, cell-phone video cameras, and similar tools increase citizens' ability to watch and record government activity. This new media content can be broadcast on the Internet and through other channels to give citizens synoptical power over the government—a power that some describe as "sousveillance" (watching from below)! These and related forms of watching can have a disciplining effect on government akin to Brin's reciprocal transparency. The various forms of watching and checking the presidency described in this book constitute a vibrant presidential synopticon. Empowered by legal reform and technological change, the "many"—in the form of courts, members of Congress and their staff, human rights activists, journalists and their collaborators, and lawyers and watchdogs inside and outside the executive branch—constantly gaze on the "one," the presidency. Acting alone and in mutually reinforcing networks that crossed organizational boundaries, these institutions extracted and revealed information about the executive branch's conduct in war—sometimes to adversarial actors inside the government, and sometimes to the public. The revelations, in turn, forced the executive branch to account for its actions and enabled many institutions to influence its operations. **The presidential synopticon** also **promoted responsible executive action merely through its broadening gaze.** One consequence of a panopticon, in Foucault's words, is "to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power."' The same thing has happened in reverse but to similar effect within the executive branch, where officials are much more careful merely by virtue of being watched. The presidential synopticon is in some respects not new. Victor Davis Hanson has argued that "war amid audit, scrutiny, and self-critique" has been a defining feature of the Western tradition for 2,500 years.' From the founding of the nation, American war presidents have been subject to intense scrutiny and criticism in the unusually open society that has characterized the United States. And many of the accountability mechanisms described in this book have been growing since the 1970s in step with the modern presidency. What is new, however, is the scope and depth of these modern mechanisms, their intense legalization, and their robust operation during wartime. In previous major wars the President determined when, how, and where to surveil, target, detain, transfer, and interrogate enemy soldiers, often without public knowledge, and almost entirely without unwanted legal interference from within the executive branch itself or from the other branches of government.' Today these **decisions are known inside and outside the government to an unprecedented degree** and are heavily regulated by laws and judicial decisions that are enforced daily by lawyers and critics inside and outside the presidency. Never before have Congress, the courts, and lawyers had such a say in day-to-day military activities; never before has the Commander in Chief been so influenced, and constrained, by law. This regime has many historical antecedents, but it came together and hit the Commander in Chief hard for the first time in the last decade. It did so because of extensive concerns about excessive presidential power in an indefinite and unusually secretive war fought among civilians, not just abroad but at home as well. These concerns were exacerbated and given credibility by the rhetoric and reality of the Bush administration's executive unilateralism—a strategy that was designed to free it from the web of military and intelligence laws but that instead galvanized forces of reaction to presidential power and deepened the laws' impact. Added to this mix were enormous changes in communication and collaboration technologies that grew to maturity in the decade after 9/11. These changes helped render executive branch secrets harder to keep, and had a flattening effect on the executive branch just as it had on other hierarchical institutions, making connections between (and thus accountability to) actors inside and outside the presidency **much more extensive**.

# Case

## loac

No modeling - strategic incentive to maintain legal ambiguity

Waxman 11

Matthew C. Waxman, Associate Professor, Columbia Law School; Adjunct Senior Fellow, Council on Foreign Relations; Member of the Hoover Institution Task Force on National Security and Law, Yale Journal of International Law, March 16, 2011, “Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," vol 36, http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1674565

B. Technology, Power Shifts, and the Strategic Logic of Legal Interpretation

With these relationships between law and power in mind, the United States has an interest in regulating cyber-attacks, but it will be difficult to achieve such regulation through international use-of-force law or through new international agreements to outlaw types of cyber-attacks.143 That is because the distribution of emerging cyber-capabilities and vulnerabilities— vulnerabilities defined not only by the defensive capacity to block actions but also by the ability to tolerate and withstand attacks—is unlikely to correspond to the status quo distribution of power built on traditional measures like military and economic might.

It is not surprising that the United States seems inclined toward an interpretation of Articles 2(4) and 51 that allows it to classify some offensive cyber-attacks as prohibited “force” or an “armed attack” but does not otherwise move previously drawn lines to encompass economic coercion or other means of subversion in that classification. Nor is it surprising to see the United States out in front of other states on this issue. The power and vulnerability distribution that accompanies reliance on networked information technology is not the same as past distributions of military and economic power, and perhaps not to the United States’s advantage relative to rivals. Moreover, some U.S. strengths are heavily built on digital interconnectedness and infrastructure that is global, mostly private, and rapidly changing; these strengths are therefore inextricably linked to new and emerging vulnerabilities.144

Although some experts assess that the United States is currently strong relative to others in terms of offensive capabilities,145 several factors make the United States especially vulnerable to cyber-attack, including the informational and electronic interconnectedness of its military and public and private sectors, and political obstacles to curing some of these vulnerabilities through regulation.146 As the Obama administration’s 2010 National Security Strategy acknowledged:

The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority . . . . Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale.147

In other words, U.S. technological strengths create corresponding exposures to threats. The U.S. government is especially constrained politically and legally in securing its information infrastructure—which is largely privately held or privately supplied—against cyber-threats, and these constraints shape its international strategy. Proposals to improve cyber-security through regulation include promulgating industry standards to enhance the security of information technology products and protect networks and computers from intrusion, and, more invasively, expanding the government’s authority to monitor information systems and communications.148 Such proposals invariably face powerful antiregulatory industry pressures and heightened civil liberties sensitivities.149 Information technology industry groups and privacy organizations have together pushed back against moves to impose government security mandates and against more intrusive government cyber-security activities, arguing that they would stifle innovation, erode civil liberties, and fail to keep up with rapidly evolving threats amid a globalized economy.150 A reluctance to secure information systems domestically through government regulation then elevates U.S. government reliance on other elements of a defensive strategy.

In that light, U.S. legal interpretations and declaratory postures that define prohibited force in ways that extend narrow Charter interpretations to take account of cyber-warfare may be seen as part of an effort to sustain a legal order in which anticipated U.S. military and economic moves and countermoves against potential adversaries fit quite comfortably—that is, a legal order that preserves U.S. comparative advantages. In extending the foundational U.N. Charter prohibition on force to cyber-attacks by emphasizing their comparable effects to conventional military attacks, such interpretations help deny that arsenal to others by raising the costs of its use. At the same time, by casting that prohibition and complementary self-defense authority in terms that help justify military force in response, this interpretation reduces the costs to the United States of using or threatening to use its vast military edge (and it helps signal a willingness to do so).

Put another way, the United States appears to be placing hedged bets about what the future strategic environment will look like and how best to position itself to operate and compete in it. On balance, for example, the United States may prefer relatively clear standards with respect to cyber-actions that have immediate destructive effects—at least clear enough to justify armed response or deterrence to activities or scenarios deemed threatening—while at the same time preferring some permissive haziness with respect to intelligence collection and its own countermeasures in cyberspace. Such a posture allows the United States to protect itself from hostile penetrations while also preserving some latitude for those activities in which it may be relatively strong.151 Internally, that clarity facilitates planning for contingencies and deliberation about options;152 externally, it may help articulate and deter the crossing of red lines.153

In trying to explain what may be driving the U.S. interpretation, this Article is neither affirming nor denying this strategic logic, which is contingent on future capabilities and vulnerabilities that are both highly uncertain and shrouded in secrecy. Rather, it is trying to uncover and scrutinize some of the underlying assumptions.

There are several strategic reasons for the United States to be cautious in considering interpretations that expand narrow definitions of “force” and “attack” so that they include potentially broad categories of cyber-attacks— risks that are often not acknowledged or addressed in discussions of the U.S. interpretive trajectory. For one thing, the United States has generally defeated efforts by other states to interpret Articles 2(4) and 51 expansively to include economic coercion and other forms of political subversion.154 In thinking about the Charter regime as a whole, therefore, the United States may not want to reopen those debates. Cyber-attacks can allow state and nonstate actors to inflict massive harm without resort to arms, but that has long been true of many other instruments, including economic and financial means, covert subterfuge, and other widely used instruments. In that regard, one advantage of promoting legal regulation of cyber-attacks through a new treaty or international agreement instead of through Charter interpretation is that such efforts would have little if any effect on broader Charter law. An advantage, however, to working through Charter interpretation rather than new agreements is that Charter law can evolve incrementally and begin shaping international actors’ expectations through unilaterally initiated state practice without having to reach consensus (the difficulties of which are discussed in the next Section).

Depending on the relative risk of different types of future cyber-attack scenarios, it might also be in the United States’s strategic interest to legally delink cyber-activities from armed force instead of defining force by reference to effects, or at least to impose extremely high legal thresholds for treating cyberattacks equivalent to force or armed attack, in order to reduce the chances of military escalation from cyber-activities.155 As capabilities proliferate among state and nonstate actors to conduct various sorts of malicious, hostile, or intelligence-gathering activities in cyberspace, any normative constraints that come from treating some cyber-attacks as force prohibited by Article 2(4) and any deterrence value of treating them as armed attacks triggering self-defense rights under Article 51 might be outweighed by the dangers of lowering legal barriers to military force in a wider range of circumstances.156 That is, the value of promoting a right of armed self-defense against cyber-attacks may turn out to be quite low—since, among other things, it may be difficult to sufficiently prove one’s case publicly in justifying military responses—while doing so may introduce greater security instability to the international system by eroding normative constraints on military responses to nonmilitary harms.157

As the following Section explores, it is very difficult to assess these risk balances because the global security environment is shifting dramatically and unpredictably. Moreover, even if the United States could assess the risks accurately, other states may be operating under different sets of strategic assumptions about that future.

C. Divergent Interests and Implications for Charter Interpretation

Assuming the United States decides firmly on a legal interpretation going forward, the redrawing of legal lines on a map of inequitably distributed power and vulnerabilities would create winners and losers and would make it difficult to reach agreement on new legal boundaries, whether through interpretive evolution of the U.N. Charter or new conventions.158 In thinking about legal interpretations of Articles 2(4) and 51, success therefore depends on the ability of proponents to articulate and defend their legal lines using combinations of traditional and new forms of power for deterrence, self-defense, enforcement, and influence.

Again, one should not divorce analysis of any proposed content of Articles 2(4) and 51 from the processes by which it is interpreted, reinterpreted, enforced, and reinforced.159 The likely factual ambiguity surrounding cyberattacks and the pressures to take aggressive responsive or escalatory measures more quickly than those facts can be resolved may sometimes require strategic and military decisionmaking amid legal gray zones. Moreover, as involved states marshal their arguments amid these moves and countermoves, and as they consider their long-term interests, they may also calculate differently what Stone calls “the expected value . . . of built-in [legal] ambiguities as future political weapons.”160

That is, even if states widely share a common, minimum interest in restricting some cyber-attacks, states may have divergent interests regarding specific substantive content as well as the desired degree of clarity in the law. Salient differences will likely stem from asymmetries of geostrategic ambitions, internal and external commitment to legal norms generally, and the nature and extent of public-private institutional relationships.161

In contrast to the United States, some states that are developing offensive cyber-warfare capabilities (such as North Korea, according to many experts) are non-status-quo powers or aspiring regional powers,162 and they may prefer legal ambiguity as to cyber-attacks or narrow interpretations of Article 51 that would allow them—if they resort to cyber-attacks—to portray themselves as victims of any responsive military strikes.163 Offensive cyber-capabilities have the potential to shift or upset international balances of power, because some states are more vulnerable than others to cyber-attack (in terms of capacity to block actions as well as to tolerate or withstand them), and attacks could have a disproportionately large impact on countries or militaries that have a higher reliance on networked information systems.164 Developing an offensive cyberwarfare capability is likely to be less expensive in resources and diplomatic costs than competing economically or militarily with much stronger states, though legal flexibility or constraints could alter that calculus.165 On the other hand, some small states that are unlikely to develop sophisticated offensive or defensive systems may advocate international legal interpretations or new agreements that are very restrictive of cyber-attacks and define attacks broadly, seeing themselves as highly reliant on protective norms.166 Individually, though, they will have little power to promote those principles.

Like the United States, other major actors may have much to lose from cyber-attacks. However, they may calculate their short- and long-term strategic interests with respect to cyber-warfare and its regulation differently than the United States, in light of their own matrix of offensive and defensive capabilities, public-private institutional relationships, and asymmetries in the ways international law constrains different actors.167 Russia, for example, has proposed to the United Nations a draft statement of principles that would prohibit the development, creation, and use of cyber-attack tools. Meanwhile, though, Russia is engaged in developing cyber-attack capabilities,168 and some analysts are skeptical of Russia’s sincerity in proposing cyber-arms control agreements, especially given the difficulties of verifying them.169 China likely sees cyber-warfare capabilities as a way of equalizing the conventional military superiority of the United States,170 so it may be reluctant to concede legally “disarming” interpretations, at least without some reciprocal benefit or legal concession. Russia and China, which, as mentioned earlier, both reportedly exploit informal relationships with private actors (i.e., “citizen hackers”) to conduct attacks and collect intelligence in cyberspace, may also incline toward legal doctrine that makes it difficult to impute private cyber-actions to governments.171 Meanwhile, some European states have approached the legal relationship between cyber-attacks and force cautiously, perhaps because of general concerns about military escalation of crises and divergent strategic assessments among themselves.172

Differences in internal politics, ideology, and government control over information will also shape state interests in competing interpretations of Charter norms. With echoes of debates from prior eras,173 various types of states are likely to view cyber-threats differently and to distinguish offensive attacks from defensive measures differently. For instance, some states that tightly control information, including major powers like China, are especially concerned about internal political dissent and might therefore define what the United States sees as “Internet freedom” as a threat to vital security interests. Efforts to crack down on what they (or other states that exercise strong state control over Internet content) may view as defensive measures against hostile subversion may be viewed by the United States (or other states that value and promote free speech) as hostile, offensive measures.174 It is hard to envision a state in China’s position strongly endorsing or standing behind U.S. visions for international legal regulation of cyber-attacks without some unlikely concessions by the United States.175

From a policy standpoint, this should sound another cautionary note about efforts to build international legal consensus about cyber-attacks and the use of force, whether through Charter interpretation or new agreements. Emergent U.S. government inclinations toward effects-based interpretations of the Charter may be legally reasonable and protective of some core U.S. interests, as well as widely shared foreign interests. But even if they help in the short term to manage competing risks of too much or too little authority to employ cyberattacks, or too much or too little leeway to resort to armed self-defense in response, a coherent legal strategy can only be forged and advanced in the long term if it is integrated effectively with broader diplomacy and security strategy, including efforts to build and sustain offensive, defensive, deterrent, and intelligence capabilities—while others do the same based on a different set of objectives, capabilities, vulnerabilities, and constraints.

International law doesn’t change state action—no compliance and selective interpretation of the law.

Posner 12 (Eric, law prof, Slate, “Obama’s Drone Dilemma”, Oct. 8, 2012, http://www.slate.com/articles/news\_and\_politics/view\_from\_chicago/2012/10/obama\_s\_drone\_war\_is\_probably\_illegal\_will\_it\_stop\_.single.html, ZBurdette)

The Wall Street Journal recently reported on debates within the Obama administration about the legality of the drone war in Pakistan. State Department legal adviser Harold Koh, the former dean of Yale Law School and even more former darling of the left for his criticisms of the Bush administration’s aggressive theories of executive power, plays a prominent role in them. Koh apparently concluded that the drone war “veers near the edge” of illegality but does not quite tumble over it.

That is a questionable judgment. The U.N. Charter permits countries to use military force abroad only with the approval of the U.N. Security Council, in self-defense, or with the permission of the country in which military force is to be used. The U.N. Security Council never authorized the drone war in Pakistan. Self-defense, traditionally defined to mean the use of force against an “imminent” armed attack by a nation-state, does not apply either, because no one thinks that Pakistan plans to invade the United States. That leaves consent as the only possible legal theory.

But Pakistan has never consented to the drone war. Publicly and officially the country has opposed it. Before the raid that killed Osama bin Laden in May 2011, the CIA sent a fax every month to Pakistan’s Inter-Services Intelligence agency that would identify the airspace in which drones would be sent. The ISI would send back an acknowledgment that it had received the fax, and the U.S. government inferred consent on the basis of the acknowledgments. But after the raid, the ISI stopped sending back the acknowledgments.

Now what to do? The administration argues that consent can still be inferred despite the unanswered faxes. The reason is that “the Pakistani military continues to clear airspace for drones and doesn’t interfere physically with the unpiloted aircraft in flight”—meaning that Pakistan does not shoot down the drones or permit private aircraft to collide with them.

We might call this “coerced consent.” Consider it this way: You walk into a jewelry store and the proprietor announces that he will deem you to have consented to the purchase of a diamond tiara for $10,000, despite all your protests to the contrary, unless you use physical force to stop him as he removes your wallet from your pocket. Imagine further that he’s 7 feet tall and weighs 400 pounds. This is what a Pakistani official meant when he told the Wall Street Journal that shooting down a drone would be “needlessly provocative.” He meant that such an action would risk provoking retaliation from the United States, a risk that Pakistan cannot afford to take. Because Pakistan lies prostrate and endures the pummeling rather than makes a futile effort to stop it, it is deemed to consent to the bombing of its own territory.

But don’t blame government lawyers like Koh for devising this theory. International law lacks the resources for constraining the U.S. government. Koh knows this now if he did not before. Since he built his academic career on the claim that international law can and should be used to control nation-states and harshly criticized the Bush administration for violating international law, this must have been a bitter pill to swallow. (Though he has swallowed so many bitter pills that perhaps he has lost his sense of taste: The man who told the Senate at the end of the Bush administration that the United States must “unambiguously reassert our historic commitments to human rights and the rule of law as a major source of our moral authority” has backed away from his earlier opposition to expansive war powers, targeted killing, military commissions, and military detention.)

The weakness of international law governing the use of military force goes back to the signing of the U.N. Charter in 1945. The founders understood that a simple rule prohibiting the use of military force except in self-defense, or with the consent of another state, would not be adequate for regulating war. But they could not draft a code complex enough to anticipate all the contingencies that might justify war. Instead they set up the Security Council and reasoned that this body could determine when war might be justified for purposes other than self-defense. But the Security Council was frozen first by the Cold War rivalry between the United States and the Soviet Union, and then the cold peace rivalries between the United States, Russia, and China. It has authorized only two wars since its inception (the Korean War and the first Iraq War; it also retroactively approved the U.S. invasion of Afghanistan in 2001).

Needless to say, there have been dozens of wars since 1945. Participants have included countries as diverse as China, the Soviet Union, India, Pakistan, the United Kingdom, Vietnam, Iran, Iraq, Egypt, Israel, and Argentina. Even the supposedly pacific European countries participated via NATO in several of these wars. The United States has on several occasions justified wars (for example, in Kosovo in 1999, Libya in 2011) as humanitarian interventions—a principle that can be found nowhere in the U.N. Charter but enjoys some international support. In other cases, including current drone operations in Pakistan, the United States has invoked a new idea of the “unable or unwilling” country, one that outside powers can invade because that country cannot prevent terrorists located on its territory from launching attacks across its borders. But most U.S. wars can be fit into these two categories only with difficulty. Those wars are undertaken to shut down a destabilizing or dangerous regime, one that typically has used violence to keep itself in power. One can put the second Iraq War in this category, as well as the Panama intervention in 1990, the interventions in Yugoslavia in the 1990s, and the intervention in Granada in 1983. During the Cold War, the United States also often evaded the U.N. prohibition on interstate war by funding and training a domestic insurgency.

The U.N. Charter does not permit states to use military force to unilaterally address long-term threats in this way. It is too easy for states to characterize other states as long-term threats regardless of whether they are. And yet this omission rendered the charter unworkable, because all states must take long-term threats seriously, whether or not the members of the Security Council can be persuaded or bribed to agree with them.

Government lawyers like Koh must scramble to revise their interpretation of international law so as to keep up with the new events that justify, in the eyes of the president, a military intervention. The “coerced consent” doctrine, the “unable and unwilling” doctrine, and the exception for humanitarian intervention all whittle away at whatever part of the law on United Nations use of force blocks U.S. goals. If the United States ever decides to invade Iran in order to prevent it from acquiring nuclear weapons, expect a new doctrine to take shape, perhaps one that emphasizes the unique dangers of nuclear weapons and Iran’s declared hostility toward a nearby country.

It is curious that there is not a global outcry about the illegality of the wars in Pakistan or Libya, as there was about the illegality of the recent war in Iraq, which the Bush administration dubiously justified on the basis of Iraq’s violations of earlier U.N. resolutions that had suspended hostilities after the first Iraq War. Maybe the world doesn’t care as much about Pakistan, which has no oil. Or maybe people have finally realized that the United States, which has been almost continuously at war since the collapse of the Soviet Union, will not be swayed by legal arguments. A powerful army is too useful not to use, whether you are a Republican president or a Democratic one.

Legal limitations on war powers not key and a laundry list of military invasions thump their internal link.

Posner 13 (Eric, law prof, “The U.S. Has No Legal Basis to Intervene in Syria”, Aug. 28, 2013, http://www.slate.com/articles/news\_and\_politics/view\_from\_chicago/2013/08/the\_u\_s\_has\_no\_legal\_basis\_for\_its\_action\_in\_syria\_but\_that\_won\_t\_stop\_us.html, ZBurdette)

Inter arma enim silent leges, said the Romans—in times of war, the law falls silent. But ours is a chattier society. Rather than keep silent, our laws speak loudly about war. We just don’t follow them—as the U.S. military intervention in Syria is about to show.

Press reports say that President Obama has **ordered his lawyers to supply him with a legal justification** for a military assault on Syria, and unnamed officials have cited the Geneva Protocol, the Chemical Weapons Convention, the Kosovo precedent, and the so-called Responsibility to Protect doctrine. They have not cited the United Nations Charter, which flatly bans military interventions without Security Council approval, which the United States cannot obtain because of Russian and Chinese opposition.

The Geneva Protocol of 1925 (which Syria ratified) and the Chemical Weapons Convention of 1993 (which Syria has not ratified) ban the use of chemical weapons, but do not authorize countries to attack other countries that violate these treaties. The United States has no more authority to attack Syria for violating these treaties than it does to bomb Europe for giving import preferences to Caribbean banana producers in violation of international trade law. At one time, countries could use military force as “countermeasures” against treaty violators, but only against violators that harmed the country in question—and Syria has not used chemical weapons against the United States—but in any event, that rule has been superseded by the U.N. Charter.

The Kosovo precedent refers to the 1999 military intervention in Serbia, launched to stop a campaign of ethnic cleansing against people living in that region of Serbia. Then, too, the United States failed to obtain approval from the Security Council but attacked anyway. It’s odd to claim the Kosovo attack as a precedent, as it was widely regarded as illegal at the time and afterward.

But most people, or at least Westerners, believed that the Kosovo intervention was morally justified because it stopped a massacre, and efforts were made to carve out an exception to the U.N. rules, so that a “humanitarian intervention” would be lawful even without Security Council approval. That effort failed because people believed it would be too easy for countries to use humanitarian intervention as a pretext for attacking countries for other reasons. After all, humanitarian conditions are bad in nearly all countries that someone might like to invade. Instead, an international conference hammered together a compromise that all countries have a “Responsibility to Protect” their own citizens and citizens of other countries. But this idea was never sanctified in a treaty and is not law.

The most honest thing to do would be to admit that the international law on the use of force is defunct, as professor Michael Glennon has argued. Virtually all major countries have broken the rules **from time to time, even the saintly European countries** that joined in the Kosovo intervention. The U.S. has ignored the U.N. rules on numerous occasions**—Vietnam, Grenada, Panama, Kosovo, the second Iraq War, and** the 2011 war in **Libya**, where it secured an authorization to stop massacres of civilians but violated its terms by seeking regime change. But the U.S. government does not repudiate the U.N. rules because it wants other countries to comply with them.

On the domestic front, things are hardly better. The Constitution gives Congress, not the executive, the power to declare war, and at present writing, the administration seems unlikely to ask Congress for authorization lest it say no. This too would be a repeat of the Libya intervention, which lacked congressional authorization. To avoid the impression that the president can go to war whenever he wants, pretty much in clear violation of the founders’ intentions, the executive branch has invented a number of largely phony limits on executive military action. At one point the theory was that the executive may send military forces anywhere in the world in order to discharge its responsibility to protect Americans or American property, a theory that was used to justify the use of military force without congressional authorization in Somalia in 1992–1993. One might wonder whether such a theory imposes any limits; one might ask, “In what country are there no Americans or American property that could be protected?” Syria, it turns out.

