## 1

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.

Spills-over to collapse prez powers

Klukowski 11 (Kenneth, Research Fellow, Liberty University School of Law; Fellow and Senior Legal Analyst, American Civil Rights Union; National-Bestselling Author. George Mason University School of Law, J.D. 2008; University of Notre Dame, B.B.A. 1998, “MAKING EXECUTIVE PRIVILEGE WORK: A MULTI-FACTOR TEST IN AN AGE OF CZARS AND CONGRESSIONAL OVERSIGHT” 2011, 59 Clev. St. L. Rev. 31)

VI. CONCLUSION

Most controversies between Congress and the White House over information are decided more by politics than by law, and so a settlement is usually reached favoring the party with the public wind to its back. n348 **Questions of law should not be decided in that fashion**. Therefore, the reach and scope of executive privilege should be settled by the courts in such situations, so that the President's power is not impaired whenever the political wind is in the President's face and at his opponents' backs, or the President is inappropriately shielded when political tides flow in his favor.

While the best outcome in any interbranch dispute is the political branches reaching a settlement, "such compromise may not always be available, or even desirable." n349 It is not desirable where it sets a precedent **that** degrades **one of the three branches of government. If one branch of government demands something to which it is not constitutionally entitled and that the Constitution has fully vested in a coequal branch, the vested branch should not be required to negotiate on the question**. Negotiation usually involves compromise. This negotiation would often result in one branch needing to cede to the other**,** encouraging additional unconstitutional demands in the future. Though this may perhaps be a quicker route to a resolution, it disrupts the constitutional balance in government. As the Supreme Court has recently explained, "'convenience and efficiency are not the primary objectives--or the hallmarks--of democratic government.'" n350

President Reagan declared that "you aren't President; you are temporarily custodian of an institution, the Presidency. And you don't have any right to do away with any of the prerogatives of that institution, and one of those is executive privilege. And **this is what was being attacked** by the Congress." n351 Thus, any White House has the obligation to fight to protect executive privilege, and the courts should draw the line to preserve that constitutional prerogative. Likewise, there are times when it is the President who is refusing to give Congress its due under the Constitution, where Congress must assert its prerogatives for future generations. Conversely, where confidentiality is not warranted, courts must ensure public disclosure and accountability.

Extinction

Paul 98 (Joel, Professor, University of Connecticut School of Law, “The Geopolitical Constitution: Executive Expediency and Executive Agreements” July, 1998, 86 Calif. L. Rev. 671) \*\*Footnote 137-139 added

Whatever the complexity of causes that led to the Cold War - ideology, economics, power politics, Stalin's personality, Soviet intrigue, or American ineptitude - the tension of the bipolar order seemed real, immutable, and threatening to the U.S. public. n135 The broad consensus of U.S. leadership held that **the immediacy of the nuclear threat**, the need for covert operations and intelligence gathering, and the complexity of U.S. relations with both democracies and dictatorships **made it impractical to engage in congressional debate and oversight of foreign policy-making**. n136 The eighteenth-century Constitution did not permit a rapid response to twentieth-century foreign aggression. The reality of transcontinental ballistic missiles collapsed the real time for decision-making to a matter of minutes. **Faced with the apparent choice between the** risk of nuclear annihilation **or amending the constitutional process for policy-making, the preference for a powerful executive was clear**. n137 Early in the Cold War one skeptic of executive power, C.C. Rossiter, acknowledged that the steady increase in executive power is unquestionably a cause for worry, but so, too, is the steady increase in the magnitude and complexity of the problems the president has been called upon by the American people to solve in their behalf. They still have more to fear from the ravages of depression, rebellion, and especially atomic war than they do from whatever decisive actions may issue from the White House in an attempt to put any such future crises to rout....It is not too much to say that **the destiny of this nation in the Atomic Age will rest in the** [\*700] **capacity of the Presidency** as an institution of constitutional dictatorship. n138 n137. President Truman warned that we live in an age when hostilities begin without polite exchanges of diplomatic notes. There are no longer sharp distinctions between combatants and noncombatants, between military targets and the sanctuary of civilian areas. Nor can we separate the economic facts from the problems of defense and security. [The] President, who is Comander in Chief and who represents the interests of all the people, must be able to act at all times to meet any sudden threat to the nation's security. 2 Harry S. Truman, Memoirs: Years of Trial and Hope 478 (1956) (commenting on the Court's decision in the Steel Seizure Case). n138. Rossiter, supra note 54, at 308-09. n139. President Truman warned that **upon the functioning of a strong executive "depends the** survival of each of us **and also on that depends the survival of the free world**." The Powers of the Presidency 114 (Robert S. Hirschfield ed., 1968). See also, e.g., Speech by John F. Kennedy delivered to the National Press Club (Jan. 14, 1960), in Hirschfield, supra, at 129-31; Congress, the President, and the War Powers: Hearings Before the Subcomm. on Nat'l Sec. Policy and Scientific Developments of the House Comm. on Foreign Affairs, 91st Cong. 12-13 (1970) (statement of McGeorge Bundy, President, Ford Foundation); Congressional Oversight of Executive Agreements: Hearings on S. 3475 Before the Subcomm. on Separation of Powers of the Senate Comm. of the Judiciary, 92d Cong. 237-40 (1972) (statement of Nicholas Katzenbach, Former Attorney General and Former Undersecretary of State).