No one alleges that the Syrian government poses a threat to Americans or American property, so the Obama administration can’t fall back on that theory, and doesn’t seem inclined to. But the executive branch claims the authority to use military intervention to protect the “national interest,” and it is not hard to find a national interest at stake. Ironically, the Justice Department’s Libya opinion identified “maintaining the credibility of the United Nations Security Council and the effectiveness of its actions to promote international peace and security” as one of the national interests justifying military intervention without congressional approval. Don’t expect a repeat of that argument in the Syria opinion. The other national interest was that of promoting regional stability—also not a good one here either, since no one seems to think that lobbing some cruise missiles onto Syrian soil will promote regional stability. Most likely the government will argue that there is a (heretofore ignored) national interest in deterring the use of chemical weapons as well as in protecting foreign civilians from massacres. With “national interest” so capaciously understood, it is clear that the president will always be able to find a national interest justifying a military intervention, so there are no constitutional constraints on his power to initiate military intervention.

Congress tried to bring the executive under control back in 1973 by enacting the War Powers Resolution, which can be read to implicitly authorize the use of military force as long as the president reports back to Congress and withdraws forces after 60 days unless Congress gives authorization in the interim. In 2011 President Obama ignored a Justice Department opinion that he must end the use of force in Libya, instead obtaining a compliant legal opinion from White House Counsel Robert Bauer and State Department Legal Adviser Harold Koh, who argued that the bombings and killings in Libya did not amount to “hostilities” and so did not trigger the withdrawal provision in the War Powers Resolution. In another indication of the administration’s respect for Congress, earlier this month the administration refused to call the coup in Egypt a coup so as to evade a statute that requires a cutoff of foreign aid to countries in which a military coup overthrows a democratically elected leader.

One can be cynical or realistic. I prefer the latter. The Romans had it right: It is not realistic to put legal constraints on war powers. Law works through general prospective rules that apply to a range of factual situations. International relations and national security are **too fluid and unpredictable to be governed by a set of legal propositions** that command general assent secured in advance. **Laws governing war make us feel more secure but they** don’t actually make us more secure. So while it is satisfying to fling the charge of hypocrisy at the president and his lawyers, and we might disagree about the wisdom of an attack on Syria, let’s just hope that when they invoke the law, they don’t actually believe what they are saying.

Plan doesn't solve norms -

Unclear retaliation policy

Harris 7/15/13

Shane Harris, Senior Writer, Foreign Policy magazine; Author of The Watchers: The Rise of America's Surveillance State, Foreign Policy, July 15, 2013, "Meet the Air Force's Top Cyberwarrior", http://killerapps.foreignpolicy.com/posts/2013/07/01/air\_forces\_cyber\_chief\_for\_frank\_discussion\_about\_rules\_of\_network\_war

The general who oversees the Air Force's online warriors says there needs to be a "frank discussion" among nations to keep misunderstandings in cyberspace from escalating into a broader conflict. "We still have to get our hands around deterrence," said Lt. Gen. Michael Basla, the Air Force's chief of information dominance and its chief information officer, in an interview with Foreign Policy. There are no hard lines that tell an adversary what response he can expect after taking action against a U.S. network, Basla explained. Nor is there a full understanding of "signaling" by a cyber-adversary -- that is, how to tell the difference between an action that may look provocative, but is actually more benign.

Basla's title reflects how priorities have changed for the Air Force in a short period of time. In June 2012, he became the first chief information officer (CIO) to hold that second title putting him in charge of "information dominance" -- read cyber-operations. In many organizations, the CIO is the guy in charge of keeping the network running. He's like the plumber. Basla's a kind of plumber too, but he's figuring out how to take out an adversary's networks, at the same time that he tries to defend the Air Force's.

Basla's comments about deterrence echo those of other cybersecurity experts who say that there is currently no cyber-analog to the strategy of nuclear deterrence, whereby nations understand what aggressive steps they might take but still stop short of a full exchange of nuclear weapons.

No definitions

Kaminski 10

Ryan T. Kaminski, Columbia University School of International and Public Affairs, “ESCAPING THE CYBER STATE OF NATURE: CYBER DETERRENCE AND INTERNATIONAL INSTITUTIONS,” NATO Cooperative Cyber Defence Center of Excellence, published 2010, http://www.ccdcoe.org/publications/2010proceedings/Kaminski%20-%20Escaping%20the%20Cyber%20State%20of%20Nature%20Cyber%20deterrence%20and%20International%20Institutions.pdf

2.1 LACK OF A UNIVERSALLY ACCEPTED CYBERWARFARE LEXICON Anyone reading lay articles, think-tank studies, published manuscripts, or even government reports on cyber attacks is likely to ﬁnd a dizzying array of terms sometimes referring to the same concept. For example, should a DDoS attack that causes disruptions to a government website, yet does not steal any sensitive information, be considered an act of cyberwar, cyber espionage, or cyber vandalism? The implications of lacking a generally accepted vocabulary in this area are twofold. First, depending on what lexical framework is used, international and customary law can be interpreted to permit vastly different reactions to the same cyber attack. For example, if two states have contrasting lexicons concerning cyberwarfare, one could view a cyber attack as an act of war, while the other could conceptualize it merely as an act of cyber vandalism (“Marching Oﬀ,” 2008). Second, given that some states even lack a universally accepted cyber glossary among their various domestic civilian and military agencies, the possibility of misinterpreting a potential cyber attack on the national level also remains high (Shanker & Markoff, 2009). Looking at the Estonian and Georgian cases, this problem is uniquely apparent. Tohn (2009), for one, hyperbolizes the attacks against both states as “cyber-blitzkriegs,” regardless of such a term’s connotation with an all-out military attack from World War II (p. 17). Former US Deputy Assistant Secretary of Defense Peter Brookes (2008) even classiﬁes the attack on Estonia as a “pre-emptive digital strike” despite the lack of any signiﬁcant evidence that Estonia was planning a cyber attack on Russia. Jaak Aaviksoo, Estonia’s Defense Minister, also declared that the cyber attack against his country “cannot be treated as hooliganism, but has to be treated as an attack against the state” (“Marching Oﬀ,” 2008). Even though Estonia did not end up invoking Article V of the NATO charter which commits states to treat an attack on one member as an attack on themselves, the defense minister’s comments nonetheless illuminate major problems associated with the lack of a comprehensive cyberwarfare lexicon. While Estonia did construct a NATO-sponsored facility in its capital to study cyber security, this also may do little good if non-NATO members like China and Russia are relying upon an entirely different cyber language.

## cyber adv

Executive flexibility is key to effective offensive cyber and deterrence—norms develop out of a policy equilibrium, which solves the aff

Bradbury 11 (Steven – partner @ Dechert, LLP, “The Developing Legal Framework for Defensive and Offensive Cyber Operations” March 2011, Cybersecurity: Law, Privacy, and Warfare in a Digital World, Harvard National Security Journal, Vol. 2)

Conclusion. So here’s my thesis: To my view, the lack of clarity on certain of these issues under international law means that with respect to those issues, **the President is free to decide**, as a policy matter, where and how the lines should be drawn on **the limits of traditional military power** in the sphere of cyberspace. For example, that means that within certain parameters, the President could decide when and to what extent military cyber operations may target computers located outside areas of hot fighting that the enemy is using for military advantage. And when a cyber attack is directed at us, the President can decide, as a matter of national policy, whether and when to treat it as an act of war.

The corollary to all this is that in situations where the customs of war, in fact, are not crystallized, **the lawyers at the State Department and the Justice Department shouldn’t make up new red lines** — out of some aspirational sense of what they think international law ought to be — that end up putting dangerous limitations on the options available to the United States. Certainly, the advice of lawyers is always important, especially so where the legal lines are established or firmly suggested. No one would contend that the laws of war have no application to cyber operations or that cyberspace is a law free zone. But it’s not the role of the lawyers to make up new lines that don’t yet exist in a way that preempts the development of policy. 14

In the face of this lack of clarity on key questions, some advocate for the negotiation of a new international convention on cyberwarfare — perhaps a kind of arms control agreement for cyber weapons. I believe there is no foreseeable prospect that that will happen. Instead, the outlines of accepted norms and limitations in this area will develop through the practice of leading nations. And the policy decisions made by the United States in response to particular events will have great influence in shaping those international norms. I think that’s the way we should want it to work.

Restraints ensure the US loses the battle

Stewart Baker, Visiting Fellow at the Hoover Institution, 12 [“Law and Cyberwar - The Lessons of History,” Patriots Debate: Contemporary Issues in National Security Law, Chapter 9: Cyberwar, http://www.americanbar.org/groups/public\_services/law\_national\_security/patriot\_debates2/the\_book\_online/ch9/ch9\_ess1.html]

Lawyers don’t win wars.¶ But can they lose a war? We’re likely to find out, and soon. Lawyers across the government have raised so many show-stopping legal questions about cyberwar that they’ve left our military unable to fight, or even plan for, a war in cyberspace.¶ No one seriously denies that cyberwar is coming. Russia may have pioneered cyber attacks in its conflicts with Georgia and Estonia, but cyber weapons went mainstream when the developers of Stuxnet sabotaged Iran’s Natanz enrichment plant, proving that computer network attacks can be more effective than 500-pound bombs. **In war, weapons that work get used again**.¶ Unfortunately, it turns out that cyber weapons may work best against civilians. The necessities of modern life—pipelines, power grids, refineries, sewer and water lines—all run on the same industrial control systems that Stuxnet subverted so successfully. These systems may be even easier to sabotage than the notoriously porous computer networks that support our financial and telecommunications infrastructure.¶ **No one has good defenses against such attacks.** The hackers will get through**.¶** Even very sophisticated network defenders—RSA, HBGary, even the Department of Defense (DOD) classified systems—have failed to keep attackers out. Once they’re in, attackers have stolen the networks’ most precious secrets. But they could just as easily bring the network down, possibly causing severe physical damage, as in the case of Stuxnet.¶ So as things now stand, a serious cyber attack could leave civilians without power, without gasoline, without banks or telecommunications or water—perhaps for weeks or months. If the crisis drags on, deaths will multiply, first in hospitals and nursing homes, then in cities and on the road as civil order breaks down. It will be a nightmare. And especially for the United States, which has trusted more of its infrastructure to digital systems than most other countries have.¶ We’ve been in this spot before. As General William Mitchell predicted, airpower allowed a devastating and unprecedented strike on our ships in Pearl Harbor. We responded with an outpouring of new technologies, new weapons, and new strategies.¶ Today, the threat of new cyber weapons is just as real, but we have responded with an outpouring, not of technology or strategy but of law review articles, legal opinions, and legal restrictions. Military lawyers are tying themselves in knots trying to articulate when a cyber attack can be classified as an armed attack that permits the use of force in response.6 State Department and National Security Council lawyers are implementing an international cyberwar strategy that relies on international law “norms” to restrict cyberwar.7 CIA lawyers are invoking the strict laws that govern covert action to prevent the Pentagon from launching cyber attacks.8 Justice Department lawyers are telling our military that it violates the law of war to do what every cyber criminal has learned to do—cover their tracks by routing attacks through computers located in other countries.9 And the Air Force recently surrendered to its own lawyers, allowing them to order that all cyber weapons be reviewed for “legality under [the law of armed conflict], domestic law and international law” before cyberwar capabilities are even acquired.10 (And that’s just the lawyers’ first bite at the apple; the directive requires yet another legal review before the weapons are used.)11¶ The result is predictable, and depressing. Top Defense Department officials recently adopted a cyberwar strategy that simply omitted any plan for conducting offensive operations.12 Apparently, they’re still waiting for all these lawyers to agree on what kind of offensive operations the military is allowed to mount.¶ \* \* \*¶ I have no doubt that the lawyers think they’re doing the right thing. Cyberwar will be terrible. If the law of war can stave off the worst civilian harms, they’d argue, surely we should embrace it. There’s just one problem: That’s exactly what we tried when airpower transformed war.¶ And we failed.¶ In the first half of the 20th century, the airplane did for warfighters what information technology has done in the last quarter of a century. Like cyber attacks, airpower was first used to gather intelligence and not to fight. Perhaps for this reason, there was never a taboo about using either airpower or cyber weapons. By the time officials realized just how ugly these weapons could be, the cat was already out of the bag¶ By the 1930s, though, everyone saw that aerial bombing would reduce cities to rubble in the next war. We have trouble today imagining how unprecedented and terrible airpower must have seemed at this time. Just a few years earlier, the hellish slaughter where armies met in the trenches of World War I had destroyed the Victorian world; now airpower promised to bring that hellish slaughter to the home front.¶ Former Prime Minister Stanley Baldwin summed up Britain’s strategic position in 1932 with a candor no American leader has dared to match in talking about cyberwar:¶ I think it is well also for the man in the street to realize that there is no power on earth that can protect him from being bombed, whatever people may tell him. The bomber will always get through. . . . The only defence is in offence, which means that you have got to kill more women and children more quickly than the enemy if you want to save yourselves.13¶ The British may have been realists about air war, but Americans still hoped to head off the nightmare. The American tool of choice was international law. (Some things never change.) When war broke out on September 1, 1939, President Franklin D. Roosevelt sent a cable to all the combatants seeking express limits on the use of airpower and expressing his view that:¶ [R]uthless bombing from the air of civilians in unfortified centers of population . . . has sickened the hearts of every civilized man and woman, and has profoundly shocked the conscience of humanity. . . . I am therefore addressing this urgent appeal to every government which may be engaged in hostilities publicly to affirm its determination that its armed forces shall in no event, and under no circumstances, undertake the bombardment from the air of civilian populations or of unfortified cities. . . .14¶ President Roosevelt had a pretty good legal case. The Hague Conventions on the Law of War, adopted just two years after the Wright Brothers’ first flight, declared that in bombardments, “all necessary steps should be taken to spare as far as possible edifices devoted to religion, art, science, and charity, hospitals, and places where the sick and wounded are collected, provided they are not used at the same time for military purposes.”15 The League of Nations had recently declared that, in air war, “the intentional bombing of civilian populations is illegal.”16¶ But FDR didn’t rely just on law. He asked for a public pledge that would bind all sides.17 Remarkably, he got it. The horror of aerial bombardment ran so deep in that era that England, France, Germany, and Poland all agreed—before nightfall on the same day.18¶ What’s more, they tried to honor their pledges. In a June 1940 order for Luftwaffe operations against Britain, Hermann Göring “stressed that every effort should be made to avoid unnecessary loss of life amongst the civilian population.”19¶ It began to look like a great victory for the international law of war. All sides had stared into the pit of horrors that civilian bombing would open up. And all had stepped back.¶ It was exactly what the lawyers and diplomats now dealing with cyberwar hope to achieve.¶ But as we know, that’s not how this story ends. On the night of August 24, a Luftwaffe air group made a fateful navigational error. Aiming for oil terminals along the Thames, they miscalculated, instead dropping their bombs in the civilian heart of the city of London.¶ It was a mistake. But that’s not how Prime Minister Winston Churchill saw it. He insisted on immediate retaliation. The next night, British bombers hit targets in Berlin for the first time. The military effect was negligible, but the political impact was profound. Göring had promised that the Luftwaffe would never allow a successful attack on Berlin. The Nazi regime was humiliated, the German people enraged. Ten days later, Hitler told a wildly cheering crowd that he had ordered the bombing of London: “Since they attack our cities, we will extirpate theirs.”20¶ The Blitz was on.¶ In the end, London survived. But the extirpation of enemy cities became a permanent part of both sides’ strategy. No longer an illegal horror to be avoided at all costs, the destruction of enemy cities became deliberate policy. Later in the war, British strategists would launch aerial attacks with the avowed aim of causing “the destruction of German cities, the killing of German workers, . . . the disruption of civilized life throughout Germany . . . the creation of a refugee problem on an unprecedented scale, and the breakdown of morale both at home and at the battle fronts.”21¶ The Hague Conventions, the League of Nations resolution, even the explicit pledges given to President Roosevelt—all these “norms” for the use of airpower had been swept away by the logic of the technology and the predictable psychology of war.¶ \* \* \*¶ So, why do today’s lawyers think that their limits on cyberwar will fare better than FDR’s limits on air war?¶ It beats me. If anything, they have a much harder task. Roosevelt could count on a shared European horror at the aerial destruction of cities. He used that to extract an explicit and reciprocal understanding from both sides as the war was beginning. We have no such understanding, indeed no such shared horror. Quite the contrary, for some of our potential adversaries, cyber weapons are uniquely asymmetric—a horror for us, another day in the field for them. It doesn’t take a high-tech infrastructure to maintain an army that is ready in a pinch to live on grass.¶ What’s more, cheating is easy and strategically profitable. American compliance will be enforced by all those lawyers. Our adversaries can ignore the rules and say—hell, they are saying—”We’re not carrying out cyber attacks. We’re victims, too. Maybe you’re the attacker. Or maybe it’s Anonymous. Where’s your proof?”¶ Even if all sides were genuinely committed to limiting cyberwar, as all sides were in 1939, we’ve seen that the logic of airpower eventually drove all sides to the horror they had originally recoiled from. Each side felt that it had observed the limits longer than the other. Each had lawyerly justifications for what it did, and neither understood or gave credence to the other’s justifications. In that climate, all it took was a single error to break the legal limits irreparably.¶ And error was inevitable. Bombs dropped by desperate pilots under fire go astray. But so do cyber weapons. Stuxnet infected thousands of networks as it searched blindly for Natanz. The infections lasted far longer than intended. Should we expect fewer errors from code drafted in the heat of battle and flung at hazard toward the enemy?¶ Of course not. But the lesson for the lawyers and the diplomats is stark: Their effort to impose limits on cyberwar is almost certainly doomed.¶ No one can welcome this conclusion, at least not in the United States. We have advantages in traditional war that we lack in cyberwar. We are not used to the idea that launching even small wars on distant continents may cause death and suffering here at home. That is what drives the lawyers. They hope to maintain the old world. But they’re driving down a dead end.¶ If we want to defend against the horrors of cyberwar, we need first to face them, with the candor of a Stanley Baldwin. Then we need to charge our military strategists, not our lawyers, with constructing a cyberwar strategy for the world we live in, not the world we’d like to live in.¶ That strategy needs both an offense and a defense. The offense must be powerful enough to **deter every adversary with something to lose in cyberspace**, and so it must include a way to identify our attacker with certainty. The defense, too, must be realistic, making successful cyber attacks more difficult and less effective because we have built resilience and redundancy into our infrastructure.¶ **Once we have a strategy for winning a** cyberwar**, we can ask the lawyers for their thoughts.** We can’t do it the other way around.

Consultation won’t be genuine – the president will just lie to get what he wants

Grimmett 8 [Grimmett; 24 April 2008; “WAR POWERS FOR THE 21ST CENTURY: THE EXECUTIVE BRANCH PERSPECTIVE HEARING BEFORE THE SUBCOMMITTEE ON INTERNATIONAL ORGANIZATIONS, HUMAN RIGHTS, AND OVERSIGHT OF THE COMMITTEE ON FOREIGN AFFAIRS”; House of Representatives (110th Congress), Second Session; Serial No. 110-168; Printed for the use of the Committee on Foreign Affairs; http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg41989/pdf/CHRG-110hhrg41989.pdf]

Mr. GRIMMETT. I would just add one thing. We are talking about consultation, so we are talking about two branches of government. And even if you organized the committee structure or the new entity, however you want to characterize it, at this end, you are still going to confront the reality of the executive branch that has been very chary about giving information out, especially on something as sensitive as possible war activity or military operations, because of concerns about operational security and about people having the proper clearances and all that sort of thing. And even though most of the major committees that deal with foreign defense policy or intelligence have got the security clearances, the fact is there is a very, very strong reluctance on the part of the executive branch, based on past history, to even engage people on that level. So if you have a committee of 45 members, I mean, the likelihood of them wanting to engage that committee on the most sensitive operational activities that they may be contemplating is pretty slim, unless some new millennium has occurred that, based on new experiences, that we are not fully aware of.

Cyber war infeasible

Clark, MA candidate – Intelligence Studies @ American Military University, senior analyst – Chenega Federal Systems, 4/28/’12

(Paul, “The Risk of Disruption or Destruction of Critical U.S. Infrastructure by an Offensive Cyber Attack,” American Military University)

The Department of Homeland Security worries that our critical infrastructure and key resources (CIKR) may be exposed, both directly and indirectly, to multiple threats because of CIKR reliance on the global cyber infrastructure, an infrastructure that is under routine cyberattack by a “spectrum of malicious actors” (National Infrastructure Protection Plan 2009). CIKR in the extremely large and complex U.S. economy spans multiple sectors including agricultural, finance and banking, dams and water resources, public health and emergency services, military and defense, transportation and shipping, and energy (National Infrastructure Protection Plan 2009). The disruption and destruction of public and private infrastructure is part of warfare, without this infrastructure conflict cannot be sustained (Geers 2011). Cyber-attacks are desirable because they are considered to be a relatively “low cost and long range” weapon (Lewis 2010), but prior to the creation of Stuxnet, the first cyber-weapon, the ability to disrupt and destroy critical infrastructure through cyber-attack was theoretical. The movement of an offensive cyber-weapon from conceptual to actual has forced the United States to question whether offensive cyber-attacks are a significant threat that are able to disrupt or destroy CIKR to the level that national security is seriously degraded. It is important to understand the risk posed to national security by cyber-attacks to ensure that government responses are appropriate to the threat and balance security with privacy and civil liberty concerns. The risk posed to CIKR from cyber-attack can be evaluated by measuring the threat from cyber-attack against the vulnerability of a CIKR target and the consequences of CIKR disruption. As the only known cyber-weapon, Stuxnet has been **thoroughly analyzed** and **used as a model** for predicting future cyber-weapons. The U.S. electrical grid, a key component in the CIKR energy sector, is a target that has been analyzed for vulnerabilities and the consequences of disruption predicted – the electrical grid has been used in multiple attack scenarios including a classified scenario provided to the U.S. Congress in 2012 (Rohde 2012). Stuxnet will serve as the weapon and the U.S. electrical grid will serve as the target in this risk analysis that concludes that there is a low risk of disruption or destruction of critical infrastructure from a an offensive cyber-weapon because of the complexity of the attack path, the limited capability of non-state adversaries to develop cyber-weapons, and the existence of multiple methods of mitigating the cyber-attacks. To evaluate the threat posed by a Stuxnet-like cyber-weapon, the complexity of the weapon, the available attack vectors for the weapon, and the resilience of the weapon must be understood. The complexity – how difficult and expensive it was to create the weapon – identifies the relative cost and availability of the weapon; inexpensive and simple to build will be more prevalent than expensive and difficult to build. Attack vectors are the available methods of attack; the larger the number, the more severe the threat. For example, attack vectors for a cyberweapon may be email attachments, peer-to-peer applications, websites, and infected USB devices or compact discs. Finally, the resilience of the weapon determines its availability and affects its usefulness. A useful weapon is one that is resistant to disruption (resilient) and is therefore available and reliable. These concepts are seen in the AK-47 assault rifle – a simple, inexpensive, reliable and effective weapon – and carry over to information technology structures (Weitz 2012). The evaluation of Stuxnet identified malware that is “unusually complex and large” and required code written in multiple languages (Chen 2010) in order to complete a variety of specific functions contained in a “vast array” of components – **it is one of the most complex threats ever analyzed by Symantec** (Falliere, Murchu and Chien 2011). To be successful, Stuxnet required a **high** **level of technical knowledge across multiple disciplines**, a laboratory with the target equipment configured for testing, and a foreign intelligence capability to collect information on the target network and attack vectors (Kerr, Rollins and Theohary 2010). The malware also needed careful monitoring and maintenance because it could be easily disrupted; as a result Stuxnet was developed with a high degree of configurability and was upgraded multiple times in less than one year (Falliere, Murchu and Chien 2011). Once introduced into the network, the cyber-weapon then had to utilize four known vulnerabilities and four unknown vulnerabilities, known as zero-day exploits, in order to install itself and propagate across the target network (Falliere, Murchu and Chien 2011). Zero-day exploits are **incredibly difficult to find** and fewer than twelve out of the 12,000,000 pieces of malware discovered each year utilize zero-day exploits and this rarity makes them valuable, zero-days can fetch $50,000 to $500,000 each on the black market (Zetter 2011). The use of four rare exploits in a single piece of malware is “unprecedented” (Chen 2010). Along with the use of four unpublished exploits, Stuxnet also used the “first ever” programmable logic controller rootkit, a Windows rootkit, antivirus evasion techniques, intricate process injection routines, and other complex interfaces (Falliere, Murchu and Chien 2011) all **wrapped up in “layers of encryption** like Russian nesting dolls” (Zetter 2011) – including custom encryption algorithms (Karnouskos 2011). As the malware spread across the now-infected network it had to utilize additional vulnerabilities in proprietary Siemens industrial control software (ICS) and hardware used to control the equipment it was designed to sabotage. Some of these ICS vulnerabilities were published but some were unknown and **required such a high degree of inside knowledge** that there was speculation that a Siemens employee had been involved in the malware design (Kerr, Rollins and Theohary 2010). The unprecedented technical complexity of the Stuxnet cyber-weapon, along with the extensive technical and financial resources and foreign intelligence capabilities required for its development and deployment, indicates that the malware was likely developed by a nation-state (Kerr, Rollins and Theohary 2010). Stuxnet had very limited attack vectors. When a computer system is connected to the public Internet a host of attack vectors are available to the cyber-attacker (Institute for Security Technology Studies 2002). Web browser and browser plug-in vulnerabilities, cross-site scripting attacks, compromised email attachments, peer-to-peer applications, operating system and other application vulnerabilities are all vectors for the introduction of malware into an Internetconnected computer system. Networks that are not connected to the public internet are “air gapped,” a technical colloquialism to identify a physical separation between networks. Physical separation from the public Internet is a common safeguard for sensitive networks including classified U.S. government networks. If the target network is air gapped, infection can only occur through physical means – an infected disk or USB device that **must be physically introduced** into a possibly access controlled environment and connected to the air gapped network. The first step of the Stuxnet cyber-attack was to initially infect the target networks, a difficult task given the probable disconnected and well secured nature of the Iranian nuclear facilities. Stuxnet was introduced via a USB device to the target network, a method that suggests that the attackers were familiar with the configuration of the network and knew it was not connected to the public Internet (Chen 2010). This assessment is supported by two rare features in Stuxnet – having all necessary functionality for industrial sabotage fully embedded in the malware executable along with the ability to self-propagate and upgrade through a peer-to-peer method (Falliere, Murchu and Chien 2011). Developing an understanding of the target network configuration was a significant and daunting task based on Symantec’s assessment that Stuxnet repeatedly targeted a total of five different organizations over nearly one year (Falliere, Murchu and Chien 2011) with physical introduction via USB drive being the only available attack vector. The final factor in assessing the threat of a cyber-weapon is the resilience of the weapon. There are two primary factors that make Stuxnet **non-resilient**: the complexity of the weapon and the complexity of the target. Stuxnet was highly customized for sabotaging specific industrial systems (Karnouskos 2011) and needed a large number of very complex components and routines in order to increase its chance of success (Falliere, Murchu and Chien 2011). The **malware required eight vulnerabilities** in the Windows operating system **to succeed** and therefore would have failed if those vulnerabilities had been properly patched; four of the eight vulnerabilities were known to Microsoft and subject to elimination (Falliere, Murchu and Chien 2011). Stuxnet also required that two drivers be installed and required two stolen security certificates for installation (Falliere, Murchu and Chien 2011); driver installation would have failed if the stolen certificates had been revoked and marked as invalid. Finally, the configuration of systems is ever-changing as components are upgraded or replaced. There is no guarantee that the network that was mapped for vulnerabilities had not changed in the months, or years, it took to craft Stuxnet and successfully infect the target network. Had specific components of the target hardware changed – the targeted Siemens software or programmable logic controller – the attack would have failed. Threats are less of a threat when identified; this is why zero-day exploits are so valuable. Stuxnet went to great lengths to hide its existence from the target and utilized multiple rootkits, data manipulation routines, and virus avoidance techniques to stay undetected. The malware’s actions occurred only in memory to avoid leaving traces on disk, it masked its activities by running under legal programs, employed layers of encryption and code obfuscation, and uninstalled itself after a set period of time, all efforts to avoid detection because its authors knew that detection meant failure. As a result of the complexity of the malware, the changeable nature of the target network, and the chance of discovery, Stuxnet is not a resilient system. It is a fragile weapon that required an investment of time and money to constantly monitor, reconfigure, test and deploy over the course of a year. There is concern, with Stuxnet developed and available publicly, that the world is on the brink of a storm of highly sophisticated Stuxnet-derived cyber-weapons which can be used by hackers, organized criminals and terrorists (Chen 2010). As former counterterrorism advisor Richard Clarke describes it, there is concern that the technical brilliance of the United States “has created millions of potential monsters all over the world” (Rosenbaum 2012). Hyperbole aside, technical knowledge spreads. The techniques behind cyber-attacks are “constantly evolving and making use of lessons learned over time” (Institute for Security Technology Studies 2002) and the publication of the Stuxnet code may make it easier to copy the weapon (Kerr, Rollins and Theohary 2010). **However**, this is something of a zero-sum game because knowledge works both ways and cyber-security techniques are also evolving, and “understanding attack techniques more clearly is the first step toward increasing security” (Institute for Security Technology Studies 2002). Vulnerabilities are discovered and patched, intrusion detection and malware signatures are expanded and updated, and monitoring and analysis processes and methodologies are expanded and honed. Once the element of surprise is lost, weapons and tactics are less useful, this is the core of the argument that “uniquely surprising” **stratagems like Stuxnet are single-use**, like Pearl Harbor and the Trojan Horse, the “very success [of these attacks] precludes their repetition” (Mueller 2012). This paradigm has already been seen in the “son of Stuxnet” malware – named Duqu by its discoverers – that is based on the same modular code platform that created Stuxnet (Ragan 2011). With the techniques used by Stuxnet now known, other variants such as Duqu are being discovered and countered by security researchers (Laboratory of Cryptography and System Security 2011). It is obvious that the effort required to create, deploy, and maintain Stuxnet and its variants is massive and it is not clear that the rewards are worth the risk and effort. Given the location of initial infection and the number of infected systems in Iran (Falliere, Murchu and Chien 2011) it is believed that Iranian nuclear facilities were the target of the Stuxnet weapon. A significant amount of money and effort was invested in creating Stuxnet but yet the expected result – assuming that this was an attack that expected to damage production – was minimal at best. Iran claimed that Stuxnet caused only minor damage, probably at the Natanz enrichment facility, the Russian contractor Atomstroyeksport reported that no damage had occurred at the Bushehr facility, and an unidentified “senior diplomat” suggested that Iran was forced to shut down its centrifuge facility “for a few days” (Kerr, Rollins and Theohary 2010). Even the most optimistic estimates believe that Iran’s nuclear enrichment program was only delayed by months, or perhaps years (Rosenbaum 2012). The actual damage done by Stuxnet is not clear (Kerr, Rollins and Theohary 2010) and the primary damage appears to be to a higher number than average replacement of centrifuges at the Iran enrichment facility (Zetter 2011). Different targets may produce different results. The Iranian nuclear facility was a difficult target with limited attack vectors because of its isolation from the public Internet and restricted access to its facilities. What is the probability of a successful attack against the U.S. electrical grid and what are the potential consequences should this critical infrastructure be disrupted or destroyed? An attack against the electrical grid is a reasonable threat scenario since power systems are “a high priority target for military and insurgents” and there has been a trend towards utilizing commercial software and integrating utilities into the public Internet that has “increased vulnerability across the board” (Lewis 2010). Yet the increased vulnerabilities are mitigated by an increased detection and deterrent capability that has been “honed over many years of practical application” now that power systems are using standard, rather than proprietary and specialized, applications and components (Leita and Dacier 2012). The security of the electrical grid is also enhanced by increased awareness after a smart-grid hacking demonstration in 2009 and the identification of the Stuxnet malware in 2010; as a result the public and private sector are working together in an “unprecedented effort” to establish robust security guidelines and cyber security measures (Gohn and Wheelock 2010).

New diplomatic efforts will solve space

Rosen 13

Armin Rosen, an Atlantic Media fellow, The Atlantic, January 16, 2013, "Give Peace a Chance—in Space", http://www.theatlantic.com/international/archive/2013/01/give-peace-a-chance-in-space/267223/

The surest way of foreclosing on the possibility of this all-too-plausible doomsday in space is through the same kind of multilateral efforts that have stanched the spread of nuclear arms,

stigmatized the use of chemical weapons, and all but stricken catastrophic inter-state warfare from the face of the earth. The world needs a system of multilateral checks and balances that relegates war against space assets to the same political and psychic space as World War III: something that humanity, by dint of mutual self-interest and robust international institutions, has successfully turned into a geopolitical boogeyman, a bandied-about but nevertheless distant worst-case scenario.

That work has already begun. There is an international effort underway to create a "rules of the road for space" -- an update to the Outer Space Treaty that would establish guidelines for conduct in space. Secretary of State Hillary Clinton endorsed the process, if not every aspect of the still-to-be determined treaty, in a January, 2012 press release. The new treaty would be what international legal experts refer to as a "soft law:" a measure that would enshrine a set of shared principles and that might eventually gain the status of "hard" customary law, given enough time and enough precedent within the international system. For instance, the U.N. Security Council could sanction a country that violates the "rules of the road." But until such sanctions are passed, the treaty would exist without any solid coercive force -- it would be a declaration, rather than a piece of law; unspecific, and largely toothless.

In the Star Wars universe, space is a place of danger, a domain where the powerful subjugate the weak, where Executors and TIE Fighters and Death Stars impose fascistic order.

Luckily, the rules of the road aren't the only space war treaty under discussion. Both China and Russia have expressed their support for a proposed Prevention of an Arms Race in Outer Space treaty, a multilateral agreement that would be more like the 1996 Comprehensive Nuclear Test Ban treaty -- a document that places very specific restrictions on the actions of its signatories. Right now, the biggest obstacle to the treaty's passage is the United States.

The U.S., which has obstructed or simply ignored the PAROS process, is concerned that the treaty could work against its interests. Russia and China might view the accord as a means of reigning in the U.S.'s future capabilities; the U.S., meanwhile, doesn't want to give its potential rivals a veto over the development of those capabilities. As von der Dunk puts it, the U.S. doesn't want to enter into "a treaty which would hurt the most powerful nation the most."

This is a legitimate concern, especially if the U.S. observes the PAROS treaty while other, less scrupulous actors attempt to undermine it. By preventing the U.S. from developing space weaponry, PAROS could theoretically shield future actors that are actually the most dead-set on weaponizing space. Johnson-Freese of the Naval War College, who is broadly supportive of a PAROS-like treaty, says that arms control issues in space are a "series of Catch-22s. It becomes difficult if not impossible to get over definitional hurdles and verification hurdles, or it can be made to seem that way by people who don't want to get things done."

But these are problems that lie at the heart of nearly every multilateral arms treaty. The U.S. has signed quite a few of those over the years. As the country with the most assets in space, the U.S. also has the most to lose from a future space conflict.

# 2NC

## 2NC---AT: Perm Do Both---Links to War Powers

The permutation links worse

Metzger ‘9

Gillian, Professor of Law, Columbia Law School, “THE INTERDEPENDENT RELATIONSHIP BETWEEN INTERNAL AND EXTERNAL SEPARATION OF POWERS,” 59 Emory L.J. 423

Equally important, the relationship between internal and external separation of powers is reciprocal: Internal and external checks reinforce and operate in conjunction with one another. Congress needs information to conduct meaningful oversight of the Executive Branch. n94 Internal agency experts and watchdogs are important sources of that information, whether in the guise of [\*445] formal reports, studies, and testimony or informal conversations and leaks. n95 Procedural constraints within agencies can serve a similar function, alerting Congress to agency activities. n96 Internal mechanisms also reinforce congressional mandates by creating bodies of personnel within the Executive Branch who are committed to enforcing the governing statutory regime that sets out the parameters of their authority and regulatory responsibilities - and on whose expertise the functioning of these regulatory regimes often depends. n97 Courts equally depend on information and evidence compiled by agency personnel to review agency actions, and they have invoked this dependence to justify the requirement that agencies disclose underlying information and offer detailed explanations of their decisions. n98 Moreover, despite courts regularly intoning that "it [is] not the function of the court to probe the mental processes of Secretaries in reaching [their] conclusions," n99 judicial review of agency actions often appears to turn on judges' perceptions of the role politics played in decisionmaking by agency officials. n100 Evidence that decisions were made over the objections of career staff and agency professionals often triggers more rigorous review. n101 A particularly striking [\*446] suggestion of how internal checks can effect judicial review came in the recent Boumediene litigation. Just a few months after refusing to grant certiorari in order to allow the Combatant Status Review Tribunal process to proceed, the Court reversed course and granted review, apparently influenced by the concerns of military lawyers about how the tribunals were functioning. n102

## 2NC---AT: Perm Do CP---General

Authority is power vested in an agent by a principal

Oxford Dictionary of Law 2009

(“Authority,” Oxford University Press via Oxford Reference, Georgetown University Library)

authority

n.

1 Power delegated to a person or body to act in a particular way. The person in whom authority is vested is usually called an agent and the person conferring the authority is the principal.

Changing authority requires the principal – the agent only operates within the powers it has been given

Hohfeld, Yale Law, 1919

(Wesley, http://www.hku.hk/philodep/courses/law/HohfeldRights.htm)

Many examples of legal powers may readily be given. Thus, X, the owner of ordinary personal property "in a tangible object" has the power to extinguish his own legal interest (rights, powers, immunities, etc.) through that totality of operative facts known as abandonment; and-simultaneously and correlatively-to create in other persons privileges and powers relating to the abandoned object,-e. g., the power to acquire title to the latter by appropriating it. Similarly, X has the power to transfer his interest to Y, that is to extinguish his own interest and concomitantly create in Y a new and corresponding interest. So also X has the power to create contractual obligations of various kinds. Agency cases are likewise instructive. By the use of some metaphorical expression such as the Latin, qui facit per alium, facit per se\* the true nature of agency relations is only too frequently obscured. **The creation of an agency relation involves**, inter alia, **the grant of legal powers to the so-called agent**, and the creation of correlative liabilities in the principal. That is to say, one party, P, has the power to create agency powers in another party, A,-for example, the power to convey P's property, the power to impose (so called) contractual obligations on P, the power to discharge a debt owing to P, the power to "receive" title to property so that it shall vest in P, and so forth. In passing, it may be well to observe that **the term** "**authority**," so frequently used in agency cases, **is** very ambiguous and **slippery in its connotation**. **Properly employed** in the present connection, the word seems to be an abstract or qualitative term corresponding to the concrete "authorization," the latter consisting of a particular group of operative facts taking place between the principal and the agent. All too often, however, the term in question is so used as to blend and **confuse these operative facts with the powers and privileges thereby created in the agent**. A careful discrimination in these particulars would, it is submitted, go far toward clearing up certain problems in the law of agency.

The President is subject to statutory and judicial restrictions – doesn’t create them

Fisher, Scholar in Residence at The Constitution Project, 2012

(Louis, served for four decades at the Library of Congress, as Senior Specialist, Congressional Research Service, “Basic Principles of the War Power,” 2012 Journal of National Security Law & Policy 5 J. Nat'l Security L. & Pol'y 319)

The second value that the Founders embraced in the Commander-in-Chief Clause is accountability. Hamilton in Federalist No. 74 wrote that the direction of war "most peculiarly demands those qualities which distinguish the exercise of power by a single hand." The power of directing war and emphasizing the common strength "forms a usual and essential part in the definition of the executive authority." n29 Presidential leadership is essential but it cannot operate outside legislative control. **The President is subject to the rule of law**, **including statutory and judicial restrictions**.

The President has discretion within the bounds of “authority” – doesn’t affect statutory or judicial restrictions

Luna, professor of law at the University of Utah, May 2000

(Erik, 85 Iowa L. Rev. 1107, Lexis)

For present purposes, a modest definition will suffice--discretion is the power to choose between two or more courses of conduct. An official, therefore, has discretion when the boundaries of his authority leave him with the freedom to choose how to act--or not to act. n88 This discretionary power is a "residual" n89 concept, the latitude remaining after the authority and decisions of other actors have been tallied. Dworkin employed a colorful simile for discretion to capture its relative, contextual nature: "Discretion, like the hole of a doughnut, does not exist except as an area left open by a surrounding belt of restriction." n90 Using this pastry-based metaphor, imagine a box containing a single doughnut. If the box's total area represents all potential courses of conduct for a particular actor, and the doughnut symbolizes the restrictions on the actor's discretion, the region within the doughnut--the doughnut hole--delineates the totality of his discretionary power. Outside of this area, the actor has no freedom of choice; he must either act in a prescribed manner or not act at all. In other words, the actor is without discretion. Greater specificity is possible by delineating discretion within American constitutionalism. Discretion inheres in each of the three branches of government--the legislative, the executive, and the judicial. n91 The term "ex  [\*1134]  ecutive discretion," therefore, refers to the authority of executive officers to choose how to act or not to act. A variety of officials enforce federal or state laws and are appropriately deemed executive officers--the President, the Secretary of Defense, a state governor, a city mayor, the local dog catcher, and so on. Each of these officials exercises a degree of executive discretion to choose a particular course of conduct without violating the dictates of the other branches. For example, a state legislature might mandate that restaurants cook food in a "safe environment"; a state court might then interpret "safe" as referring to bacterial and viral hazards to the customers rather than the risks of the work environment to the employees. But once the legislative branch has enacted the law and the judiciary has interpreted the law (or squared it with the relevant constitutional provisions), the executive official generally has the discretion to enforce the law as seen fit. The relevant executive officer might, for instance, establish a grading system or minimum standards for the sanitary condition of restaurants. It is this residual power, the freedom to choose a particular course of conduct after the other branches have exercised their authority, that can be referred to as executive discretion. B. Criminal Justice Discretion in the Abstract Discretion can be further specified by placing it within the context of penal law. American constitutionalism has adopted a number of strategies to strike a balance between individual liberty and societal order in the criminal justice system. n92 Most notably, the federal Constitution enumerates individual rights protected from "the vicissitudes of political controversy," n93 thereby removing certain subjects as fodder for order maintenance. But American constitutionalism also secures order and liberty through the structural design of government, dividing official power between the three coordinate branches. n94 Specifically, the legislature determines what acts are criminal and subject to coercive sanction. The judiciary interprets the criminal law where necessary, nullifies those penal statutes that are deemed inconsistent with relevant constitutional provisions, and precludes certain modes of enforcement of otherwise valid criminal laws. Finally, the executive enforces those criminal laws that have been duly enacted by the  [\*1135]  legislature and approved by the judiciary, pursuant to procedures prescribed by the legislature or (more likely) found by the courts to pass constitutional muster. A couple of caveats should be mentioned. Not all laws are backed by penal sanctions, and not all executive officials are empowered to enforce criminal law. In general, only two groups--police and prosecutors--have the authority to implement the relevant penal code. The term "police" refers to those actors officially licensed to uncover and investigate crime and arrest suspected offenders: FBI agents, city police officers, county sheriffs, and so on. Similarly, the term "prosecutors" refers to the officials authorized to bring criminal charges against an alleged offender and to represent the government in a subsequent criminal case against the accused: the U.S. Attorney General, a U.S. Attorney, a state attorney general, a county district attorney, and their subordinates. Moreover, the passage, judicial approval, and execution of a penal statute do not necessarily follow a linear progression in practice. A given criminal law might be enacted and administered, but its constitutionality might never be questioned in the courts. Or the statute might be judicially approved in an initial proceeding but subsequently unenforced by executive officials. In turn, the courts might strike down a criminal law prior to enforcement, or the statute might not be reviewed until some official attempts to apply its strictures to a particular individual. Moreover, the ostensibly clean division among the three branches is the subject of ongoing academic and professional debate, including the battle between "formalism" and "functionalism" in the separation of powers. n95 Finally, various checks and balances are intended to ensure an interrelationship and interdependency among the branches of government. For example, a proposed federal criminal statute only becomes law if the President signs the bill or if Congress overrides his veto by a two-thirds majority. With these admonitions, it can be said that the legislature enacts criminal laws, the judiciary reviews the constitutionality of the laws and relevant enforcement procedures, and the executive administers the laws consistent with the mandates of the other branches. n96 An executive officer is without authority to suppress conduct that the legislature has not deemed criminal. Likewise, the officer has no power to enforce penal statutes that have been judicially invalidated or to use enforcement techniques disapproved by the courts.  [\*1136]  Building upon Dworkin's doughnut metaphor, Figure 1 schematically depicts American criminal justice. n97 The total area of the figure represents all potential combinations of criminal law and enforcement procedures. The area within the exterior circle ("the legislative act") depicts all conduct that has been criminalized by the legislature and the methods of enforcement that have been expressly or implicitly approved by the legislature. n98 The first band within the circle (B) represents those laws that the judiciary deems substantively invalid and therefore unenforceable under any procedure. The second band (C) represents those criminal statutes that pass constitutional muster but are being administered in an unconstitutional fashion. Finally, the internal core (D) depicts the combination of criminal laws and enforcement procedures that have been enacted by the legislature and are deemed unobjectionable by the courts. This area represents executive discretion in criminal justice--the freedom to enforce or not enforce particular criminal laws pursuant to particular procedures without interference from the other branches.  [\*1137]  To test this structure, imagine a hypothetical law "making it a crime for any person to remove another person's gall bladder." n99 Prior to the statute's enactment, assume that it was perfectly legal to remove gall bladders for any reason; graphically, this conduct exists outside of the exterior circle (A) and therefore well beyond any type of executive discretion to administer coercive sanctions. Once duly enacted by the legislature, the courts might review the statute's content under the substantive constitutional provisions: First Amendment freedom of speech and conscience, Fifth Amendment substantive due process, Eighth Amendment prohibition of cruel and unusual punishment, Fourteenth Amendment equal protection, and so on. If the gall bladder statute was found to be constitutionally obnoxious as a matter of substance--lying in area B of the graph--the executive branch would be precluded from enforcing this statute under any policing methodology. Now assume that the courts determine that there is nothing objectionable about the law's content but find that the mode of enforcing its provisions violates the procedural aspects of the Constitution. For example, maybe the police burst into a doctor's office without a warrant or probable cause and discover her performing the prohibited operation; or maybe law enforcement agents beat the physician into confessing her crimes. This time the problem is not the substance of the statute but the executive officer's impermissible enforcement. The police conduct--represented in area C--is lawless and therefore, outside the area of executive discretion. Once again, in area A the executive has not been authorized to act by the legislature; in area B the judiciary has invalidated the relevant criminal  [\*1138]  statute as substantively unconstitutional; and in area C the courts have precluded a particular enforcement methodology of an otherwise valid law. What if the legislature enacts the gall bladder statute and the courts approve both the substantive content of the law and the subsequent method of enforcement? This combination of criminal law and police procedure lies in area D, the totality of executive discretion in criminal justice. In this area, executive officials exercise complete freedom in the administration of the criminal law. In the abstract, the legislative and judicial branches might make every attempt to narrow the scope of unchecked executive discretion. For example, lawmakers might enact only a few criminal statutes and repeal ineffective or counterproductive laws, thereby limiting the grounds for coercive enforcement. Statutory drafters might also be very specific in the coverage of a particular provision, making clear the situations in which the law applies. In turn, the judicial branch might exercise substantial oversight in all facets of the criminal process, including decisions not to enforce the law. Courts might strike down or narrowly interpret vague criminal statutes and refuse to allow the application of penal provisions suffering from desuetude. Judicial review might freely entertain claims of selective enforcement or prosecutorial overreaching in the plea bargaining process. Graphically, the circumference of legislatively proscribed conduct ("the legislative act") would be relatively constricted, the band of judicial review and invalidation (B and C) would be broad, and the residual area of executive discretion (D) would be quite small.

## 2NC---AT: Perm Do CP---Statutory

“Statutory” requires a statute

Merriam Webster No Date

stat·u·to·ry adjective \ˈsta-chə-ˌtȯr-ē\

Definition of STATUTORY

1: of or relating to statutes

2: enacted, created, or regulated by statute <a statutory age limit>

That’s a law enacted by Congress

The Oxford Guide to the U.S. Government 2012

(Oxford University Press via Oxford Reference, Georgetown Library)

statute

A statute is a written law enacted by a legislature. **A federal statute is a law enacted by Congress**. State statutes are enacted by state legislatures; those that violate the U.S. Constitution may be struck down by the Supreme Court if the issue is appealed to the Court.