## 2

The 1AC is military futurology, an attempt to secure reality against disorder via force causing apathy–they need to justify their prediction model first.

Matt Carr 10, freelance writer, published in Race & Class, Slouching towards dystopia: the new military futurism, <http://www.societaitalianastoriamilitare.org/libri%20in%20regalo/2010%20CARR%20New-Military-Futurism.pdf>

This determination to shape, control and ‘dominate’ the turbulent and conflict prone twenty-first century in the foreseeable (and unforeseeable) future is a key component of the new military futurism. On the one hand, **military futurism is a by-product of the megalomaniac military doctrine of ‘full spectrum dominance’**. At the same time, its predictions about the future express very real fears amongst the US ruling elite that the United States is inextricably connected to a world that may be slipping out of its control. Perhaps not surprisingly, therefore, **the new military futurists** are often considerably more pessimistic than their predecessors and tend to **paint a very bleak future of an unsafe and unstable world that demands a constant military presence to hold it together**. From Yevgeny Zemyatin’s We to Brave New World and Orwell’s Nineteen Eighty-Four, twentieth-century writers have used dystopian visions of the future as a warning or as a satirical commentary on the often lethal consequences of twentieth-century utopianism. The dystopias of the new military futurists have a very different purpose. The US military often tends to perceive itself as the last bastion of civilisation against encroaching chaos and disorder. **The worse the future is perceived to be, the more these dark visions of chaos and disorder serve to justify limitless military ‘interventions’, technowarfare, techno-surveillance and weapons procurement programmes**, and the predictions of the military futurists are often very grim indeed.

## 3

The aff must specify statutory or judicial restrictions—

“And/or” means one or the other or both

CED ‘9

(http://dictionary.reference.com/browse/and%2For)

and/or

— conj

( coordinating ) used to join terms when **either one or the other or both** is indicated: passports and/or other means of identification

Vote neg—plan text clarity key to specific negative ground and tests the core question of the resolution—where the authority is located—

Presumption

CMS ‘3

(http://www.chicagomanualofstyle.org/CMS\_FAQ/CapitalizationTitles/CapitalizationTitles32.html, accessed 10/16/07, re-accessed at <http://www.chicagomanualofstyle.org/qanda/data/faq/topics/CapitalizationTitles/faq0015.html>, 8/19/2013)

Q. When I refer to the government of the United States in text, should it be US Federal Government or US federal government? A. **The government of the** United States **is not a single official entity**. Nor is it when it is referred to as the federal government or the U.S. government or the U.S. federal government. It’s just a government, which, like those in all countries, has some official bodies that act and operate in the name of government: the Congress, the Senate, the Department of State, etc.