“Statutory restrictions on authority” require the Congress

Peterson, Associate Professor of Law @ George Washington University, 1991

(Todd D. Peterson,; B.A. 1973, Brown University; J.D. 1976, University of Michigan, Book Review: The Law And Politics Of Shared National Security Power -- A Review Of The National Security Constitution: Sharing Power After The Iran-Contra Affair by Harold Hongju Koh, New Haven, Conn.: Yale University Press. 1990. Pp. x, 330, March, 1991 59 Geo. Wash. L. Rev. 747)

Based on both case law and custom, it is hard to argue that Congress does not have substantial power to control the President's authority, even in the area of national security law. From the time of Little v. Barreme, n77 the Supreme Court has recognized Congress's power to regulate, through legislation, national security and foreign affairs. No Supreme Court case has struck down or limited Congress's ability to limit the President's national security power by passing a statute. n78 Although there may be some areas where the Court might not permit statutory regulation to interfere with the President's national security powers, these are relatively insignificant when compared to the broad authority granted to Congress by express provisions of the Constitution and the decisions of the Supreme Court. n79

Even in cases in which the Court has given the President a wide berth because of national security concerns, the Court has noted the absence of express statutory limitations. For example, in Department of the Navy v. Egan, n80 the Court refused to review the denial of a security clearance, but it concluded that "unless Congress specifically has provided otherwise, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security [\*762] affairs." n81 In other cases, of course, such as Youngstown, n82 the Supreme Court has clearly stated that Congress may restrict the President's authority to act in matters related to national security.

Not even Koh's bete noire, the Curtiss-Wright case, n83 could reasonably be interpreted as a significant restriction on Congress's authority to limit the President's authority by statute. First, as Koh himself forcefully demonstrates, Curtiss-Wright involved the issue whether the President could act pursuant to a congressional delegation of authority that under the case law existing at the time of the decision might have been deemed excessively broad. n84 Thus, the question presented in Curtiss-Wright was the extent to which Congress could increase the President's authority, not decrease it. At most, the broad dicta of Curtiss-Wright could be used to restrict the scope of mandatory power sharing on the ground that the President's inherent power in the area of international relations "does not require as a basis for its exercise an act of Congress." n85

Even the dicta of Curtiss-Wright, however, give little support to those who would restrict permissive power sharing on the ground that Congress may not impose statutory restrictions on the President in the area of national security and foreign affairs. Justice Sutherland's claims with respect to exclusive presidential authority are comparatively modest when compared with his sweeping statements about the President's ability to act in the absence of any congressional prohibition. n86 He asserts that the President alone may speak for the United States, that the President alone negotiates treaties and that "[i]nto the field of negotiation the Senate cannot intrude; and Congress itself is powerless to invade it." n87 It is in this context of the President's power to be the communicator for the nation that Justice Sutherland cites John Marshall's famous statement that the President is the "sole organ of the nation" in relations with other nations. n88 This area of exclusive authority in which even permissive sharing is inappropriate is limited indeed. When he writes of the [\*763] need to "accord to the President a degree of discretion and freedom from statutory restriction which would not be admissible were domestic affairs alone involved," n89 Justice Sutherland refers to the permissibility of a broad delegation, not the constitutional impermissibility of a **statutory restriction**. **Indeed**, **the Court specifically recognized that Congress could withdraw the authority of the President to act** and prohibit him from taking the actions that were the subject of the case. n90

To be fair to Koh, he would not necessarily disagree with this reading of Curtiss-Wright; he clearly believes that Congress does have the authority to restrict the President's national security power. Nevertheless, Koh's emphasis on Curtiss-Wright still gives the case too much import. Oliver North's protestations to the contrary notwithstanding, there is no Supreme Court authority, including the dicta in Curtiss-Wright, that significantly restricts the power of Congress to participate by statutory edict in the national security area. Thus, contrary to Koh's model, Curtiss-Wright and Youngstown do not stand as polar extremes on a similar question of constitutional law. To be sure, they differ significantly in tone and in the attitude they take to presidential power, but the cases simply do not address the same issue. Therefore, it does Koh's own thesis a disservice to suggest that the cases represent different views on the scope of permissive power sharing. There simply is no Supreme Court precedent that substantially restricts Congress's authority to act if it can summon the political will.

**The absence of judicial restrictions on permissive power sharing is particularly important because** it means that **the question of statutory restrictions on the President's** national security **powers should** for the most part **be a political one**, not a constitutional one. **Congress has broad power to act**, and the Court has not restrained it from doing so. n91 The problem is that Congress has refused to take effective action.

## 2NC---Durable Fiat / AT: Rollback

And executive orders have the force of law:

Oxford Dictionary of English 2010

(Oxford Reference, Georgetown Library)

executive order

▶ noun US (Law) a rule or order issued by the President to an executive branch of the government and having the force of law.

Executive orders are permanent

Duncan, Associate Professor of Law at Florida A&M, Winter 2010

(John C., “A Critical Consideration of Executive Orders,” 35 Vt. L. Rev. 333, Lexis)

The trajectory of the evolution of the executive power in the United States, as seen through the prism of the growing edifice of executive orders have become increasingly formal and permanent. The evolution of executive power in the United States has shifted executive orders from mere legislative interpretation to ancillary legislation. **Executive orders continue to influence subsequent presidents**. The elaboration of executive order promulgation, as an autopoietic process was necessary to the very existence of presidential power. That is, the mechanisms for formalizing executive orders have always existed in the executive power in a government whose legitimacy lives in written pronouncements treated as delicate, sacred, and worth protecting at all cost. **Part of this formalization is** a consequence of **the reverence for precedent**. Thus, **prior presidents influence future presidents**, less because future presidents wish to mimic their predecessors, but more **because future presidents act within an edifice their predecessors have already erected**. Thus, the growth and elaboration of an ever more robust structure of executive orders resembles an autopoietic process. n561

CP constrains future Presidents – it creates a legal framework

Brecher, JD University of Michigan, December 2012

(Aaron, Cyberattacks and the Covert Action Statute, 111 Mich. L. Rev. 423, Lexis)

The executive might also issue the proposed order, even though it would limit her freedom in some ways, because of the possible benefits of **constraining future administrations** or preempting legislative intervention. n149 For example, in this context, an administration may choose to follow the finding and reporting requirements in order to convince Congress that legislative intervention is unnecessary for proper oversight. This is acceptable if the covert action regime is in fact adequate on its own. Moreover, if greater statutory control over cyberattacks is needed, the information shared with Congress may give Congress the tools and knowledge of the issue necessary to craft related legislation. n150 Additionally, while executive orders are hardly binding, **the inertia following adoption of an order may help constrain future administrations**, which may be more or less trustworthy than the current one. **Creating a presumption through an executive order** also **establishes a stable legal framework** for cyberattacks that allows law to follow policy in this new field, and permits decisionmakers to learn more about the nature of cyberoperations before passing detailed statutes that may result in unintended consequences.

Executive order binds future administrations

Jensen, JD Drake University, Summer 2012

(Jase, FIRST AMERICANS AND THE FEDERAL GOVERNMENT, 17 Drake J. Agric. L. 473, Lexis)

At the historic 1994 meeting with the tribes, President Clinton signed a Presidential memorandum which provided executive departments and agencies with principles to guide interaction with and policy concerning Indian tribes. n83 President Clinton sought to ensure that the government recognizes that it operates on a government-to-government relationship with the federally recognized tribes. n84 Agencies were to consult with tribes prior to taking action which would affect them, consider tribal impact regarding current programs and policies, and remove barriers to communication. n85

Toward the end of Clinton's second term he issued an executive order which provided the executive branch with more detailed directions on how to implement the broader policy of government-to-government tribal consultation set forth in the 1994 memorandum. n86 **The order had a stronger binding effect on future administrations**. President Clinton signed Executive Order 13175 on November 6, 2000, and the order went into effect on January 5, 2001. n87 The order was binding upon all executive departments and executive agencies and all independent agencies were encouraged to comply with the order on a voluntary basis. n88 Each agency was required to designate an official which is to head the crea [\*486] tion of a tribal consultation plan, prepare progress reports, and ensure compliance with Executive Order 13175. n89

## Deterrence – 2NC

Declaratory policies solve transparency and deterrence – creates clear response policy

Waxman 13 (Matthew, Professor, Columbia Law School; Adjunct Senior Fellow, Council on Foreign Rela-tions; Member of the Hoover Institution Task Force on National Security and Law, “Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions” 2013, 89 INT’L L. STUD. 109)

III. A STRATEGIC PERSPECTIVE

A strategic perspective on the question of cyber attacks as armed attacks sees the issue as one linking a purported right of armed self-defense to long-term policy interests—both national interests and global ones in the case of the United States—including security and stability. The substance and clarity of any such legal right has the potential to significantly enhance or detract from those strategic ends.

Armed self-defense to cyber attacks may be strategically valuable in several respects. First, anticipatory or responsive military actions might be important in some cases to protecting military and critical infrastructure vulnerable to cyber attacks—for example, by striking at facilities or indi-viduals responsible for launching or directing them—though, because the physical infrastructure associated with cyber attacks may be quite small and widely dispersed, this sort of preventive use of force specifically to neutral-ize the possibility of initial or follow-on cyber attacks has not been the sub-ject of much discussion. Second, the credible threat of self-defensive mili-tary actions might help deter cyber attacks by raising the prospective costs of hostile cyber activities in the minds of adversaries (though probably not much so of non-State adversaries, against whom deterrent threats of mili-tary action will not be very potent). Such strategic logic likely underlies the U.S. declaratory postures described in the previous section, putting adver-saries on notice that they should expect a possible military response to some cyber threats.

Self-defense red lines are good – establishes clear thresholds to induce deterrence

Waxman 13 (Matthew, Professor, Columbia Law School; Adjunct Senior Fellow, Council on Foreign Rela-tions; Member of the Hoover Institution Task Force on National Security and Law, “Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions” 2013, 89 INT’L L. STUD. 109)

This is not the place to discuss in any detail the specific challenges and nuances of relying in part on military defense or deterrence against cyber attacks, a topic that many others have written about in detail.23 The salient concern here is the way in which—to turn our lens back a bit and open the aperture to capture the legal and strategic perspectives together—legally regarding some cyber attacks to constitute armed attack might contribute strategically. It could do so in a number of ways.

For example, if one believes that armed self-defense is important to protecting against cyber attacks through anticipatory or responsive military actions, internally a well-established legal right helps strengthen the hand of political leaders weighing such options (an issue taken up further in the next session, which turns our lens toward a political perspective). An estab-lished or articulated right adds legitimacy to forceful options and may be taken as a guide of likely global reactions. A well-established right also facil-itates military planning for such contingencies by clearing internal obstacles and bolstering the legitimacy and bureaucratic expectation of doing so. Within agencies charged with operationalizing them, it is much easier to plan and develop options for policy routes that are declared legal.

By thinking externally about the expectations of others, a legal right of armed self-defense might contribute to deterrence by establishing and communicating more emphatically and clearly red lines associated with self-defensive threats.24 It helps to signal to others thresholds beyond which they should expect significant escalation, to include military means. When combined with rules of State responsibility, a right of armed self-defense might also induce States to crack down more strongly on cyber attacks launched from their territory, or perhaps to share more intelligence about cyber threats within their jurisdiction, whether out of a sense of legal obli-gation or for fear of being targeted with armed self-defense.

## Norms – 2NC

The CP’s declaratory policy creates international norms – the executive drives change

Segal 11 (Adam, Maurice R. Greenberg Senior Fellow for China Studies, “Cyberspace Governance: The Next Step” Policy Innovation Memorandum No. 2, March 2011, Council on Foreign Relations)

After years of dismissing the utility of international negotiations on cyberspace, U.S. officials now say that they will participate in talks to develop rules for the virtual world. But which norms should be pursued first and through which venues? As a start, the United States should issue two "cyber declaratory statements," one about the thresholds of attacks that constitute an act of war and a second that promotes "digital safe havens"--civilian targets that the United States will consider off-limits when it conducts offensive operations. These substantive statements should emerge from a process of informal multilateralism rather than formal negotiations. **Washington should engage allies and close partners such as India first and then reach out to other powers such as China and Russia with the goal that they also issue similar statements. Washington should also reach out to the private corporations that operate the Internet and nongovernmental organizations responsible for its maintenance and security.**

Declaratory statements play an important role in the definition, diffusion, and adoption of international norms. The discussions that precede the statements encourage actors to identify desirable and realistically attainable norms; the statements themselves set the behaviors that states will be held to. They are also likely to increase strategic stability. Explicit statements give potential attackers a more concrete picture of what type of attacks the United States will respond to and how, making signaling easier and improving stability.

The Problem

Increased U.S. receptivity to international negotiations reflects a growing sense **that domestic efforts to secure cyberspace are inadequate and that the United States has hurt itself by sitting on the sidelines.** There is real fear that a cyberattack--the use of computer power to attack computer, communication, transportation, and energy networks--could disrupt the economy, destroy critical infrastructure, or degrade military capabilities. The Internet was originally designed for the use and convenience of a small group of researchers in the United States; security was an afterthought. Now the network is global and there has been a proliferation of devices from laptops to smartphones connecting to it. No one agency, either national or multilateral, exerts authority over all parts of the Web.

As the United States has focused on domestic efforts to make cyberspace more secure--appointing a cyber coordinator, standing up Cyber Command, and deploying Einstein 2, an intrusion detection system--other states have challenged the U.S. conception of the web as a global commons open to commerce and the free exchange of information. Moreover, **the United States' refusal to enter into negotiations reinforced the sense that it intended to dominate cyberspace and limit the ability of other countries to maneuver in this new domain**.

The Obama administration's May 2009 Cyberspace Policy Review revealed a shift in U.S. attitudes. "International norms are critical to establishing a secure and thriving digital infrastructure," the report concluded. In December 2009 the United States agreed to talk with Russia and a United Nations arms control committee about Internet security.

International cooperation is necessary, but some fundamental characteristics of cyberspace make traditional arms control agreements unlikely. The technologies used in most attacks are commercial and widely available. Attacks can be masked and routed across several networks, obscuring whether they are the work of independently operating "patriotic hackers," criminal groups, an official security agency, bored teenagers, or some combination of all four. This problem of attribution undermines verification; signatories to any agreement would have little confidence they could identify violators.

Moreover, there is no consensus about what constitutes a cyberattack. The United States talks primarily about defending critical infrastructure like the power grid or financial systems; China, Russia, and others worry about these vulnerabilities but also see the free flow of information as a threat to domestic stability. As a result, in any negotiations, Beijing and Moscow are likely to demand that the United States limit its support for "digital activists" in return for China and Russia controlling "patriotic hackers," a requirement Washington is unlikely to meet.

The Rules of Cyberspace

While a more formal agreement may never be reachable, the United States has a clear interest in defining the rules of interstate behavior in cyberspace. It has a particular interest in identifying the point at which a cyberattack becomes the equivalent of an "armed attack" in international law as well as in defining what constitutes a legitimate target of cyberattack. In the physical world, for example, states are expected to abide by the principle of distinction which requires attacks only be made on legitimate military targets and permits attacks on civilian targets only when "demanded by the necessities of war." This norm was developed through several centuries of war and formalized after World War II in the Geneva Protocols.

At this point, most countries would accept that a cyberattack with "kinetic effects" equivalent to those of a conventional armed attack should be treated in the same manner, allowing for individual and collective self-defense as well as cyber and kinetic responses. But **what about attacks below this threshold that nonetheless threaten critical interests, say, by destroying public data or disrupting financial markets?** After consulting with its allies and friends, **the United States should issue a public "cyber declaratory statement" that reserves the right to respond either through a conventional or computer network attack, but leaves some room for maneuver**. Attacks on data and financial markets could both be covered by this statement as long as the consequences of an attack resulted in real suffering, not simply inconvenience.

**The United States will not renounce the development and use of offensive weapons, but it should still work to develop "digital safe havens" and then in a separate initiative declare these targets off limits.** Again, there is likely to be relatively easy consensus around some areas--hospitals and medical data--and much less agreement around others such as financial systems, power grids, and Internet infrastructure. The United States should also develop methods to mark its digital safe havens. It may have to separate its own network and data systems--data, for example, from the Department of Health and Human Services and the Pentagon should not sit on the same servers. U.S. policy makers should also work with companies and NGOs to address what are likely to be significant technical challenges in disentangling protected and non-protected spaces.

Building International Support

Since communication networks are global and primarily in private hands, an informal multilateralism is a more appropriate approach than a more formal multilateralism. U.S. officials should continue to show flexibility about venue, engaging through bilateral and multilateral meetings such as the United Nations, the G20, and regional groupings. There have been several moves to limit the role of nongovernmental groups in Internet governance--most recently in a December 2010 decision to involve only member states and exclude the Internet Governance Caucus and other organizations from a UN working group. By insisting on their participation in the relevant forum, the United States can continue to strengthen the authority of these groups.

In the case of thresholds and digital safe havens, **the United States should conduct discussions with close allies, friends, private companies, and NGOs over a twelve-to-eighteen month period**. The discussions about thresholds are particularly important for the United States to have with its allies; the large scale distributed denial of service attacks on Estonia in 2007 raised the question of whether the country should, or could, have invoked Article 5 of the NATO charter, in which members agree that an "armed attack against one or more of them . . . shall be considered an attack against them all." At the time and as is still the case today, NATO and international law lacked an accepted definition of what constitutes a cyberattack. These discussions should then be expanded to include other partners such as India and then to potential adversaries. **After all of these consultations, the United States should issue substantive statements about thresholds and response.** Although these statements will be unilateral**,** the goal of the consultative process should be to spur others to issue similar commitments.

This decentralized strategy is particularly important after Stuxnet, the malware that appears to target the Iranian nuclear program. It is now widely assumed that the United States, along with Israel, was behind the code. As a result, many countries will remain skeptical about Washington's intentions. Rules that appear to be the work of the United States alone will have little chance of gaining international support. **But building a coalition of states who will gain from and are willing to push for new rules may give these norms greater legitimacy**.

There has been in the United States' international engagement, however, a tendency to substitute process for strategy. While the decentralized approach to cyberconflict is the right one, it does not help in identifying strategic goals. The White House will have to become actively involved in order to push the process forward. **The National Security Council's** Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC) **subcommittee on international cyberspace policy efforts should** drive action, **not just coordinate and share information about what other agencies are doing**.

An informal multilateralism is best suited to cyberspace, and by focusing on some of the norms of interstate cyberconflict, and on thresholds and legitimate targets in particular, the U**nited** S**tates** will be better able to begin shaping international norms.

Unilateral self-restraint creates international norms

Herbert Lin, affiliate at CISAC and chief scientist at the Computer Science and Telecommunications Board, National Research Council of the National Academies, where he has been study director of major projects on public policy and information technology. Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues. He received his doctorate in physics from MIT, ‘13 [“Chapter 2: Laying an Intellectual Foundation for Cyberdeterrence: Some Initial Step,” from “The Secure Information Society Ethical, Legal and Political Challenges,” Editors: Jörg Krüger, Bertram Nickolay, Sandro Gaycken, Springer-Verlag London 2013]

The preceding discussion suggests that at the very least, **classical deterrence** theory¶ (as construed for deterring nuclear attacks on the United States) **is quite problematic¶ when applied to cyberattacks on the United States because many of the conditions¶ necessary for nuclear deterrence are absent from the cyber domain.**¶ Whether a deterrence framework can be developed for the cyber domain is open¶ to question, and indeed is one primary subject of the papers to be commissioned¶ for this project. But **whatever the useful scope for deterrence, there may also be¶ a complementary and helpful role for international legal regimes** and codes of be-¶ havior **designed to reduce the likelihood of highly destructive cyberattacks** and to¶ minimize the realized consequences if cyberattacks do occur. **That** is, participation¶ in international agreements **may be an important aspect of U.S. policy.¶ In the past, nations have pursued a variety of agreements intended to reduce the¶ likelihood of conflict and to minimize the realized consequences if conflict does¶ occur** (and also to reduce the financial costs associated with arms competitions)¶ under the broad rubric of arms control. To achieve these objectives, arms control¶ regimes often seek to limit capabilities of the signatories or to constrain the use¶ of such capabilities. Thus, in the nuclear domain, agreements have (for example)¶ been reached to limit the number and type of nuclear weapons and nuclear weapons¶ platforms of the signatories—a limitation on capability that putatively reduces the¶ destructiveness of conflict by limiting the capabilities on each side.¶ **Agreements have also been reached for purposes of constraining the use of such¶ capabilities—for example, the United States and Russia are parties to an agreement¶ to provide advance notice to each other of a ballistic missile launch**. Other pro-¶ posed restrictions on use have been more controversial—for example, nations have¶ sometimes sought agreement on “no first use of nuclear weapons.” Agreements con-¶ straining the use of such capabilities are intended to reduce the possibility of mis-¶ understandings that might lead to conflict and thus reduce the likelihood of conflict.¶ Lastly, international legal regimes and codes of behavior can make certain kinds¶ of weapons unacceptable from a normative standpoint. **For example, most nations¶ today would eschew the overt use of biological weapons, and thus the likelihood of¶ such use by any of these nations is lower than it would be in the absence of such a¶ behavioral norm**.¶ In the present case (that is, in thinking about ways to prevent cyberattacks of¶ various kinds), **one of the most powerful rationales for considering international¶ agreements in the cyber domain is that all aspects of U.S. society, both civilian and military, are increasingly dependent on information technology**, and to the extent¶ that such dependencies are greater for the United States than for other nations, re-¶ strictions on cyberattack asymmetrically benefit the United States. **Proponents of¶ such agreements also argue that aggressive pursuit of cyberattack capabilities will¶ legitimize cyberattack as a military weapon and encourage other nations to develop¶ such capabilities for use against the United States** and its interests, much to its detri-¶ ment.¶ Objections to such regimes usually focus on the difficulty (near-impossibility)¶ of verifying and enforcing such an agreement. But the United States is a party to a¶ number of difficult-to-enforce and hard-to-verify regimes that regulate conflict and¶ prescribe rules of behavior—notably the Biological Weapons Convention (BWC).¶ In recent years, the BWC has been criticized for lacking adequate verification pro-¶ visions, and yet few policy makers suggest that the convention does not further U.S.¶ interests.¶ **In the cyber domain, meaningful agreements to limit acquisition of cyberattack¶ capability are unlikely to be possible.** Perhaps **the most important impediment to¶ such agreements is the verification issue—technology development for cyberattack¶ and the testing of such technology would have few signatures that could be ob-¶ served, even with the most intrusive inspection regimes imaginable.¶** **Agreements to** constrain cyberattack capabilities **are also problematic**, in the¶ sense that **little can be done to verify that a party to such an agreement will in¶ fact restrict its use when it decides it needs to conduct a cyberattack**. On the other¶ hand, **such agreements have a number of benefits**.¶ •¶ **They help to create international norms regarding the acceptability of such be-¶ havior** (and major nation-states tend to avoid engaging in broadly stigmatized¶ behavior).¶ •¶ **They help to inhibit training that calls for such use** (though secrecy will shield¶ clandestine training).¶ •¶ **The violation of such agreements may be detectable.** Specifically, cyberattacks¶ that produce small-scale effects may be difficult to detect, but massively destruc-¶ tive attacks would be evident from their consequences, especially with appropri-¶ ate rules to assist forensic assessment. **If a violation is detected, the violator is¶ subject to the consequences that follow from such detection.¶ Lastly, even though the development of regimes constraining use would address¶ only cyberattacks associated with nation-states, they could have significant bene-¶ fit, as nation-states do have advantages in pursuing cyberattack that most nonstate-¶ supported actors do not have**. Although **such regimes** would not obviate the need¶ for passive defenses, they **could be useful in tamping down risks of escalation and¶ might help to reduce international tensions in some circumstances**.¶ As illustrations of regimes constraining use, **nations might agree to confidence-¶ building measures that** **committed them to providing mutual transparency** **regarding¶ their activities in cyberspace, to cooperate on matters related to securing cyberspace**¶ (e.g., in investigating the source of an attack), **to notify each other regarding certain¶ activities that might be viewed as hostile or escalatory, or to communicate directly with each other during times of tension or crisis**. Agreements to eschew certain kinds¶ of cyberattack under certain circumstances could have value in reducing the likeli-¶ hood of kinetic conflict in those cases in which such cyberattacks are a necessary¶ prelude to a kinetic attack.¶ **Limitations on cyber targeting (e.g., no cyberattacks on civilian targets; require-¶ ments that military computers be explicitly identified; no first use of cyberattack¶ on a large scale; or no attacks on certain classes of targets, such as national power¶ grids, financial markets or institutions, or air traffic control systems) could prevent¶ or reduce the destructiveness of an attack, assuming that collateral and/or cascading¶ damage could be limited.** Agreements (or unilateral declarations) to abide by such¶ agreements might be helpful in establishing appropriate rules of conduct (norms of¶ behavior) and a social structure to enforce those rules.¶ On the other hand, U.S. policy makers and analysts have not seriously explored¶ the utility and feasibility of international regimes that deny the legitimacy of cyber-¶ attacks on critical infrastructure assets, such as power grids, financial markets, and¶ air traffic control systems.¶ 11¶ How useful would such a regime be, especially applied¶ in concert with a significantly improved cyberdefensive posture for these assets?¶ How would difficulties of verification and enforcement affect relative national mili-¶ tary postures and the credibility of the regime? What meaningful capabilities would¶ the United States be giving up if it were to agree to such a regime? These and other¶ related questions find few answers in the literature. **The feasibility of these or other¶ regimes to limit use of cyberattack is unclear, especially in light of the difficulties¶ of working out the details of how the regime would actually operate**. It is for this¶ reason that research is needed to explore their feasibility.¶ **Agreements in a cyber context might also usefully address important collateral¶ issues, such as criminal sanctions or compensation for damages sustained under¶ various circumstances**. They might also require signatories to pass national laws¶ that criminalize certain kinds of cyber behavior undertaken by individuals and to¶ cooperate with other nations in prosecuting such behavior, much as the Convention¶ on Cyber Crime has done.¶ 12

## 2NC No Cyber War Impact

Err neg - their authors exaggerate and cyber defense tech is improving

Libicki 8/16/13

MARTIN C. LIBICKI is a Senior Management Scientist at the RAND Corporation and a Visiting Professor at the U.S. Naval Academy, Foreign Affairs, August 16, 2013, "Don't Buy the Cyberhype: How to Prevent Cyberwars From Becoming Real Ones", http://www.foreignaffairs.com/articles/139819/martin-c-libicki/dont-buy-the-cyberhype

These days, most of Washington seems to believe that a major cyberattack on U.S. critical infrastructure is inevitable. In March, James Clapper, U.S. director of national intelligence, ranked cyberattacks as the greatest short-term threat to U.S. national security. General Keith Alexander, the head of the U.S. Cyber Command, recently characterized “cyber exploitation” of U.S. corporate computer systems as the “greatest transfer of wealth in world history.” And in January, a report by the Pentagon’s Defense Science Board argued that cyber risks should be managed with improved defenses and deterrence, including “a nuclear response in the most extreme case.”

Although the risk of a debilitating cyberattack is real, the perception of that risk is far greater than it actually is. No person has ever died from a cyberattack, and only one alleged cyberattack has ever crippled a piece of critical infrastructure, causing a series of local power outages in Brazil. In fact, a major cyberattack of the kind intelligence officials fear has not taken place in the 21 years since the Internet became accessible to the public.

Thus, while a cyberattack could theoretically disable infrastructure or endanger civilian lives, its effects would unlikely reach the scale U.S. officials have warned of. The immediate and direct damage from a major cyberattack on the United States could range anywhere from zero to tens of billions of dollars, but the latter would require a broad outage of electric power or something of comparable damage. Direct casualties would most likely be limited, and indirect causalities would depend on a variety of factors such as whether the attack disabled emergency 911 dispatch services. Even in that case, there would have to be no alternative means of reaching first responders for such an attack to cause casualties. The indirect effects might be greater if a cyberattack caused a large loss of confidence, particularly in the banking system. Yet scrambled records would probably prove insufficient to incite a run on the banks.

Officials also warn that the United States might not be able to identify the source of a cyberattack as it happens or in its immediate aftermath. Cyberattacks have neither fingerprints nor the smell of gunpowder, and hackers can make an intrusion appear legitimate or as if it came from somewhere else. Iran, for example, may not have known why its centrifuges were breaking down prematurely before its officials read about the covert cyber-sabotage campaign against the country’s nuclear program in The New York Times. Victims of advanced persistent threats -- extended intrusions into organization networks for the purpose of espionage -- are often unaware for months, or even years, that their servers have been penetrated. The reason that such attacks go undetected is because the removal of information does not affect the information in the system, so nothing seems amiss. The exfiltration of information can also be easily hidden, such as in the daily flow of web traffic from an organization.

But since everything is becoming increasingly dependent on computers, could levels of damage impossible today become inevitable tomorrow? As it happens, all of the trend lines -- good and bad -- in cyberspace are rising simultaneously: the sophistication of attackers, but also that of the defenders; the salience of cyberattacks as weapons, but also the awareness of the threat they pose; the bandwidth available for organizing larger attacks, but also the resources to ward them off. It is bad news that Iran is beginning to see cyberwar as a deniable means of exploiting easy targets. And it is good news that software companies are now rethinking the architectural features of their systems that permit such vulnerabilities to exist in the first place.

We don’t have to prove that a cyber attack is impossible, just that high costs will cause enemies to seek alternatives

Rid, reader in war studies – King's College London, and McBurney, professor – Agents and Intelligent Systems Group – Department of Informatics @ King's College, ‘12

(Thomas and Peter, “Cyber-Weapons,” *The RUSI Journal* Volume 157, Issue 1, p. 6-13)

A thorough conceptual analysis and a detailed examination of **the empirical record corroborates our hypothesis**: developing and deploying potentially destructive cyber-weapons against hardened targets will require significant resources, hard-to-get and highly specific target intelligence, and time to prepare, launch and execute an attack. Attacking secured targets would probably require the resources or the support of a state actor; terrorists are unlikely culprits of an equally unlikely cyber-9/11. The scant empirical record also suggests that the greatest benefit of cyber-weapons may be using them in conjunction with conventional or covert military strikes, as Israel did when it blinded the Syrian air defence in 2007. This leads to a second conclusion: the cost-benefit payoff of weaponised instruments of cyber-conflict may be far more questionable than generally assumed: target configurations are likely to be so specific that a powerful cyber-weapon may only be capable of hitting and acting on one single target, or very few targets at best. The equivalent would be a HARM missile that can only destroy one unique emitter, not a set of targets emitting at the same frequency. But in contrast to the missile – where only the seeker needs to be specifically reprogrammed and the general aviation and propulsion systems remain functional – the majority of modular components of a potent cyber-weapon, generic and specific, would have a rather short shelf-life after discovery.

Two findings contravene the debate's received wisdom. One insight concerns the dominance of the offence. Most weapons may be used defensively and offensively. But the information age, the argument goes since at least 1996, has ‘offence-dominant attributes’.37 A 2011 Pentagon report on cyberspace again stressed ‘the advantage currently enjoyed by the offense in cyberwarfare’.38 But when it comes to cyber-weapons, the offence has higher costs, a shorter shelf-life than the defence, and a very limited target set.39 All this **drastically reduces the coercive utility of cyber-attacks.** Any threat relies on the offender's credibility to attack, or to repeat a successful attack. Even if a potent cyber-weapon could be launched successfully once, it would be highly questionable

f an attack, or even a salvo, could be repeated in order to achieve a political goal. At closer inspection cyber-weapons do not seem to favour the offence.

A second insight concerns the risk of electronic arms markets. One concern is that sophisticated malicious actors could resort to asymmetric methods, such as employing the services of criminal groups, rousing patriotic hackers, and potentially redeploying generic elements of known attack tools. Worse, more complex malware is likely to be structured in a modular fashion. Modular design could open up new business models for malware developers. In the car industry, for instance,40 modularity translates into a possibility of a more sophisticated division of labour. Competitors can work simultaneously on different parts of a more complex system. Modules could be sold on underground markets. But if our analysis is correct, potential arms markets pose a more limited risk: the highly specific target information and programming design needed for potent weapons is unlikely to be traded generically. To go back to our imperfect analogy: paintball pistols will continue to be commercially available, but probably not pre-programmed warheads of smart missiles.

Cyberattacks nearly impossible – empirics and defenses solve

**Rid 12** (Thomas Rid, reader in war studies at King's College London, is author of "Cyber War Will Not Take Place" and co-author of "Cyber-Weapons.", March/April 2012, “Think Again: Cyberwar”, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full)

"Cyberwar Is Already Upon Us." No way. "Cyberwar is coming!" John Arquilla and David Ronfeldt predicted in a celebrated Rand paper back in 1993. Since then, it seems to have arrived -- at least by the account of the U.S. military establishment, which is busy competing over who should get what share of the fight. Cyberspace is "a domain in which the Air Force flies and fights," Air Force Secretary Michael Wynne claimed in 2006. By 2012, William J. Lynn III, the deputy defense secretary at the time, was writing that cyberwar is "just as critical to military operations as land, sea, air, and space." In January, the Defense Department vowed to equip the U.S. armed forces for "conducting a combined arms campaign across all domains -- land, air, maritime, space, and cyberspace." Meanwhile, growing piles of books and articles explore the threats of cyberwarfare, cyberterrorism, and how to survive them. Time for a reality check: Cyberwar is still more hype than hazard. Consider the definition of an act of war: It has to be potentially violent, it has to be purposeful, and it has to be political. The cyberattacks we've seen so far, from Estonia to the Stuxnet virus, simply don't meet these criteria. Take the dubious story of a Soviet pipeline explosion back in 1982, much cited by cyberwar's true believers as the most destructive cyberattack ever. The account goes like this: In June 1982, a Siberian pipeline that the CIA had virtually booby-trapped with a so-called "logic bomb" exploded in a monumental fireball that could be seen from space. The U.S. Air Force estimated the explosion at 3 kilotons, equivalent to a small nuclear device. Targeting a Soviet pipeline linking gas fields in Siberia to European markets, the operation sabotaged the pipeline's control systems with software from a Canadian firm that the CIA had doctored with malicious code. No one died, according to Thomas Reed, a U.S. National Security Council aide at the time who revealed the incident in his 2004 book, At the Abyss; the only harm came to the Soviet economy. But did it really happen? After Reed's account came out, Vasily Pchelintsev, a former KGB head of the Tyumen region, where the alleged explosion supposedly took place, denied the story. There are also no media reports from 1982 that confirm such an explosion, though accidents and pipeline explosions in the Soviet Union were regularly reported in the early 1980s. Something likely did happen, but Reed's book is the only public mention of the incident and his account relied on a single document. Even after the CIA declassified a redacted version of Reed's source, a note on the so-called Farewell Dossier that describes the effort to provide the Soviet Union with defective technology, the agency did not confirm that such an explosion occurred. The available evidence on the Siberian pipeline blast is so thin that it shouldn't be counted as a proven case of a successful cyberattack. Most other commonly cited cases of cyberwar are even less remarkable. Take the attacks on Estonia in April 2007, which came in response to the controversial relocation of a Soviet war memorial, the Bronze Soldier. The well-wired country found itself at the receiving end of a massive distributed denial-of-service attack that emanated from up to 85,000 hijacked computers and lasted three weeks. The attacks reached a peak on May 9, when 58 Estonian websites were attacked at once and the online services of Estonia's largest bank were taken down. "What's the difference between a blockade of harbors or airports of sovereign states and the blockade of government institutions and newspaper websites?" asked Estonian Prime Minister Andrus Ansip. Despite his analogies, the attack was no act of war. It was certainly a nuisance and an emotional strike on the country, but the bank's actual network was not even penetrated; it went down for 90 minutes one day and two hours the next. The attack was not violent, it wasn't purposefully aimed at changing Estonia's behavior, and no political entity took credit for it. The same is true for the vast majority of cyberattacks on record. Indeed, there is no known cyberattack that has caused the loss of human life. No cyberoffense has ever injured a person or damaged a building. And if an act is not at least potentially violent, it's not an act of war. Separating war from physical violence makes it a metaphorical notion; it would mean that there is no way to distinguish between World War II, say, and the "wars" on obesity and cancer. Yet those ailments, unlike past examples of cyber "war," actually do kill people. "A Digital Pearl Harbor Is Only a Matter of Time." Keep waiting. U.S. Defense Secretary Leon Panetta delivered a stark warning last summer: "We could face a cyberattack that could be the equivalent of Pearl Harbor." Such alarmist predictions have been ricocheting inside the Beltway for the past two decades, and some scaremongers have even upped the ante by raising the alarm about a cyber 9/11. In his 2010 book, Cyber War, former White House counterterrorism czar Richard Clarke invokes the specter of nationwide power blackouts, planes falling out of the sky, trains derailing, refineries burning, pipelines exploding, poisonous gas clouds wafting, and satellites spinning out of orbit -- events that would make the 2001 attacks pale in comparison. But the empirical record is less hair-raising,

even by the standards of the most drastic example available. Gen. Keith Alexander, head of U.S. Cyber Command (established in 2010 and now boasting a budget of more than $3 billion), shared his worst fears in an April 2011 speech at the University of Rhode Island: "What I'm concerned about are destructive attacks," Alexander said, "those that are coming." He then invoked a remarkable accident at Russia's Sayano-Shushenskaya hydroelectric plant to highlight the kind of damage a cyberattack might be able to cause. Shortly after midnight on Aug. 17, 2009, a 900-ton turbine was ripped out of its seat by a so-called "water hammer," a sudden surge in water pressure that then caused a transformer explosion. The turbine's unusually high vibrations had worn down the bolts that kept its cover in place, and an offline sensor failed to detect the malfunction. Seventy-five people died in the accident, energy prices in Russia rose, and rebuilding the plant is slated to cost $1.3 billion. Tough luck for the Russians, but here's what the head of Cyber Command didn't say: The ill-fated turbine had been malfunctioning for some time, and the plant's management was notoriously poor. On top of that, the key event that ultimately triggered the catastrophe seems to have been a fire at Bratsk power station, about 500 miles away. Because the energy supply from Bratsk dropped, authorities remotely increased the burden on the Sayano-Shushenskaya plant. The sudden spike overwhelmed the turbine, which was two months shy of reaching the end of its 30-year life cycle, sparking the catastrophe. If anything, the Sayano-Shushenskaya incident highlights how difficult a devastating attack would be to mount. The plant's washout was an accident at the end of a complicated and unique chain of events. Anticipating such vulnerabilities in advance is extraordinarily difficult even for insiders; creating comparable coincidences from cyberspace would be a daunting challenge at best for outsiders. If this is the most drastic incident Cyber Command can conjure up, perhaps it's time for everyone to take a deep breath. "Cyberattacks Are Becoming Easier." Just the opposite. U.S. Director of National Intelligence James R. Clapper warned last year that the volume of malicious software on American networks had more than tripled since 2009 and that more than 60,000 pieces of malware are now discovered every day. The United States, he said, is undergoing "a phenomenon known as 'convergence,' which amplifies the opportunity for disruptive cyberattacks, including against physical infrastructures." ("Digital convergence" is a snazzy term for a simple thing: more and more devices able to talk to each other, and formerly separate industries and activities able to work together.) Just because there's more malware, however, doesn't mean that attacks are becoming easier. In fact, potentially damaging or life-threatening cyberattacks should be more difficult to pull off. Why? Sensitive systems generally have built-in redundancy and safety systems, meaning an attacker's likely objective will not be to shut down a system, since merely forcing the shutdown of one control system, say a power plant, could trigger a backup and cause operators to start looking for the bug. To work as an effective weapon, malware would have to influence an active process -- but not bring it to a screeching halt. If the malicious activity extends over a lengthy period, it has to remain stealthy. That's a more difficult trick than hitting the virtual off-button. Take Stuxnet, the worm that sabotaged Iran's nuclear program in 2010. It didn't just crudely shut down the centrifuges at the Natanz nuclear facility; rather, the worm subtly manipulated the system. Stuxnet stealthily infiltrated the plant's networks, then hopped onto the protected control systems, intercepted input values from sensors, recorded these data, and then provided the legitimate controller code with pre-recorded fake input signals, according to researchers who have studied the worm. Its objective was not just to fool operators in a control room, but also to circumvent digital safety and monitoring systems so it could secretly manipulate the actual processes. Building and deploying Stuxnet required extremely detailed intelligence about the systems it was supposed to compromise, and the same will be true for other dangerous cyberweapons. Yes, "convergence," standardization, and sloppy defense of control-systems software could increase the risk of generic attacks, but the same trend has also caused defenses against the most coveted targets to improve steadily and has made reprogramming highly specific installations on legacy systems more complex, not less.

No capability or motive

Rid 7/29/13

Thomas Rid, Reader in War Studies at King's College London, His most recent book is Cyber War Will Not Take Place, also a non-resident fellow at the Center for Transatlantic Relations in the School for Advanced International Studies, Johns Hopkins University, The Economist, July 29, 2013, "Cyber-warfare: Statements", http://economist.com/debate/days/view/998/print

Is a violent cyber-attack possible? Of course it is. Nobody said it wasn't. Risk is the probability of harm multiplied by its cost. The question thus has two parts: how likely are acts of violent, computer-executed sabotage, and how damaging could those acts be? Could computer network attacks rise to a level that sensible people would call "cyber-warfare"?

The answer: probably not—for four reasons.

First, facts matter. Facts must drive analysis, not fear. That means scholars, analysts and security professionals have to analyse the empirical record, not the wild and unlimited realm of imagination. If "cyberwar" would be so easy and imminent, it would have happened already. But, again, the world has yet to witness a single injury or fatality as a result of a computer attack. Even material destruction has happened only once, in Iran. Yes, the future has surprises in store. Sometimes the unexpected happens. Which leads to reason two.

Intentions matter. Most likely some states have the capability to hack critical infrastructure. America has demonstrated that this is possible with Stuxnet, although that required significant lead-time, development, testing and co-operation between different types of experts and engineers. Others could do it as well, possibly China or Russia, although not poorly organised militants. But China and Russia have a commercial interest in stealing stuff, not in breaking stuff: those with the means to do harm by cyber don't have the intention, and those with the intention don't have the means. Yes, that could change. But even when it changes, the intensity of the damage would probably remain more limited than broadly assumed.

Because, third, intelligence matters. Penetrating complex targets requires intelligence, highly detailed, hard-to-get intelligence. This is true for conventional military strikes and it is also true for computer sabotage. An anonymous-style denial-of-service attack requires no target intelligence, only a URL—like blocking access to a building by standing in front of the doors. Sabotage is different. It requires not just breaking and entering and then finding the locked machine room. The saboteur's problem is that just stopping the machine isn't enough. The goal is subtly and clandestinely modifying the output parameters of a uniquely configured automat, bolted together from arcane parts, without the operators taking notice. This requires intelligence not available easily on the web. It also means targeting is bespoke.

Lastly, of course, technology matters. Richard Bejtlich argues that "the power to access data via unauthorised means inherently contains the power to destroy that data". This is indeed true in conventional IT security, or espionage, where confidentiality, integrity and availability of data have to be protected, in this order of priority: C-I-A. But, as the opposition knows, the same does not apply for industrial control systems—the golden target in "cyber-warfare".

For the engineers who run power plants, water facilities, or chemical factories, the highest priority is the stability of their plant's operations, not data confidentiality. The logic controllers that run critical processes are fragile systems—for that reason they should not be connected to the computers that company employees use to check their e-mail and browse the web. Truly critical systems are "air-gapped", physically disconnected. Or they are linked to a company network with a so-called unidirectional gateway, known as "data diodes". This is like a Gore-Tex jacket for a turbine: it can "sweat" data out, but it doesn't get wet when it rains. True: some systems that should not be connected to the internet indeed are, but not the most critical ones like nuclear plants.

In sum: stolen and occasionally deleted data are a problem of major proportions, not just a risk. But a cyber-attack that could cause the pain and damage that, say, even a small air-force bombing campaign could cause—that is in the realm of fiction, not fact.

Countermeasures solve

**Zenko and Cohen 12** (Micah Zenko, Fellow in the Center for Preventive Action at the Council on Foreign Relations, and MIchael Cohen, Senior Fellow at the American Security Project, serves on the board of the National Security Network and has taught at Columbia University’s School of International and Public Affairs, served in the U.S. Department of State, former Senior Vice President at the strategic communications firm of Robinson, Lerer and Montgomery, bachelor’s degree in international relations from American University and a master’s degree from Columbia University, 3/14/2012, "Clear and Present Safety", yaleglobal.yale.edu/content/clear-and-present-safety)

A more recent bogeyman in national security debates is the threat of so-called cyberwar. Policymakers and pundits have been warning for more than a decade about an imminent “cyber–Pearl Harbor” or “cyber-9/11.” In June 2011, then Deputy Defense Secretary William Lynn said that “bits and bytes can be as threatening as bullets and bombs.” And in September 2011, Admiral Mike Mullen, then chairman of the Joint Chiefs of Staff, described cyberattacks as an “existential” threat that “actually can bring us to our knees.” Although the potential vulnerability of private businesses and government agencies to cyberattacks has increased, the alleged threat of cyberwarfare crumbles under scrutiny. No cyberattack has resulted in the loss of a single U.S. citizen’s life. Reports of “kinetic-like” cyberattacks, such as one on an Illinois water plant and a North Korean attack on U.S. government servers, have proved baseless. Pentagon networks are attacked thousands of times a day by individuals and foreign intelligence agencies; so, too, are servers in the private sector. But the vast majority of these attacks fail wherever adequate safeguards have been put in place. Certainly, none is even vaguely comparable to Pearl Harbor or 9/11, and most can be offset by commonsense prevention and mitigation efforts.

Empirics

Hirsh, chief correspondent – National Journal, frmr foreign editor – Newsweek, 7/23/’11

(Michael, “Here, There Be Dragons,” National Journal)

It all sounds terrifying until one begins to look a little more closely at the facts. Lynn cites only one successful penetration of U.S. classified computers used by the Defense Department or the intelligence community. That was in 2008, when a flash drive infected by a “foreign intelligence agency” was inserted into a U.S. military laptop in the Middle East and uploaded a spybot onto a network run by the U.S. Central Command. “That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control,” Lynn wrote in *Foreign* *Affairs* last year.

But little seems to have come of that beachhead. The vast majority of cyberattacks against the United States amount to spying or misguided mischief, without anything like the consequences envisioned in *War Games*. Warnings about cyberspying and malevolent hacking have been around for more than 10 years. Even today, however, most experts believe that known rogue actors, such as al-Qaida and other terrorist groups, don’t have anything close to the technical sophistication to infiltrate the U.S. defense or intelligence computer system.

The occasional global hackers who have cropped up—one prominent example was “Lulz Security,” a pirate hacker group that appeared suddenly this year and then abruptly disbanded—have done little but paralyze servers and act as an annoyance. (WikiLeaks succeeded in breaking into the State Department computers, but only because it had an inside accomplice: Army Pvt. Bradley Manning, according to authorities.) As far as nation-states go, the Cold War principle of deterrence is still operative: What you do to us, we can do to you—and more. Indeed, China, which desperately seeks to restrict Internet freedom and this year arrested hundreds of people for fear that a “Jasmine Spring” could imitate the Arab Spring, seems more worried about battening down its own cyberhatches even as it probes our own.

Countermeasures solve

Bailey, science correspondent – Reason Magazine, 1/18/’11

(Ronald, <http://reason.com/archives/2011/01/18/cyberwar-is-harder-than-it>)

Brown and Sommer observe that the Internet and the physical telecommunications infrastructure were designed to be robust and self-healing, so that failures in one part are routed around. “You have to be cautious when hearing from people engaging in fear-mongering about huge blackouts and collapses of critical infrastructures via the Internet,” says University of Toronto cyberwarfare expert Ronald Deibert in the January/February 2011 issue of the *Bulletin of the Atomic Scientists*. “There is a lot of redundancy in the networks; it’s not a simple thing to turn off the power grid.” In addition, our experience with current forms of malware is somewhat reassuring. Responses to new malware have generally been found and made available within days and few denial of service attacks have lasted more than a day. In addition, many critical networks such as those carrying financial transactions are not connected to the Internet requiring insider information to make them vulnerable.

## 2NC - Diplomacy Solves

US is specifically pursuing peaceful uses of space now—creates international consensus for a space code of conduct.