## 4

NSA reform is in a narrow Congressional sweet spot

David Hawkings, Roll Call, 3/25/14, Hill’s Bipartisan Deadlock on Phone Records May Be Easing, blogs.rollcall.com/hawkings/obama-nsa-reform-plan-could-ease-congressional-deadlock-on-spying/2/

Eight months ago, in one of its most important and fascinatingly nonpartisan votes of recent memory, the House came up just seven members short of eviscerating the government’s vast effort to keep tabs on American phone habits. The roll call revealed a profound divide in Congress on how assertively the intelligence community should be allowed to probe into the personal lives of private citizens in the cause of thwarting terrorism. It is a split that has stymied legislative efforts to revamp the National Security Agency’s bulk data collection programs. Until now, maybe. Senior members with jurisdiction over the surveillance efforts, in both parties and on both sides of the Hill, are signaling generalized and tentative but nonetheless clear support for the central elements of a proposed compromise that President Barack Obama previewed Tuesday and will formally unveil by week’s end. The president, in other words, may be close to finding the congressional sweet spot on one of the most vexing problems he’s faced — an issue that surged onto Washington’s agenda after the secret phone records collection efforts were disclosed by former NSA contractor Edward Snowden. If Obama can seal the deal, which he’s pledged to push for by the end of June, it would almost surely rank among his most important second-term victories at the Capitol. It also would create an exception that proves the rule about the improbability of bipartisan agreement on hot-button issues in an election season.

“I recognize that people were concerned about what might happen in the future with that bulk data,” Obama said at a news conference in The Hague, where he’s been working to gain support for containing Russia from a group of European leaders who have their own complaints about U.S. spying on telephone calls. “This proposal that’s been presented to me would eliminate that concern.” The top two members of the House Intelligence Committee, GOP Chairman Mike Rogers of Michigan and ranking Democrat C.A. Dutch Ruppersberger of Maryland, introduced their own bill to revamp surveillance policy Tuesday — and declared they expect it would track very closely with the language coming from the administration. They said they had been negotiating with White House officials for several weeks and viewed the two proposals as compatible. At their core, both the Obama and House bills would end the NSA practice of sucking up and storing for five years the date and time, duration and destination of many millions of phone calls placed or received by Americans. Instead, the phone companies would be required to retain this so-called metadata (and comparable information about email and Internet use) for 18 months, their current practice. And the government would have to obtain something like a search warrant from the Foreign Intelligence Surveillance Court, meaning in each discreet case a judge would limit how deeply the telecom companies would have to query their databases in hopes of finding calling patterns that suggest national security threats. Since both Rogers and Ruppersberger have been prominent defenders of the bulk collection system, any agreement they reach that has Obama’s blessing can be expected to pass the House. It should garner support from a lopsided majority of the 217 House members (three-fifths of the Republicans and two-fifths of the Democrats) who voted to stick with the status quo last July. And it stands a chance to win over at least some on the other side — an unusual coalition of 94 mostly libertarian-leaning tea party Republicans and 111 liberal Democrats, who say NSA searches of the databases should be limited to information about existing targets of investigations. But one leader of that camp vowed to work for the defeat of any measure that looks like either the Obama or Intelligence panel plans. Republican Rep. Jim Sensenbrenner of Wisconsin, who as chairman of House Judiciary a decade ago was instrumental in writing the Patriot Act, believes that law has been grossly misapplied by the NSA to invade personal privacy much too easily. Sensenbrenner said he would continue to push his measure to almost entirely prevent the NSA from looking at telecommunications metadata. But the sponsor of the companion Senate bill, Judiciary Chairman Patrick J. Leahy, D-Vt., said he would remain open to finding the makings of a deal in the Obama plan. Leahy signaled the legislative negotiating would be much smoother if Obama suspended the bulk data collection during the talks. Much more enthusiastic was Calfornia’s Dianne Feinstein, the Democratic chairwoman of the Senate Intelligence Committee, who said she generally supports the House proposal and views Obama’s plan “a worthy effort.” Her committee’s top Republican, the retiring Saxby Chambliss of Georgia, was a bit more equivocal but gave a strong indication he was eager to cut a deal based on the ideas from the House and the White House.