Huntley ‘11

(Wade, senior lecturer in the National Security Affairs department at the Naval Postgraduate School in Monterey, California, “The 2011 U.S. National Space Security Policy: Engagement as a Work in Progress”, Disarmament Times, Spring, http://disarm.igc.org/index.php?option=com\_content&view=article&id=429:the-2011-us-national-space-security-policy-engagement-as-a-work-in-progress&catid=154:disarmament-times-spring-2011&Itemid=2)

As is well understood, the space policies of the Bush administration were decidedly oriented toward military security concerns and independent action. The 2006 National Space Policy unabashedly proclaimed the U.S. intention to maintain a dominant position in space indefinitely. This policy orientation dismissed multilateral cooperation as impinging on U.S. “freedom of action,” throwing weight instead behind a wide range of technology development initiatives founded on the assumption that deployment of weapons in space was, if not already factual, certainly inevitable.2 U.S. commercial and civil engagement was overshadowed by these security concerns, expressed through the tightening of export control restrictions inhibiting a broad range of technology sharing. Once again, U.S. space policy was subsumed by other national priorities, in this case dominated by military security concerns. This background is essential for appreciating how the space policies of the Obama administration are beginning **to genuinely break new trails.** The U.S. National Space Policy issued in June 2010 has been **widely recognized** for its cooperative and multilateral tone, including as explicit near-term goals the expansion of international cooperation on all activities and pursuing international as well as national measures to enhance space stability. Particularly notable are the document’s emphasis on orienting U.S. “leadership” toward fostering international cooperation, and its references, in its concluding section, to cooperation with other states and non-state actors in the pursuit of national security space objectives.3 Less broadly noticed was this policy’s clarity and coherence in articulating a vision for U.S. space activities on its own terms. The document is organized around core principles, subsidiary goals and implementing guidelines that exceed its predecessors in delineating a longer-term direction for U.S. space policy that is integrated with, rather than derivative of, broader U.S. global aims.4 The policy also was generated and issued far earlier in the tenure of the administration than either of its predecessors, indicating an increased prioritization of attention to space policy at higher levels of policy-making. To some degree, a turn toward multilateral cooperation in U.S. space policy was to be expected. China’s 2007 anti-satellite weapon (ASAT) test and the 2009 Iridium-Cosmos collision increased awareness of the challenge of space debris and the need for better global information sharing on space situational awareness (SSA).5 Also, new budget realities and unpromising technological developments have scaled back ambitions in some quarters for solving U.S. space security concerns with new independent capabilities. Finally, the Obama administration has pursued a more cooperative disposition across a wide range of global policy challenges, from Iranian nuclear ambitions to global climate change. But the improved clarity of vision in the 2010 Space Policy suggests that the emphasis on fostering global cooperation on space-related activities is more grounded in deliberate foresight than sailing the prevailing political winds. The 2011 National Security Space Strategy, released February 4, is best interpreted against this background of the Obama administration’s turn toward both greater international space cooperation and greater attention to space policy in general. This first-of-its-kind strategic statement culminates a congressionally mandated space posture review.6 The initial section portraying the strategic environment to which U.S. security policy must be responsive highlights the growing problems of space debris, orbital congestion and coordination among a growing number of space actors — not state-based security threats per se. The Security Space Strategy features the objective of a “stable space environment in which nations exercise shared responsibility.”7 Specific provisions intended to implement this strategy, relevant to the preceding observations, include:8 • The strategy presents a full section on “Partnering with Responsible Nations, International Organizations, and Commercial Firms.” This category is not wholly multilateral in the traditional sense, displaying a symbiosis of alliance-building and collective cooperation not always carefully distinguished; i.e., “The United States will lead in building coalitions of like-minded space-faring nations and, where appropriate, work with international institutions to do so.” • The strategy intends to “encourage responsible behavior in space and lead by the power of example,” a significant observation given the tendency of U.S. policy-makers (as noted above) not to expect quid pro quo responses to cooperative gestures. Also, the strategy states the U.S. “will support development of data standards, best practices, **t**ransparency and **c**onfidence-**b**uilding **m**easure**s**, and *norms of behavior for responsible space operations*.” [italics added] In the context of the section on “Preventing and Deterring Aggression,” the strategy similarly intends to “support diplomatic efforts to promote norms of responsible behavior in space” as well as “pursue international partnerships that encourage potential adversary restraint,” along with other measures. **This emphasis on norm-building and the role of example suggests a near-term endorsement of the development of “codes of conduct” for space activities** (such as the recently revised European Union Code of Conduct, discussed below), whether or not such concord leads to more formal arms control arrangements in the longer-term. • The Department of Defense is directed to “foster cooperative SSA relationships,” and to “expand provision of safety of flight services to U.S. Government agencies, other nations, and commercial firms.” Greater SSA information sharing has been a key suggestion for fostering international cooperation; the U.S. possesses globally superior SSA capabilities, but restricts the sharing of this information on the basis of national security concerns.9 Hence, this nominal commitment is significant in its own right. • The strategy commits to reforming export controls. “In particular, as new opportunities arise for international collaboration, a revised export control system will better enable the domestic firms competing for these contracts.” As noted above, the oppressive impact of current U.S. export controls not only impinges on U.S. commercial space actors but also epitomizes the high degree to which U.S. policy has subsumed commercial and civil interests to national security concerns. The strategy appears to acknowledge this connection and commit to remedy it. • The most assertive passages of the statement are moderated with community-building intent. For example, the strategy’s section on “Preventing and Deterring Aggression” concludes that the U.S. “will retain the right and capabilities to respond in self-defense, should deterrence fail,” but immediately adds that the U.S. “will use force in a manner that is consistent with longstanding principles of international law, treaties to which the United States is a party, and the inherent right of self defense.” • The concluding and most conflict-oriented section of the strategy opens by noting that “some actors may still believe counterspace actions could provide military advantage.” Counterspace capabilities, unarticulated in the document, include ASATs, ground-based directed energy weapons and satellite transmission jamming. Deputy Assistant Secretary of Defense for Space Policy Gregory Schulte explained at the strategy’s rollout that China is a principal concern in this regard, but so is the proliferation of these technologies: “If Ethiopia can jam a commercial satellite, you have to worry what others can do.”10 This section of the strategy does not, however, call for maintaining options to develop complementary space conflict capabilities. Rather, the strategy asserts that the U.S. “must be prepared to ‘fight through’ a degraded environment,” and identifies “resilience” and “space protection” as the key criteria. The preceding survey of elements of the 2011 National Security Space Strategy is deliberately selective, highlighting those elements expressing consistency with the 2010 National Space Policy’s bend toward fostering greater international collaboration. Perhaps as striking as the prevalence of such passages, however, is the absence of expressed intention — even couched in hedging language — to sustain or expand the kind of independent space-based military capabilities that were the centerpiece of the prior administration’s aims (if not its accomplishments). Again, to some extent this turn in tone is overdetermined by extenuating global circumstances. But one must still be struck by the degree to which developments such as the Chinese ASAT test have not ignited the kind of response one might have anticipated only a few short years after Donald Rumsfeld’s notorious warning of a “space Pearl Harbor.”11 The most immediate significance of the National Security Space Strategy is likely the signals its sends concerning U.S. policy toward the recently revised European Union Code of Conduct.12 The strategy did not explicitly endorse this EU initiative, but Mr. Schulte, at the February 4 presentation of the strategy, highlighted the initiative “as a potential way” to promote “transparency and confidence-building measures, which tend to be voluntary as opposed to legally binding.” A week earlier, Rose Gottemoeller, Assistant Secretary of State for Arms Control, Verification and Compliance, stated at the Conference on Disarmament that the administration was nearing a decision on whether the U.S. would sign on to the code, and what modifications might be required in order to do so.13 As U.S. interest in the Code of Conduct has increased, debates over its provisions and its relationship to the Outer Space Treaty have intensified. These policy movements toward multilateral engagement and commitment to behavioral standards (even if non-binding) mark a sharp departure from the stiff resistance to curtailing U.S. “freedom of action” in the previous administration, and have accordingly generated resistance from congressional opponents on just those terms. Prior to the release of the National Security Space Strategy, a group of 37 Republican senators led by Arizona Senator Jon Kyl issued a letter to Secretary of State Hillary Rodham Clinton expressing concern over a potential multilateral commitment that might limit development and/or deployment of space-based missile defense interceptors and ASAT-defeating systems.14 Critics also decried the strategy’s emphasis on “the old fallacious assumption that the power of example will prevent adversaries from doing the United States harm,” and endorsed maintaining the goal of U.S. retention of a “dominant position in military and intelligence space capabilities.”15 In fact, the administration’s warming toward normative commitments in general — and the EU Code of Conduct in particular — are in part intended to forestall pressure for more formal and binding measures that would definitively cut off the “hedge” of unilateral U.S. weapons development options.16 The balance of U.S. debate may have shifted toward greater international cooperation, but the terms of the debate remain the same. In sum, the National Security Space Strategy appears to mark not only a swing in U.S. policy toward greater global engagement but also, and more importantly, a step toward greater long-term coherence in thinking concerning the core goals of U.S. space activities. Even supporters of the general directions of the strategy noted its more-than-expected breadth of thought.17 But if this reading is sound, the strategy is still but one step on a long road, and ongoing debates over the role of U.S. space policy vis-à-vis broader national security interests will insure that road is bumpy. Suggesting such limitations, Mr. Schulte acknowledged that the classified version of the strategy is only four pages longer than the released version, indicating that more specific guidelines for military implementation of the strategy remain to be developed.18 Many devils may lurk in these details.

Diplomacy solves tensions

Zhang 11

Baohui Zhang, Professor of Political Science and Director of the Center for Asia Pacific Studies at Lingnan University, Hong Kong, Asian Survey, March/April 2011, “The Security Dilemma in the U.S.-China Military Space Relationship”, Pg 328-31, Vol. 51, No. 2, <http://www.jstor.org/action/showArticleInfo?doi=10.1525%2FAS.2011.51.2.311>

Important changes in U.S. strategic posture, missile defense, and the Taiwan Strait situation may now allow Washington and Beijing to extricate themselves from their space security dilemma, paving the way for arms control. In fact, these changes have already led to rising optimism among Chinese security experts with regard to the possibility of arms control in outer space. Zhao Kejin, a space security expert at Qinghua University, argues that there is no need for China to “engage the U.S. in a space arms race.” Instead, “Facing the possibility of emerging anarchy in outer space, China and the U.S. can work together to push for arms control negotiations, with the aim of establishing effective mechanisms for the monitoring and management of outer space.” 50 This upbeat mood among Chinese experts represents a big change from the pessimism of the Bush era. The challenge for China and the U.S. is to seize the opportunity and forge a realistic approach to space arms control. In this regard, China and the U.S. could pursue a two-stage strategy. The first stage would have to focus on reducing strategic misunderstandings and thus the vicious effects of the security dilemma. If so, the root cause of the action/counteraction spiral that defines a classic arms race will lose its hold on the two countries. Recent and important changes in the strategic landscape have improved the chances of achieving such a goal. Once the vicious circle of action and counteraction has been minimized, China and the U.S. could move on to the second stage, which is to pursue multilateral agreements banning weapons in space. Until recently, because of the Bush administration’s steadfast opposition to any legally binding treaty that would limit the U.S.’s military use of space, a multilateral approach to arms control seemed beyond reach. Now, however, the Obama administration’s willingness to take a leadership role in constructing a global treaty offers the hope of success. In the context of the changing strategic landscape between China and the U.S., specific measures could be taken to reduce their mutual concerns. One important measure, often overlooked in the space relationship, is for top civilian leaders to exercise greater oversight over military space programs. Often, statements and actions by the military have driven the fears of the other side. If the U.S. and China intend to build a new partnership in world affairs, civilian leaders must recognize that unscrutinized actions by their own militaries can invite mutual mistrust, which in turn hinders broader political and security cooperation. On the U.S. side, the Obama government needs to take a much closer look at the U.S. Air Force (especially its Space Command) and the Missile Defense Agency. These two institutions periodically try out new space projects that China and Russia perceive as threatening to their national security. For example, in October 2005 the U.S. Air Force conducted a maneuverability experiment with its XSS-11 microsatellite. According to internal Air Force studies, the XSS program was intended as a precursor to an anti-satellite program. Theresa Hitchens, a longtime watcher of the U.S. military space program, suggests that both Congress and the White House should exercise much tighter control over military space programs. She noted during an interview that the U.S. military’s move toward space warfare is a strategic issue with a lot of potential fallout. Thus, the military cannot make that decision on its own. As Hitchens said, “Congress hasn’t asked about this. Congress hasn’t debated this. There hasn’t been a change of White House policy and therefore there has been no public debate. And I think it is a serious mistake. This is something that ought to be debated at the national level with congressional and public input. It’s a bigger deal than just a military decision.” 51 China’s civilian leadership must also rein in the military space program. Indeed, after the 2007 ASAT test, some U.S. experts questioned whether the Chinese civilian leadership fully grasped the issue. Just as many U.S. projects have caused concern in China and Russia, the Chinese leadership must recognize that its own military space projects may be worrying U.S. decision makers. Thus, China’s political leadership needs to understand that restraining its military space program will be vital for forging security cooperation with the U.S.

UN vote count proves support for a ban

Krepon 05

Michael Krepon, Co-Founder of the Henry L. Stimson Center and a Diplomat Scholar at the University of Virginia, Henry L. Stimson Center, 2005, “Space Security or Space Weapons”, http://www.gsinstitute.org/docs/Stimson\_Space\_brief.pdf

On August 12th 2003, 174 nations voted “Yes” on a UN resolution to prevent an arms race in outer space. Only four countries abstained: the Federated States of Micronesia, the Marshall Islands, Israel, and the United States.

Multiple trends solve

Moltz 07

James Clay Moltz, associate director and research professor with the Center for Nonproliferation Studies at the Monterey Institute of International studies, Space Policy, November 2007, "Protecting Safe Access to Space: Lessons from the First 50 Years of Space Security”, Vol. 23, page 204, <http://www.sciencedirect.com/science/article/pii/S0265964607000860>

If these are some of the lessons of the past 50 years of space security, what can be said of the next 50 years? Undoubtedly, new national actors will emerge calling for the deployment of space-based weapons of various sorts to deter or defend against real, anticipated, or even hypothetical threats. At the same time, however, improved space situational awareness in many countries will greatly reduce the chances for national breakout and increase international knowledge of the problem of space debris. Similarly, the rise of new, non-military actors in space, including private companies offering new space services, universities, and new international consortia involved in science, commerce, and human exploration will begin to reduce the comparative weight of hostile actors and their militaries, who tended to dominate the early decades of space activity. These factors could increase the prospects for cooperative outcomes in space.

## 2NC - No Space Weapons

There is zero reason to weaponize

Krepon 11

Michael Krepon, co-founder of the Henry L. Stimson Center and the Diplomat Scholar at the University of Virginia. He is the author or editor of 13 books, Institute for National Strategic Studies, 2011, “Preserving Freedom of Action in Space: Realizing the Potential and Limits of U.S. Spacepower", <http://www.ndu.edu/press/lib/pdf/spacepower/spacepower.pdf>

These dilemmas are widely, but not universally, recognized. Together with the widespread public antipathy to elevating humankind's worst practices into space, they help explain why the flight-testing and deployment of dedicated space weapons have not become commonplace. These capabilities are certainly not difficult to acquire, as they are decades old. Indeed, tests of dedicated ASAT weapons have periodically occurred, and such systems were deployed for short periods during the Cold War. If the weaponization of space were inevitable, it surely would have occurred when the United States and the Soviet Union went to extraordinary lengths to compete in so many other realms. The weaponization of space has not occurred to date and is not inevitable in the future because of strong public resistence to the idea of weapons in space, and because most national leaders have long recognized that this would open a Pandora's box that would be difficult to close. Much has changed since the end of the Cold War, but the fundamental dilemmas of space control, including the linkage of satellites to nuclear deterrence among major powers, have not changed. The increased post– Cold War U.S. dependence on satellites makes the introduction of dedicated space weapons even more hazardous for national and economic security. Advocates of muscular space control must therefore take refuge in the fallacy of the last move, since warfighting plans in space make sense only in the absence of successful countermoves. Offensive counterforce operations in space do not come to grips with the dilemmas of spacepower, since proposed remedies are far more likely to accentuate than reduce satellite vulnerability. This analysis leads inexorably to a deeply unsatisfactory and yet inescapable conclusion: Realizing the enormous benefits of spacepower depends on recognizing the limits of power. The United States now enjoys unparalleled benefits from the use of space to advance national and economic security. These benefits would be placed at risk if essential zones in space become unusable as a result of warfare. Spacepower depends on the preservation and growth of U.S. capabilities in space. Paradoxically, the preservation and growth of U.S. spacepower will be undercut by the use of force in space. Because the use of weapons in or from space can lead to the loss or impairment of satellites of all major space powers, all of whom depend on satellites for military and economic security, we believe it is possible to craft a regime based on self-interest to avoid turning space into a shooting gallery. This outcome is far more difficult to achieve if major space powers engage in the flight-testing and deployment of dedicated ASAT weapons or space-to-Earth weapons. We therefore argue that it would be most unwise for the United States, as the spacepower with the most to lose from the impairment of its satellites, to initiate these steps. Similar restraint, however, needs to be exercised by other major spacefaring nations, some of which may feel that the preservation and growth of U.S. spacepower are a threat, or that it is necessary to hold U.S. space assets at risk. The United States is therefore obliged to clarify to others the risks of initiating actions harmful to U.S. satellites without prompting other spacefaring nations to take the very steps we seek to avoid. Consequently, a preservation and growth strategy for U.S. spacepower also requires a hedging strategy because, even if the United States makes prudent decisions in space, others may still make foolish choices.

Economic incentives outweigh

Krepon 05

Michael Krepon, Co-Founder of the Henry L. Stimson Center and a Diplomat Scholar at the University of Virginia, Henry L. Stimson Center, 2005, “Space Security or Space Weapons”, http://www.gsinstitute.org/docs/Stimson\_Space\_brief.pdf

Why hasn’t space become a shooting gallery? One reason is that satellites serve as the eyes and ears of nations that have nuclear weapons. An attack on satellites could therefore trigger a nuclear war. Second, satellites are very vulnerable. The nation that starts a space war would have great difficulty protecting its satellites. Third, space warfare would cause debris, and debris lingers and kills indiscriminately in space. Fourth, satellites support global business and commerce. Every nation would be harmed by a space war. Lastly, space is widely viewed as a global commons that should remain a sanctuary blessedly free from the disputes that plague us on planet Earth.

# 1NR

## 2nc ov

Howell ‘7

William, professor of political science at U-Chicago, and Jon C. Pevehouse, professor of Political Science UW-Madison, “While Dangers Gather : Congressional Checks on Presidential War Powers,” 2007 ed.

SIGNALING RESOLVE To the extent that congressional discontent signals domestic irresolution to other nations, the job of resolving a foreign crisis is made all the more difficult. As Kenneth Schultz shows, an ''opposition party can undermine the credibility of some challenges by publicly opposing them. Since this strategy threatens to increase the probability of resistance from the rival state, it forces the government to be more selective about making threats "—and, concomitantly, more cautious about actually using military force.'4 When members of Congress openly object to a planned military operation, would-be **adversaries** of the United States may feel emboldened, believing that the president lacks the domestic support required to see a military venture through. Such nations, it stands to reason, will be more willing to enter conflict, and if convinced that the United States will back down once the costs of conflict are revealed, they may fight longer and make fewer concessions. Domestic political strife, as it were, weakens the ability of presidents to bargain effectively with foreign states, while increasing the chances that military entanglements abroad will become **protracted and unwieldy.** A large body of work within the field of international relations supports the contention that a nation's ability to achieve strategic military objectives in short order depends, in part**,** on the head of state's **credibility in conveying political resolve.** Indeed, a substantial game theoretic literature underscores the importance of domestic political institutions and public opinion as state leaders attempt to credibly commit to war,75 Confronting widespread and vocal domestic opposition, the president may have a difficult time signaling his willingness to see a military campaign to its end, While congressional opposition may embolden foreign enemies, the perception on the part of allies that the president lacks support may make them wary of **committing any troops at all.**

Also causes rollback/circumvention

Laura Young, Ph.D., Purdue University Associate Fellow, June 2013, Unilateral Presidential Policy Making and the Impact of Crises, Presidential Studies Quarterly, Volume 43, Issue 2

A president looks for chances to increase his power (Moe and Howell 1999). Windows of opportunity provide those occasions. These **openings create an environment where the president faces little backlash from Congress, the judicial branch, or even the public**. Though institutional and behavioral conditions matter, domestic and international crises play a pivotal role in aiding a president who wishes to increase his power (Howell and Kriner 2008, 475). These events overcome the obstacles faced by the institutional make-up of government. They also allow a president lacking in skill and will or popular support the opportunity to shape the policy formation process. In short, focusing events increase presidential unilateral power.

Outweighs their mechanism

Laura Young, Ph.D., Purdue University Associate Fellow, June 2013, Unilateral Presidential Policy Making and the Impact of Crises, Presidential Studies Quarterly, Volume 43, Issue 2

During periods of crisis, the time available to make decisions is limited. Because the decision-making process is often arduous and slow in the legislative branch, it is not uncommon for the executive branch to receive deference during a crisis because of its ability to make swift decisions. The White House centralizes policies during this time, and presidents seize these opportunities to expand their power to meet policy objectives. Importantly, presidents do so with limited opposition from the public or other branches of government (Howell and Kriner 2008). In fact, despite the opposition presidents often face when centralizing policies, research shows policies formulated via centralized processes during times of crisis receive more support from Congress and the American people (Rudalevige 2002, 148-49). For several reasons, a crisis allows a president to promote his agenda through unilateral action. First, a critical exogenous shock shifts attention and public opinion (Birkland 2004, 179). This shift is a phenomenon known as the “rally round the flag” effect (Mueller 1970). The rally effect occurs because of the public's increase in “its support of the president in times of crisis or during major international events” (Edwards and Swenson 1997, 201). Public support for the president rises because he is the leader and, therefore, the focal point of the country to whom the public can turn for solutions. Additionally, individuals are more willing to support the president unconditionally during such times, hoping a “united front” will increase the chance of success for the country (Edwards and Swenson 1997, 201). As a result, a crisis or focusing event induces an environment that shifts congressional focus, dispels gridlock and partisanship, and increases positive public opinion—each of which is an important determinant for successful expansion of presidential power (Canes-Wrone and Shotts 2004; Howell 2003). In other words, a crisis embodies key elements that the institutional literature deems important for presidential unilateral policy making. The president's ability to focus attention on a particular issue is also of extreme importance if he wishes to secure support for his agenda (Canes-Wrone and Shotts 2004; Edwards and Wood 1999; Howell 2003; Neustadt 1990). The role the media play is pivotal in assisting a president in achieving such a result because of its ability to increase the importance of issues influencing the attention of policy makers and the priorities of viewers. Although it is possible a president can focus media attention on the policies he wishes to pursue through his State of the Union addresses or by calling press conferences, his abilities in this regard are limited, and the media attention he receives is typically short lived (Edwards and Wood 1999, 328-29). High-profile events, on the other hand, are beneficial because they allow the president to gain focus on his agenda. This occurs because the event itself generates attention from the media without presidential intervention. Thus, the ability of crises to set the agenda and shift media and public attention provides another means for overcoming the constraints placed upon the president's ability to act unilaterally. Finally, Rudalevige finds support that a crisis increases the success of presidential unilateral power even if the policy process is centralized. A crisis allows little time to make decisions. As a result, “the president and other elected officials are under pressure to ‘do something’ about the problem at hand” (2002, 89, 148). Because swift action is necessary, presidents rely on in-house advice. As a result, the policy formation process is centralized, and the president receives deference to unilaterally establish policies to resolve the crisis. During a crisis, the president has greater opportunity to guide policy because the event helps him overcome the congressional and judicial obstacles that typically stand in his way.2 This affords the president greater discretion in acting unilaterally (Wildavsky 1966). It is possible the institutional make-up of the government will align so that the president will serve in an environment supportive of his policy decisions. It is also likely a president will have persuasive powers that enable him to gain a great deal of support for his policy agenda. An event with the right characteristics, however, enhances the president's ability to act unilaterally, regardless of the institutional make-up of government or his persuasive abilities.

## a2 syria

Only constrains humanitarian operations

Goldsmith 8/31/13

Jack, Henry L. Shattuck Professor at Harvard Law School, where he teaches and writes about national security law, presidential power, cybersecurity, international law, internet law, foreign relations law, and conflict of laws. Before coming to Harvard, Professor Goldsmith served as Assistant Attorney General, Office of Legal Counsel from 2003–2004, and Special Counsel to the Department of Defense from 2002–2003. Professor Goldsmith is a member of the Hoover Institution Task Force on National Security and Law, “Obama’s Request to Congress Will Not Hamstring Future Presidents (Except for Some Humanitarian Interventions),” <http://www.lawfareblog.com/2013/08/obamas-request-to-congress-will-not-hamstring-future-presidents-except-for-some-humanitarian-interventions/>

Peter Spiro at OJ, and David Rothkopf of FP whom he cites, both say that President Obama’s request for congressional authorization for Syria will allow Congress to hamstring future Presidents from using military force. Rothkopf exaggerates when he says that President Obama reversed “decades of precedent regarding the nature of presidential war powers” by going to Congress here, and Spiro exaggerates when he says that this is “a huge development with broad implications . . . for separation of powers.” What would have been unprecedented, and a huge development for separation of powers, is a unilateral strike in Syria. Seeking congressional authorization here in no way sets a precedent against President using force in national self-defense, or to protect U.S. persons or property, or even (as in Libya) to engage in humanitarian interventions (like Libya) with Security Council support. Moreover, the President and his subordinates have been implying for a while now that they will rely on Article II to use force without congressional authorization against extra-AUMF terrorist threats (and for all we know they already are). There is no reason to think that unilateral presidential military powers for national self-defense are in any way affected by the President’s decision today. That is as it should be. To the extent that Spiro is suggesting that **pure humanitarian interventions** might be harder for presidents to do unilaterally after today (I think this is what he is suggesting, but I am not sure), I agree. Kosovo is the only other real precedent here, and the Clinton administration never explained why it was lawful as an original matter. The constitutional problem with pure humanitarian interventions – and especially ones (like Kosovo and Syria) that lack Security Council cover, and thus that do not implicate the supportive Korean War precedent – is that Presidents cannot easily articulate a national interest to trigger the Commander in Chief’s authority that is not at the same time boundless. President Obama, like President Clinton before him in Kosovo, had a hard time making that legal argument because it is in fact a hard argument to make. That is one reason (among many others) why I think it was a good idea, from a domestic constitutional perspective, for the President in this context to seek congressional approval.

Syria is a link magnifier—it only constrains Obama with the plan

Bradley 9/2/13

Curtis, William Van Alstyne Professor of Law, Professor of Public Policy Studies, and Senior Associate Dean for Academic Affairs. He joined the Duke law faculty in 2005, after teaching at the University of Virginia and University of Colorado law schools. His courses include International Law, Foreign Relations Law, and Federal Courts. He was the founding co-director of Duke Law School’s Center for International and Comparative Law and serves on the executive board of Duke's Center on Law, Ethics, and National Security. Recently, he was appointed to serve as a Reporter on the American Law Institute's new Restatement project on The Foreign Relations Law of the United States., “War Powers, Syria, and Non-Judicial Precedent,” <http://www.lawfareblog.com/2013/09/war-powers-syria-and-non-judicial-precedent/>

One claim that is being made about President Obama’s decision to seek congressional authorization for military action in Syria is that it is likely to weaken the authority of the presidency with respect to the use of force. Peter Spiro contends, for example, that Obama’s action is “a watershed in the modern history of war power” that may end up making congressional pre-authorization a necessary condition for even small-scale military operations. David Rothkopf states even more dramatically that “Obama’s decision may have done more—for better or worse—to dial back the imperial presidency than anything his predecessors or Congress have done for decades.” If this claim is correct, it will be welcome news to those concerned about the growth of executive power and a matter of concern for those who are fans of robust executive unilateralism. Unfortunately, the commentators making this claim do not identify **the mechanism** through which the weakening of presidential war authority will occur and have relied instead only on vague intuitions. As an initial matter, we need to bracket the issue of whether Obama’s action will weaken his own power as a political matter. This is a complicated issue: on the one hand, it may signal weakness both to Congress and to other nations; on the other hand, if he obtains congressional authorization, he may be in an ultimately stronger political position, as Jack Goldsmith has pointed out. As I understand it, the claim being made by Spiro, Rothkopf, and others is that the power of the presidency more generally is being weakened. How might this happen? Not through an influence on judicial doctrine: Although courts sometimes take account of historic governmental practices when assessing the scope of presidential authority, they have consistently invoked limitations on standing and ripeness, as well as the political question doctrine, to avoid addressing constitutional issues relating to war powers. In the absence of judicial review, what is the causal mechanism by which the “precedent” of Obama seeking congressional authorization for the action in Syria could constrain future presidential action? When judicial review is unavailable, the most obvious way in which the President is constrained is through the political process—pressure from Congress, the public, his party, etc. In an extreme case, this pressure could take the form of impeachment proceedings, but it does not take such an extreme case for the pressure to have a significant effect on presidential decisionmaking. Indeed, it is easy to think of political considerations that might have motivated Obama to go to Congress with respect to Syria. That’s all fairly clear, but what is unclear is how a non-judicial precedent, such as Obama’s decision to seek congressional authorization for Syria, will have an effect on later decisions with respect to the use of force. The intuition, I think, is that Obama’s action will strengthen the hand of critics of later efforts by presidents to act unilaterally. It will give the critics more “ammunition,” so to speak. But why is this so, and what is meant, specifically, by “ammunition”? Obama claims that he is seeking congressional authorization for policy reasons, not because he is required to do so, and a later president is likely to reiterate that explanation. Moreover, if Obama is seeking congressional authorization for Syria because of political considerations (weak international and domestic support, public weariness about war, etc.), why would a later president feel compelled to follow that precedent when those political considerations do not apply? It is easier to imagine a constraining precedential effect, I think, if Congress votes down an authorization bill on Syria, and the President then declines to take action. After all, Obama has already stated that **he has made a decision as Commander in Chief to use force.** If he responds to a negative vote in Congress by not doing so, it might seem like a concession against interest that he lacks authority to act when Congress is opposed. Even if this did produce a constraining precedent, it would have limited effect, since it would not apply when (as is often the case) Congress does not take action one way or the other. But even here, the mechanism of the constraint is uncertain: Obama would likely claim that he was declining to take action for political reasons, such as the reduced likelihood of success created by the disunity between the branches, or the passage of time, or the lack of sufficient international support. Why would a future president facing different circumstances feel constrained by Obama’s inaction?

## at twilight

The aff’s abdication of executive war power authority to congress causes unchecked proliferation and destroys war fighting capabilities.

**Yoo ‘12**

John, Harvard University, B.A. Yale Law School, J.D. Law professor at Berkeley, former official in the United States Department of Justice, “War Powers Belong to the President,” <http://www.abajournal.com/magazine/article/war_powers_belong_to_the_president>

Common sense does not support replacing the way our Constitution has worked in wartime with a radically different system that mimics the peacetime balance of powers between president and Congress. If the issue were the environment or Social Security, Congress would enact policy first and the president would faithfully implement it second. But the Constitution does not duplicate this system in war. Instead, our framers decided that the president would play the leading role in matters of national security. Those in the pro-Congress camp call upon the anti-monarchical origins of the American Revolution for support. If the framers rebelled against King George III’s dictatorial powers, surely they would not give the president much authority. It is true that the revolutionaries rejected the royal prerogative, and they created weak executives at the state level. Americans have long turned a skeptical eye toward the growth of federal powers. But this may mislead some to resist the fundamental difference in the Constitution’s treatment of domestic and foreign affairs. For when the framers wrote the Constitution in 1787 they rejected these failed experiments and restored an independent, unified chief executive with its own powers in national security and foreign affairs. The most important of the president’s powers are commander in chief and chief executive. As Alexander Hamilton wrote in Federalist 74, “The direction of war implies the direction of the common strength, and the power of directing and employing the common strength forms a usual and essential part in the definition of the executive authority.” Presidents should conduct war, he wrote, because they could act with “decision, activity, secrecy and dispatch.” In perhaps his most famous words, Hamilton wrote: “Energy in the executive is a leading character in the definition of good government. ... It is essential to the protection of the community against foreign attacks.” The framers realized the obvious. Foreign affairs are unpredictable and involve the highest of stakes, making them unsuitable to regulation by pre-existing legislation. Instead, they can demand swift, decisive action—sometimes under pressured or even emergency circumstances—that is best carried out by a branch of government that does not suffer from multiple vetoes or is delayed by disagreements. Congress is too large and unwieldy to take the swift and decisive action required in wartime. Our framers replaced the Articles of Confederation, which had failed in the management of foreign relations because they had no single executive, with the Constitution’s single president for precisely this reason. Even when it has access to the same intelligence as the executive branch, Congress’ loose, decentralized structure would paralyze American policy while foreign threats grow. Congress has no political incentive to mount and see through its own wartime policy. Members of Congress, who are interested in keeping their seats at the next election, do not want to take stands on controversial issues where the future is uncertain. They will avoid like the plague any vote that will anger large segments of the electorate. They prefer that the president take the political risks and be held accountable for failure. Congress’ track record when it has opposed presidential leadership has not been a happy one. Perhaps the most telling example was the Senate’s rejection of the Treaty of Versailles at the end of World War I. Congress’ isolationist urge kept the United States out of Europe at a time when democracies fell and fascism grew in their place. Even as Europe and Asia plunged into war, Congress passed the Neutrality Acts designed to keep the United States out of the conflict. President Franklin Roosevelt violated those laws to help the Allies and draw the nation into war against the Axis. While pro-Congress critics worry about a president’s foreign adventurism, the real threat to our national security may come from inaction and isolationism. Many point to the Vietnam War as an example of the faults of the “imperial presidency.” Vietnam, however, could not have continued without the consistent support of Congress in raising a large military and paying for hostilities. And Vietnam ushered in a period of congressional dominance that witnessed American setbacks in the Cold War and the passage of the ineffectual War Powers Resolution. Congress passed the resolution in 1973 over President Richard Nixon’s veto, and no president, Republican or Democrat, George W. Bush or Obama, has ever accepted the constitutionality of its 60-day limit on the use of troops abroad. No federal court has ever upheld the resolution. Even Congress has never enforced it. Despite the record of practice and the Constitution’s institutional design, critics nevertheless argue for a radical remaking of the American way of war. They typically base their claim on Article I, Section 8, of the Constitution, which gives Congress the power to “declare war.” But these observers read the 18th century constitutional text through a modern lens by interpreting “declare war” to mean “start war.” When the Constitution was written, however, a declaration of war served diplomatic notice about a change in legal relations between nations. It had little to do with launching hostilities. In the century before the Constitution, for example, Great Britain—where the framers got the idea of the declare-war power—fought numerous major conflicts but declared war only once beforehand. Our Constitution sets out specific procedures for passing laws, appointing officers and making treaties. There are none for waging war because the framers expected the president and Congress to struggle over war through the national political process. In fact, other parts of the Constitution, properly read, support this reading. Article I, Section 10, for example, declares that the states shall not “engage” in war “without the consent of Congress” unless “actually invaded, or in such imminent danger as will not admit of delay.” This provision creates exactly the limits desired by anti-war critics, complete with an exception for self-defense. If the framers had wanted to require congressional permission before the president could wage war, they simply could have repeated this provision and applied it to the executive. Presidents, of course, do not have complete freedom to take the nation to war. Congress has ample powers to control presidential policy, if it wants to. Only Congress can raise the military, which gives it the power to block, delay or modify war plans. Before 1945, for example, the United States had such a small peacetime military that presidents who started a war would have to go hat in hand to Congress to build an army to fight it. Since World War II, it has been Congress that has authorized and funded our large standing military, one primarily designed to conduct offensive, not defensive, operations (as we learned all too tragically on 9/11) and to swiftly project power worldwide. If Congress wanted to discourage presidential initiative in war, it could build a smaller, less offensive-minded military. Congress’ check on the presidency lies not just in the long-term raising of the military. It can also block any immediate armed conflict through the power of the purse. If Congress feels it has been misled in authorizing war, or it disagrees with the president’s decisions, all it need do is cut off funds, either all at once or gradually. It can reduce the size of the military, shrink or eliminate units, or freeze supplies. Using the power of the purse does not even require affirmative congressional action. Congress can just sit on its hands and refuse to pass a law funding the latest presidential adventure, and the war will end quickly. Even the Kosovo war, which lasted little more than two months and involved no ground troops, required special funding legislation. The framers expected Congress’ power of the purse to serve as the primary check on presidential war. During the 1788 Virginia ratifying convention, Patrick Henry attacked the Constitution for failing to limit executive militarism. James Madison responded: “The sword is in the hands of the British king; the purse is in the hands of the Parliament. It is so in America, as far as any analogy can exist.” Congress ended America’s involvement in Vietnam by cutting off all funds for the war. Our Constitution has succeeded because it favors swift presidential action in war, later checked by Congress’ funding power. If a president continues to wage war without congressional authorization, as in Libya, Kosovo or Korea, it is only because Congress has chosen not to exercise its easy check. We should not confuse a desire to escape political responsibility for a defect in the Constitution. A radical change in the system for making war might appease critics of presidential power. But it could also seriously threaten American national security. In order to forestall another 9/11 attack, or to take advantage of a window of opportunity to strike terrorists or rogue nations, the executive branch needs flexibility. It is not hard to think of situations where congressional consent cannot be obtained in time to act. Time for congressional deliberation, which leads only to passivity and isolation and not smarter decisions, will come at the price of speed and secrecy. The Constitution creates a presidency that can respond forcefully to prevent serious threats to our national security. Presidents can take the initiative and Congress can use its funding power to check them. Instead of demanding a legalistic process to begin war, the framers left war to politics. As we confront the new challenges of terrorism, rogue nations and WMD proliferation, now is not the time to introduce sweeping, untested changes in the way we make war.

It’s sufficient to cause our impacts

Yoo 6—Professor of Law, UC-Berkeley (John, “Energy in the Executive: Re-examining Presidential Power in the Midst of the War on Terrorism,” The Heritage Foundation, 24 April 2006, <http://www.heritage.org/research/reports/2006/04/energy-in-the-executive-reexamining-presidential-power-in-the-midst-of-the-war-on-terrorism>, Accessed 6-19-2013)

On the other hand, congressional action has led to undesirable outcomes. Congress led us into two "bad" wars, the 1798 quasi-war with France and the War of 1812. Excessive congressional control can also prevent the U.S. from entering conflicts that are in the national interest. Most would agree that congressional isolationism before World War II harmed U.S. interests and that the United States and the world would have been far better off if President Franklin Roosevelt could have brought us into the conflict much earlier. Congressional participation does not automatically, or even consistently, produce desirable results in war decision-making. Critics of presidential war powers exaggerate the benefits of declarations or authorizations of war. What also often goes unexamined are the potential costs of congressional participation: delay, inflexibility, and lack of secrecy. Legislative deliberation may breed consensus in the best of cases, but it also may inhibit speed and decisiveness. In the post-Cold War era, the United States is confronting several major new threats to national security: the proliferation of WMD, the emergence of rogue nations, and the rise of international terrorism. Each of these threats may require pre-emptive action best undertaken by the President and approved by Congress only afterwards. Take the threat posed by the al-Qaeda terrorist organization. Terrorist attacks are more difficult to detect and prevent than those posed by conventional armed forces. Terrorists blend into civilian populations and use the channels of open societies to transport personnel, material, and money. Despite the fact that terrorists generally have no territory or regular armed forces from which to detect signs of an impending attack, weapons of mass destruction allow them to inflict devastation that once could have been achievable only by a nation-state. To defend itself from this threat, the United States may have to use force earlier and more often than was the norm during the time when nation-states generated the primary threats to American national security. In order to forestall a WMD attack, or to take advantage of a window of opportunity to strike at a terrorist cell, the executive branch needs flexibility to act quickly, possibly in situations where congressional consent cannot be obtained in time to act on the intelligence. By acting earlier, perhaps before WMD components have been fully assembled or before an al-Qaeda operative has left for the United States, the executive branch might also be able to engage in a more limited, more precisely targeted, use of force. Similarly, the least dangerous way to prevent rogue nations from acquiring weapons of mass destruction may depend on secret intelligence gathering and covert action rather than open military intervention. Delay for a congressional debate could render useless any time-critical intelligence or windows of opportunity.

No link turns—not a fast enough op tempo to win fourth-gen conflicts.

Howell ‘7

William, professor of political science at U-Chicago, and Jon C. Pevehouse, professor of Political Science UW-Madison, “While Dangers Gather : Congressional Checks on Presidential War Powers,” 2007 ed.

In foreign policy making generally, and on issues involving the use of force in particular this feature of unilateral powers reaps special rewards. If presidents had to build broad-based consensus behind every deployment before any military planning could be executed, most ventures would never get off the ground. Imagine having to explain to members of Congress why events in Liberia this month or Ethiopia the next demand military action, and then having to secure the formal consent of a supermajority before any action could be taken. The federal government could not possibly keep pace with an increasingly interdependent world in which every region holds strategic interests for the United States. Because presidents, as a practical matter, can unilaterally launch ventures into distant locales without ever having to guide a proposal through a circuitous and uncertain legislative process, they can more effectively manage these responsibilities and take action when **congressional deliberations** often result in gridlock. It is no wonder, then, that in virtually every system of governance, executives [not legislatures or courts) mobilize their nations through wars and foreign crises. Ultimately, it is their ability to act unilaterally that enables them to do so. in sum, the advantages of unilateral action arc significant: they allow the president to move first and move alone.

Congressional involvement causes extinction

**Li ‘9**

Zheyao, J.D. candidate, Georgetown University Law Center, 2009; B.A., political science and history, Yale University, 2006. This paper is the culmination of work begun in the "Constitutional Interpretation in the Legislative and Executive Branches" seminar, led by Judge Brett Kavanaugh, “War Powers for the Fourth Generation: Constitutional Interpretation in the Age of Asymmetric Warfare,” 7 Geo. J.L. & Pub. Pol'y 373 2009

On the other hand, the slow-moving, deliberative Congress has no role to play in authorizing military action against non-state actors in the fourth generation of warfare. The President must have the ability to react quickly in conducting offensive military action against these transnational enemies, both in response to terrorist attacks that have already occurred and to prevent imminent attacks. Congress's powers over the initiation of war or the seeking of peace have no role in this civilizational conflict against extremist terrorists who will not rest until they destroy the United States and who have made such intentions known. In light of the fundamental difference in the nature of the threats posed, the nature of the adversaries, and the different strategies and tactics necessary to combat them, these parallel constitutional decision-making processes in the area of war-one conforming to the Framers" conception of traditional Westphalian warfare against nation-states, and the other adapting to the realities of asymmetric warfare waged by non-state actors-are both necessary to ensure the survival and prosperity of the United States in the twenty-first century and beyond.

Guarantees missed windows of opportunity

Yoo 4—Professor of Law, UC-Berkeley (John, “War, Responsibility, and the Age of Terrorism,” Berkeley Law, <http://works.bepress.com/cgi/viewcontent.cgi?article=1015&context=johnyoo>)

In order to weigh the advantages of the Congress-first approach, it is also important to understand its potential costs. The costs may not be obvious, since grounding the use of force in ex ante congressional consent bears a close resemblance to the process for enacting legislation. The legislative process increases the costs of government action. It is heavily slanted against the enactment of legislation by requiring the concurrence not just of the popularly elected House but also the state-representing Senate and the President. 50 This raises decision costs by increasing the delay needed to get legislative concurrence, requiring an effort to coordinate between executive and legislature, and demanding an open, public discussion of potentially sensitive information. Decision costs are not encapsulated merely in the time-worn hypotheticals that ask whether the President must go to Congress for permission to launch a preemptive strike against a nation about to launch its own nuclear attack. Rather, these decision costs might arise from delay in using force that misses a window of opportunity, or one in which legislative discussion alerts an enemy to a possible attack, or the uncertainty over whether congressional authorization will be forthcoming.

## link—OCOs

Plan destroys executive commander-in-chief supremacy—cyber capabilities are the key

Lorber ’13

Eric, J.D. Candidate, University of Pennsylvania Law School, Ph.D Candidate, Duke University Department of Political Science, “Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?,” 15 U. Pa. J. Const. L. 961

Yet a surprising amount of uncertainty exists as to which - if any - domestic laws constrain the use of OCOs and how they fit into the congressional-executive balance. As policymakers, scholars, and journalists have lamented, a coherent policy framework governing the use of OCOs does not exist and many questions remain unanswered. n8 Would an attack [\*963] using cyber weapons trigger the requirements of the War Powers Resolution? n9 Would OCOs be subject to reporting requirements under the Intelligence Authorization Act? n10 Conversely, do cyber operations grant the executive branch another tool with which it can prosecute attacks but avoid reporting and responding to congressional inquiries? These questions are largely unanswered both because the rise of OCOs is a relatively recent phenomenon and because much of the information about U.S. technical capability in this field is highly classified. n11 Yet addressing these questions is increasingly important for two reasons. First, as states such as China, Israel, Russia, and the United States use these weapons now and likely will do so more in future conflicts, determining the domestic legal strictures governing their use would provide policymakers and military planners a better sense of how to operate in cyberspace. n12 Second, the possible employment of these tools adds yet another wrinkle to the battle between the executive and legislative branches over war-making authority. n13 In particular, if neither the War Powers Resolution nor the Intelligence Authorization Act governs OCOs, the executive may be allowed to employ U.S. military power in a manner largely unchecked by congressional authority. n14 As a result, the employment of these tools [\*964] implicates - and perhaps problematically shifts - the balance between the executive's commander-in-chief power n15 and Congress's war-making authority. n16 This Comment provides an initial answer to the question of whether current U.S. law can effectively govern the Executive's use of OCOs. n17 It explores the interaction between this new tool and the current statutory limits on presidential war-making authority, with a particular focus on whether the two current federal laws meant to restrict executive power in this field - the War Powers Resolution n18 and the Intelligence Authorization Act n19 - apply to a wide range of potential offensive cyber operations undertaken by the executive branch. Beyond suggesting that neither the War Powers Resolution nor the Intelligence Authorization Act can effectively regulate most types of offensive cyber operations, this Comment suggests that while marginally problematic for a proper balance of war-making power between the executive and legislative branches, this lack of oversight does not fundamentally shift the current alignment. It does argue, however, that - given this lack of regulatory oversight - **the President now has another powerful war-making tool to use at his discretion**. Finally, the Comment suggests that this lack of limitation may be positive in some ways, as laying down clear legal markers before having a developed understanding of these capabilities may problematically limit their effective use.

## 2nc—OCOs

It’s the key issue

Healey et al ‘13

Jason, Director, Cyber Statecraft Initiative, The Atlantic Council Moderator: Harvey Rishikof, Chair, American Bar Association (ABA) Advisory Standing Committee on Law and National Security; Co-chair, ABA Taskforce on Cyber and Security Speakers: Tom Bossert, President, Civil Defense Solutions; Andrew Grotto, Professional Staff Member, Select Committee on Intelligence, U.S. Senate; Jason Healey, Director, Cyber Statecraft Initiative, Brent Scowcroft Center on International Security, The Atlantic Council; Derek Khanna, Political Consultant, Former Professional Staffer, Republican Study Committee, U.S. House of Representatives, “"The Role of Congress in Cyber Conflict"

MR. HEALEY: Thank you very much. Now, we want to start out -- it's clear that the administration has **and** deserves **wide latitude** in deciding on a lot of these issues under their constitutional authority **in Article Two** of the Constitution. So I absolutely do support that, you know, especially with Congress having granted significant authority under the authorization to use military force in the days after 9/11. So as a -- but as a legal matter or as a policy matter, there's two or three aspects that I just wanted to touch on really briefly. First, one of the reasons we're holding this conference today, this event today, was DOD's response to Congress in what's called the Section 934 report, which covered a lot of their cyber policy -- it was for the NDAA -- where essentially they were saying that they would -- that the Department of Defense would essentially never -- they didn't say never, but they didn't really see why they would ever have to report a cyberconflict to Congress because they -- because it did not seem U.S. troops would ever come into harm's way. And if U.S. troops weren't going to come into harm's way, which seems to be the traditional reading of the War Powers Resolution, then Congress really didn't have a role. And that struck me as an answer I wasn't necessarily comfortable with and that probably needs some examination by some smart people here, especially because I think there's more reasons to be cautious in cyberconflict than in other areas, for in cyberspace the future is still a jump ball. It's not like conflict in the air, the land or the sea, where we've got hundreds of years of practice between states and law and understanding the interaction. We're brand new into this age. You know, we're really 25 years in for what we're thinking is cyberconflict. And especially because of the role of the private sector, I'm **very cautious** in looking for more control -- I don't want to say "control" is the wrong word, but more caution on behalf of the executive branch and more checks and balances than we might do, because it could be that if we have -- if we're very aggressive with offense today, it might lead to a far worse cyberspace for all of us tomorrow. Cyberspace may be very -- more sensitive to conflict and state-sponsored conflict that will make it far worse tomorrow. And then we can talk about more of that later. I'd also like to just say I don't believe it's just about the War Powers Resolution. It also fits into Title 10, Title 50, the role of covert actions in this, the role of very aggressive intelligence gathering, as well as traditional -- you know, things that under the War Powers might be considered traditional military authorities, but that might be more aggressive than we might want to have unchecked. Thank you. MR. RISHIKOF: OK. Great. I know you're going to have thoughts on this, Derek. DEREK KHANNA: Absolutely. I want to kind of go to a little bit more macro of a level here. Obviously, the Obama interpretation of the War Powers Resolution is essentially, if American ground troops are involved, if there isn't a real threat to our armed forces, well, then this antiquated law doesn't really go into effect. Well, that's really problematic for a number of reasons. It's problematic because it seems to misunderstand the context surrounding the War Powers Resolution. And it's really disturbing, particularly in the context of cyberwar, which it's difficult to predict in the future, but at least in concept -- and I can't imagine a situation where cyberwar would involve the use of U.S. armed forces. You could have an espionage situation, but I digress. So cyberwar presents a whole bunch of new opportunities along the lines that we've already experienced in Libya. And so we have to wonder, how are we going to continue to constrain the executive power in war making if the future of war making is going to involve cyberwar, not necessarily just as a tool of the executive but perhaps the main instrument of war making in the future, as we've already seen that drone warfare has become a main instrument of warfare in a particular theater. And so it's very critical that we're able to establish checks and balances upon the executive there. And the -- and an additional problem here is we often hear sometimes from conservative audiences that, you know, the power of the purse is the main control upon executive power. Well, when you have cyberwar being initiated by intelligence agencies, it's very difficult to see how you would ever use the power of the purse in order to restrain presidential war power in the context of cyber. The War Powers Resolution was created in order to limit the power of the president, but you also had an additional check and balance, which was actually having 18 to 24-year-olds, primarily men -- at the time only men and still only men -- being deployed abroad. And you had that kind of blowback from, at the time, the draft. In a cyberwar, you don't have that check and balance either. So we need to ensure that we are able to craft a system that limits executive power consistent with the interests of those who pass the War Powers Resolution. MR. RISHIKOF: OK. Tom, you've worked in the executive branch and you've worked very closely with Oval Office issues. TOM BOSSERT: And the legislative branch. I -MR. RISHIKOF: Are you on board with this or what's your position? MR. BOSSERT: Well, if I'm not, we'll have a boring panel today. I want to thank the Atlantic Council and thank Jay. And I appreciate Barry Pavel as well and the work you're doing in this field. And let me give a short answer and then I'll elaborate. The short answer is that the War Powers Resolution does not govern this conduct in my view, to lead with controversy. However, I believe the Constitution is always in place, as we know, does. And Article One grants an enumerated power to the Congress to declare war and not that power to the executive. So we have an agreement on some points here, but I guess the theme of my day today will be that we suffer from a potential for great interpretative uncertainty and that's in our international understanding of what constitutes war and how we fight it, but in our domestic balances and checks on how we decide, who decides and so forth. So my controversy of today -- the War Powers Resolution by any stretch -- the closest stretch I can come to justifying I think the position here articulated by my other panelists is to suggest that if we know the cyber conduct in which we're about to engage is so obviously going to justify a reaction, a violent reaction, a justifiable international reaction that would put us in danger, you could stretch one of the provisions of the War Powers Resolution to suggest that we are putting ourselves in -- I think the word or term is "immediate danger." Immediacy becomes strained at that point because it requires not only our presupposition about how the enemy will respond and what they'll think about our intent and -- but then their ability and their effectiveness to really put us in danger. And so, frankly, the Congress has to change it or the DOD and the executive branch, under multiple administrations -- I served under the previous one -- will continue, I think with some unanimity in reading it the way they do, in the way we did, in the way the presidents I think since it was implemented under President Nixon's objection have. MR. RISHIKOF: Great. So what's great about the Atlantic Council is they don't just admire problems. They suggest solutions to problems. So, Andrew, to put you on the spot, one of the papers that was prepared today has the following recommendation after going off 25 pages, but that is the (old ?) way. And it says, quote: "Congress must close this," quote, "limited war close call loophole to the War Powers Resolution. Congress must make clear that offensive action itself, not the scale of that action, requires an authorization of war or an authorization for the use of force." So, as we say, aye or nay on that? ANDREW GROTTO: Well, let me first echo Tom's thanks to you, Jason, the Atlantic Council, and to you, Harvey, for moderating. And I also should say I think I'm the only member of the panel who, you know, actually works in the government and so I have to give the obligatory whatever I say here is my own view, doesn't reflect the views of any senators. It doesn't reflect the views of the intelligence committee. And it may or may not reflect my own views. So, you know, I obviously react here to your question, Harvey. I also want to kind of react to some things that have been said already. I think there's kind of two questions: would it be good policy for the executive branch to keep the Congress fully informed about the conduct of its operations in cyberspace? Easy answer: yes, right? I mean -- and that strikes me as a pretty simple proposition that I think -- you know, OK. Does current law require that? And the answer really kind of depends. And here you need to sort of parse the world of cyberoperations in two: operations occurring under Title 50, that is an intelligence activity, or under Title 10, a military activity. Activities conducted by the intelligence community, they are not armed forces for the purposes of the War Powers Resolution. However, intelligence community activities are subject to the requirements of the National Security Act, which requires that the Congress be kept fully and currently informed on all intelligence activities, requires a presidential finding and memorandum of notification for covert action activities for programs. And last but not least, you know -- and I think this might be unique to the intelligence community, that the National Security Act requires that all intelligence activities be specifically authorized by the Congress and so the power of the purse I think is amplified -- Congress' power of the purse is amplified in the National Security Act vis-a-vis intelligence activities. Now, Title 10 operations, you know, putting aside the constitutional debate about the War Powers Resolution, you know, I think there -- you know, there's obviously, you know, a long history of debate over what kinds of activities are covered by the War Power Resolution, what activities rise to the level of notification and congressional approval under that resolution. I think, you know, a panel like this has probably been held -- you know, you could probably go back to the Clinton years and -- you know, Bosnia, Kosovo, a lively debate then, same during the '80s, you know, with some of the Reagan administration. You can go to back to I think probably Carter. And so, to me, you know, on some level, cyber isn't necessarily the problem. It's I think our fundamental -- the fundamental tension between the executive branch and the legislative branch over the conduct of military activities**, regardless of what form they take**. So, Harvey, does that answer your question? MR. RISHIKOF: Yeah. I think you scratched the surface. MR. GROTTO: Right. MR. RISHIKOF: And I think what's interesting is in the cyber area, we often talk about cyber crime, cyberespionage, and cyberwar. And cybercrime uses Title 18. And you scratched the surface because the recommendation talks -- what is offensive cyber? And so, as you know, most of us refer to cyberincidents. We don't really classify it, because when you start classifying the concept, then you have to take action. So how do you guys see classification of what offense is versus what we think of cyberespionage, which is as old as the Old Testament and has always been done by state nations and it's not to be considered quote-unquote, "a hostile act," which, under international law, also is a term of we say art to define what it is. So how do you guys understand what offense is? If you were general counsel to the president and said, well, we have to inform Congress when we do something offensive, that's what these guys want, how would you define it in the cyber area? Why don't we do -- start going down the other end. Yeah. MR. BOSSERT: Sure. There's a number of assumptions, I guess, building to that question. I'll start with -- it helps me to conceive of cyber largely as a medium and not a domain. And I know there's not much distinction there, but it's useful because the conduct of the people -- this is kind of the gun rights debate, right? -- it's people who use cyber, not cyber. So this is a medium over which we conduct operations that are an age-old tradecraft. And so for me, I think of this as the one area for interpretive difference. So I'm glad we're into this area because I do believe we're going to agree on a number of our conversation points today. How do I view offensive? It is an absolute reality and necessity of today's cyberworld that we break into other nations' electronic systems for the purpose of gaining information and espionage, conducting espionage. And I believe that that has been largely viewed at least up until now as somebody that does not constitute an act of war. And could we with the control over those systems, over those electronic systems use them to then shut down a switch or cause some physical consequence? Yes. And so I think what becomes unique here, unlike in other areas or aspect of this review is we had to look at the consequences to decide whether we think it was an act of war. If you want to talk about offensive, I think we should probably not use that term. Simply it triggers the notion that we're committing an offense, an offense that the international community will not tolerate. I think there's a long history of tolerating espionage on both sides. MR. GROTTO: Just to add -- you know -- I mean, I agree. The phrase, you know, "offensive cyber operations," is imprecise, right? And, you know, I prefer to use -- you know, sort of the trifecta: computer network defense, computer network exploitation and computer network attack, CND, CNE and CNA as us cyber nerds refer to the three. You know, CNA, computer network attack, usually means something along the lines of any action that impairs the availability of information or an information system, affects the integrity, confidentiality of information or information system. Exploitation is merely gaining unauthorized access to an information system without necessarily, you know, manipulating the underlying data, the information without impairing the availability of the system. It's typically limited to, you know, pulling perhaps information back. And, obviously, computer network defense -- you know, sometimes, you know, can be kind of hard to draw a line. But, generally, it means defending your own network against unauthorized intrusions. MR. HEALEY: And we like those definitions. Those have been around since the late '90s. And they really helped when the DOD agreed on those, take a lot of different ideas that had been going around different services and bring them together so that we could all agree. And so the CNA, CNE, CND were very effective at getting us all talking about the same thing. But what they've also done is they've kept us focused on the purpose of the activity. If you're breaking something, it's CNA, if you're not breaking something, it's CNE. And that's a good way of classifying and thinking, but I've also found that since we instituted those, particularly in the Department of Defense, we then stopped any further thought about what differentiates this kind of conduct, and we have tended to focus on a single mission only. It's as -- so when I think about offense, there's probably four that really kind of fit -- that could fit in broadly. Some people fit in intelligence activity, you know, for espionage. I don't, but I think it certainly fits in Congress' role to -- and especially to see if we're drawing the line right, especially as we might be seeing more blowback on the private sector. The three main ways that I've seen nations in practice using offense are: one, the doctrine of battlefield use, of nations saying, you know, we're going to use this and we're going to integrate it with our kinetic military force. We don't have great examples of this. You know, arguably, Georgia, in 2008, Marine Corps General Mills said that he was using cybereffects on the battlefield in Afghanistan. But that might have been more referring to just getting into people's cell phones. And so -- but it stands out as -- if you talk to DOD people that's certainly what they mean by offense. We're going to -- we're going to drop cybers like we dropped bombs from an F-16. Second is the way the U.S. seems to be quite active with this in using it like drones -- sorry to use the D word -- but using it as a quiet, covert capability to disrupt either in line with an existing authorization of use of military force or in other ways, in the way that we would use commandoes. We've got to affect someone somewhere, very precisely, very quickly, very quietly, and cyber gives a great way to do that. Third is the way our adversaries tend to be using it is through proxies. Whether that's China or Russia, they tend not to have uniform people doing this as much. They tend to use state-owned enterprises or patriotic hackers or others. But what we found when we looked at the history -- I'll hold it up again if you want -- is that -- all of these tend to be looking at single uses, a single tactical engagement, if you will, to get -- to start using military terms -- rather than saying, all right. Well, what about all of these tactical engagements rollup? And so when I really think a lot about offense and the role of Congress and a lot of other areas, I find it's best to think of these cyberconflicts and cybercampaigns, because as we found -- the more strategically significant a cyberconflict, so that is not the little petty cybercrime stuff, not when someone tries to hack into the DOD, but the real campaigns, whether that's Estonia, 2007, Georgia 2008, Stuxnet -- the more strategically significant, the more similar it is to conflict in the other domains, meaning odds are you're going to know who the other adversary involved is. Odds are it's not going to happen at the speed of light. It's going to take place over weeks, months or years. So it's not network speed. The tactical engagement might be network speed, but that's true in every domain that a tactical engagement might be over quickly. If I was Air Force, the dogfight could be over before you know it. If you're a Marine, you could get ambushed before you even know the adversary is there and the fight's over. The same is true in cyber. You could get hacked. You could get owned. They could have their effect before you know that you're in their system. But the more strategically significant -- the conflict, history has shown -- I'm not saying it's always going to be that way -- odds are it's going to be this back and forth of adversary versus adversary, attack versus defense, back and forth. And that I think opens up a different conversation about the scope of Congress than what we're hearing from Fort Meade, that this is network speed. Congress can't have a role **because it happens like that.**

It’s the Litmus test for Presidential war powers authority

Lorber ’13

Eric, J.D. Candidate, University of Pennsylvania Law School, Ph.D Candidate, Duke University Department of Political Science, “Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?,” 15 U. Pa. J. Const. L. 961

Should these statutes be adjusted (or new ones created) that give Congress additional oversight in this area? Two competing desiderata suggest that oversight should be increased, but only to a limited extent. On the one hand, policymakers have suggested that developing strict rules and limitations on the use of offensive cyber operations will handicap the military's ability to **quickly and effectively** employ these tools in critical situations, such as cyber warfare against adversarial states. n236 According to these arguments, developing red lines that proscribe the use of these capabilities will create reluctance and trepidation among strategists and will lead to disadvantages in combat situations. n237 On the other hand, developing some legal rules is necessary to ensure that, as these cyber [\*1002] capabilities continue to develop, the President does not gain sufficient leverage to **substantially** tilt the balance between the President and Congress. Moreover, because these capabilities are still developing at a fast rate, understanding how they should and should not be employed is an important goal and having senior members of Congress and their staffs - professional staff members on the intelligence committees, who likely have substantial experience in these areas - provide input would be useful in developing this understanding.

It’s the key future warfighting technology—the aff neuters the executive

Chen ‘12

Julia, “RESTORING CONSTITUTIONAL BALANCE: ACCOMMODATING THE EVOLUTION OF WAR,” 53 B.C. L. Rev 1767 November, 2012

The use of technology, such as UAVs and cyber-warfare, which fall outside the War Powers Resolution, **is on the rise.** n313 Thus, although the Obama administration claimed that the conflict in Libya was a unique situation and a narrow carve-out from the Resolution, the **evolution of technology and changes in modern warfare demonstrate** that Libya is not unique. n314 There is also increasing wartime involvement of government civilians and contractors, which is outside the scope of the Resolution. n315 Thus, the small exception to the War Powers Resolution claimed by the executive branch is a rapidly growing gap that nullifies the Resolution's attempt to balance war powers. n316 The characteristics of UAVs and cyber-warfare that make them beneficial to the military also put them squarely within the Obama administration's [\*1799] exception to the War Powers Resolution. n317 UAVs and cyber-warfare allow the United States to fight long-distance wars, without deploying military personnel overseas, and with little risk of endangering American lives. n318 Nonetheless, both UAVs and cyber-attacks could have the same effects as a conventional military attack, and both could result in reprisal by adversaries against America. n319 Thus, just as a nation could pay a heavy price for introducing soldiers into combat, use of remotely operated technology could also be costly. n320 Nonetheless, these technologies enable the President to act against adversaries without having to negotiate the obstacle of congressional consultation. n321

## a2: LOAC Solves escalation

**Not in the case of terrorism – they don’t adhere to ILaw**

We turn LOAC

Abebe and Posner 11

DANIEL ABEBE & ERIC A. POSNER, Assistant Professor and Kirkland & Ellis Professor, University of Chicago Law School, Virginia Journal of International Law, 2011, "The Flaws of Foreign Affairs Legalism", Vol. 51, Issue 3, http://www.vjil.org/assets/pdfs/vol51/issue3/Abebe\_\_\_Posner.pdf

2. The American Executive’s Contribution to International Law Let us now compare the judiciary’s record with that of the executive. To keep the discussion short, we will focus on post-World War II activity. The executive has been the leading promoter of international law. It has negotiated and ratified (sometimes with the Senate’s consent, sometimes with Congress’s consent, and sometimes without legislative consent) thousands of treaties over the last sixty years,153 including the fundamental building blocks of the modern international legal system, such as the UN Charter, the GATT/**WTO**, the International Covenant for Civil and Political Rights, and the Genocide Convention. Through the U.S. State Department, the executive issues annual reports criticizing foreign countries for human rights violations, and the U.S. government has frequently, although not with complete consistency, issued objections when foreign countries violate human rights.154 **The executive has also negotiated and signed other important treaties to which the Senate has withheld consent** — including the Vienna Convention on the Law of Treaties, the International Covenant on Economic, Social and Cultural Rights, the Convention on the Law of the Sea, the Convention on the Rights of the Child, and the Convention on the Elimination of All Forms of Discrimination Against Women, among others.155 The executive has also been instrumental in creating modern international institutions, including the UN Security Council, the GATT/WTO system, the World Bank, and the IMF.156 Much of what we said might seem too obvious to mention. One can hardly imagine the judiciary deciding on its own that the United States must create or join some new treaty regime. But these obvious points have been overlooked in the debate about the role of the judiciary in foreign affairs. Virtually everything the judiciary does in this area depends on prior executive action. Only the constitutional interpretation cases seem truly judge-initiated, for in these cases, the Court sometimes cites treaties that the United States has not ratified and sometimes cites the laws of foreign nations. The claim that the judiciary can, and even does, play a primary role in the adoption of international law is puzzling. In almost all cases, the judiciary must follow the executive’s lead. This also means that if the judiciary interprets treaties and other sources of international law in an aggressive way — in a way that the executive rejects — the executive may respond **by being more cautious about negotiating treaties and adopting** i**nternational law in the first place.** This possible backlash effect has not been documented, but is plausible. As we discuss in the next section, fears of judicial enforcement of certain treaty obligations led to an effort by the Senate to ensure that those treaties would not have domestic legal effect.

## Solvency

No definitions

Kaminski 10

Ryan T. Kaminski, Columbia University School of International and Public Affairs, “ESCAPING THE CYBER STATE OF NATURE: CYBER DETERRENCE AND INTERNATIONAL INSTITUTIONS,” NATO Cooperative Cyber Defence Center of Excellence, published 2010, http://www.ccdcoe.org/publications/2010proceedings/Kaminski%20-%20Escaping%20the%20Cyber%20State%20of%20Nature%20Cyber%20deterrence%20and%20International%20Institutions.pdf

2.1 LACK OF A UNIVERSALLY ACCEPTED CYBERWARFARE LEXICON Anyone reading lay articles, think-tank studies, published manuscripts, or even government reports on cyber attacks is likely to ﬁnd a dizzying array of terms sometimes referring to the same concept. For example, should a DDoS attack that causes disruptions to a government website, yet does not steal any sensitive information, be considered an act of cyberwar, cyber espionage, or cyber vandalism? The implications of lacking a generally accepted vocabulary in this area are twofold. First, depending on what lexical framework is used, international and customary law can be interpreted to permit vastly different reactions to the same cyber attack. For example, if two states have contrasting lexicons concerning cyberwarfare, one could view a cyber attack as an act of war, while the other could conceptualize it merely as an act of cyber vandalism (“Marching Oﬀ,” 2008). Second, given that some states even lack a universally accepted cyber glossary among their various domestic civilian and military agencies, the possibility of misinterpreting a potential cyber attack on the national level also remains high (Shanker & Markoff, 2009). Looking at the Estonian and Georgian cases, this problem is uniquely apparent. Tohn (2009), for one, hyperbolizes the attacks against both states as “cyber-blitzkriegs,” regardless of such a term’s connotation with an all-out military attack from World War II (p. 17). Former US Deputy Assistant Secretary of Defense Peter Brookes (2008) even classiﬁes the attack on Estonia as a “pre-emptive digital strike” despite the lack of any signiﬁcant evidence that Estonia was planning a cyber attack on Russia. Jaak Aaviksoo, Estonia’s Defense Minister, also declared that the cyber attack against his country “cannot be treated as hooliganism, but has to be treated as an attack against the state” (“Marching Oﬀ,” 2008). Even though Estonia did not end up invoking Article V of the NATO charter which commits states to treat an attack on one member as an attack on themselves, the defense minister’s comments nonetheless illuminate major problems associated with the lack of a comprehensive cyberwarfare lexicon. While Estonia did construct a NATO-sponsored facility in its capital to study cyber security, this also may do little good if non-NATO members like China and Russia are relying upon an entirely different cyber language.

## LOAC Fails

States will just manipulate the legal framework

Jensen ’12 (Eric Talbot, J. Ruben Clark School of Law, Brigham Young University, “Applying a Sovereign Agency Theory of the Law of Armed Conflict,” Chicago Journal of International Law12.2 (Winter 2012): 685-727)

Instead, states have tended to avoid the applicability of these Protocols to their conflicts.78 State arguments supporting this resistance take various forms. Some states, such as Israel, claim to be involved in a conflict that does not fit into either category but is in a different category altogether.79 Or, as discussed in relation to the US in the introduction to this paper, states argue that for various reasons, the categories do not apply, or, at least, the law does not apply. As will be discussed below, Mexico is also hesitant to apply officially Common Article 3 or APII to its current fight against narcotics trafficking.80 These are but a few examples that highlight the **manipulability of the conflict classification methodology.**

By dramatically restricting the number of conflicts to which its provisions would apply (protections under APII can only be triggered by sufficiently broad violence), the bifurcation model **has effectively withheld international protections** for the victims of armed conflicts unless the host state is willing to admit that the internal struggle has reached the stage where their opposing armed groups control territory and can conduct sustained and concerted military operations. Such a government statement would have the natural effect of legitimizing those armed groups with whom the state is involved in the domestic conflict.81 **This** powerfully disincentivizes **states to take such action**, with the practical effect of denying critical protections to victims in these types of armed conflicts.

Furthermore, often no clear distinction exists between different types of armed conflict or between armed conflicts and lesser uses of force. For example, there is now almost always some form of third state involvement in internal armed conflicts, prompting the designation of a whole new category of armed conflict, that is, "internationalized armed conflict."82 In Colombia, "[t]he armed dissident movements have developed a confusing combination of alliances and simultaneous clashes with other actors in organized crime. The armed dissident groups have also developed ties with the drug trade, where they frequently levy taxes against drug producers and transporters in exchange for protection."83 Blurring lines between categories only adds further complication to the existing classification scheme that determines the applicable law in a given situation.

In the end, the bifurcated system has developed such that there is a danger that states will manipulate the law for political purposes, choosing how they intervene in the affairs of another state as a means of ensuring that particular provisions of law will apply to the conflict. As Stewart put it: States and non-state actors have proved equally willing to favour or fabricate accounts of foreign participation in internal conflicts for their own wider political gain. As a result, the characterization of armed conflicts involving international and internal elements, and the applicable law that flows from that characterization, are frequently "the subject of fierce controversy of a political nature."84

## ALt Causes

5) Alt cause – disputes over terrorist status on drone strikes

Margulies ’12 (Peter, Professor of Law, Roger Williams University, “The Fog of War Reform: Change and Structure in the Law of Armed Conflict After September 11,” Marquette Law Review Vol. 95 Iss. 4 Summer 2012)

In the last forty years, the rise of non-state actors has prompted new tensions. Drafters of Additional Protocol I to the Geneva Conventions believed that non-state actors “fighting against colonial domination and . . . racist régimes”67 had standing to participate in international armed conflict. That innovation challenged the traditional jus ad bellum norm of “right authority,” which extends to state actors the sole privilege of conducting hostilities while denying this privilege to non-state actors, whom LOAC has traditionally assumed could obtain a remedy from their states of nationality.68 While compelling examples supporting higher status for non-state actors span centuries, from the American colonists at Lexington and Concord to the African National Congress (ANC), the drafters of Additional Protocol I **did not provide any criteria** for deciding which group among rivals would be found the authentic representative. This **definitional vacuum** left inter-group violence as the default selection process, risking harm to members of the community that each group purports to represent. Protocol I yielded additional anomalies. While it codified the principle of distinction that forbids targeting civilians,69 it also made **concessions to irregular forces** that severely complicated implementation of that “basic principle.” Article 44(3) shields such forces until they have “engaged in a military deployment preceding the launching of an attack.”70 Some countries have construed this language as barring targeting of such forces until “‘moments immediately prior to an attack.’”71 Because a state’s uniformed forces can be targeted at any time,72 this reading creates a **marked asymmetry** in the targeting options of non-state and state actors. The drafters felt that this tactical advantage would at least encourage non-state actors to shun the most egregious forms of perfidy, where no arms were displayed until the attack was in progress.73 Although some non-state actors may have considered availing themselves of this opportunity, one cannot imagine Al Qaeda operatives following suit.74 However, a non-state fighting force without the duty to identify itself will **impel states to cut corners on the principle of distinction, shooting first and asking questions about participation in hostilities later**. As with even more blatant forms of perfidy, the result is greater risk to those hors de combat. Because LOAC, like other forms of international law, is increasingly fragmented,75 the increasing role of non-state actors has buttressed arguments for giving states more flexibility in the jus ad bellum. For example, states dealing with ideologically committed terrorist networks have sought to relax the customary requirement of imminent attack as a condition for self-defense. Scholars argued that obliging a state to wait until a terrorist plot approaches consummation was both unrealistic and risky for civilians whom the network plans to target.76

These debates have accelerated since September 11. Two opposing developments each reflected an effort to change LOAC. First, in the eighteen months after September 11, Bush administration officials sought to deprive suspected terrorists of protections against coercive interrogation and also sought to establish indefinite detention without judicial review and military commission trials that lacked fundamental guarantees of fairness.77 Even more recently, the ICRC proposed that civilians be shielded from targeting even if they have participated in hostilities.78 Over the objections of a majority of commentators convened for its study, the ICRC asserted that only civilians with a narrowly defined “continuous combat function” could be targeted at all times. Others could in effect choose the time and place of their vulnerability, even as they planned a return to the fray. Each change **threatened to destabilize LOAC**.