The plan’s fight over authority crowds it out

John Grant, Minority Counsel for the Senate Committee on Homeland Security and Governmental Affairs, 8/13/2010, Will There Be Cybersecurity Legislation?, jnslp.com/2010/08/13/will-there-be-cybersecurity-legislation/

In the course of just a few decades, information technology has become an essential component of American life, playing a critical role in nearly every sector of the economy. Consequently, government policy affecting information technology currently emanates from multiple agencies under multiple authorities – often with little or no coordination. The White House’s Cyberspace Policy Review (the Review) wisely recognized that the first priority in improving cybersecurity is to establish a single point of leadership within the federal government and called for the support of Congress in pursuit of this agenda. Congressional involvement in some form is inevitable, but there is considerable uncertainty as to what Congress needs to do and whether it is capable of taking action once it decides to do so. With an agenda already strained to near the breaking point by legislation to address health care reform, climate change, energy, and financial regulatory reform – as well as the annual appropriations bills – the capacity of Congress to act will depend, in some part, on the necessity of action. For the last eight years, homeland security has dominated the congressional agenda. With the memory of the terrorist attacks of September 11 becoming ever more distant, there may be little appetite for taking on yet another major piece of complex and costly homeland security legislation.

That’s key to NSA authority—Congress would easily reject all NSA surveillance

Brendan Sasso, National Journal, 3/25/14, Why Obama and His NSA Defenders Changed Their Minds, www.nationaljournal.com/tech/why-obama-and-his-nsa-defenders-changed-their-minds-20140325

It was only months ago that President Obama, with bipartisan backing from the heads of Congress's Intelligence committees, was insisting that the National Security Agency's mass surveillance program was key to keeping Americans safe from the next major terrorist attack. They were also dismissing privacy concerns, saying the program was perfectly legal and insisting the necessary safeguards were already in place. But now, Obama's full-speed ahead has turned into a hasty retreat: The president and the NSA's top supporters in Congress are all pushing proposals to end the NSA's bulk collection of phone records. And civil-liberties groups—awash in their newly won clout—are declaring victory. The question is no longer whether to change the program, but how dramatically to overhaul it. So what changed? It's not that Obama and his Hill allies suddenly saw the error of their ways and became born-again privacy advocates. Instead, with a critical section of the Patriot Act set to expire next year, they realized they had no choice but to negotiate. If Congress fails to reauthorize that provision—Section 215—by June 1, 2015, then the NSA's collection of U.S. records would have to end entirely. And the growing outrage prompted by the Snowden leaks means that the NSA's supporters would almost certainly lose an up-or-down vote on the program. Rep. Adam Schiff, a Democratic member of the House Intelligence Committee, said that looming sunset is what forced lawmakers to the bargaining table. "I think what has changed is the growing realization that the votes are simply not there for reauthorization," he said in an interview. "I think that more than anything else, that is galvanizing us into action."

Obama and the House Intelligence Committee leaders believe their proposals are now the NSA's best bet to retain some power to mine U.S. phone records for possible terror plots. Senate Intelligence Committee Chairwoman Dianne Feinstein, another leading NSA defender, also indicated she is on board with the changes, saying the president's proposal is a "worthy effort." And though the Hill's NSA allies are now proposing reforms to the agency, they don't seem particularly excited about it. At a Capitol Hill press conference Tuesday, Rep. Mike Rogers, the Republican chairman of the House Intelligence Committee, and Rep. Dutch Ruppersberger, the panel's top Democrat, often sounded like they were arguing against their own bill that they were unveiling. "I passionately believe this program has saved American lives," Rogers said. Ruppersberger said if the program had been in place in 2001, it may have prevented the Sept. 11 attacks. But the lawmakers acknowledged there is broad "discomfort" with the program as it is currently structured. "We need to do something about bulk collection because of the perception of our constituents," Ruppersberger admitted. Under their legislation, the vast database of phone records would stay in the hands of the phone companies. The NSA could force the phone companies to turn over particular records, and the Foreign Intelligence Surveillance Court would review the NSA orders after the fact. But Rogers rejected a reporter's suggestion that the NSA should have never had control of the massive database of phone records in the first place. "There was no abuse, no illegality, no unconstitutionality," he said. For all their hesitance, however, Rogers and company much prefer their version to a competing proposal to change the way the government gathers information. That would be the USA Freedom Act, a proposal from Senate Judiciary Committee Chairman Patrick Leahy and Rep. Jim Sensenbrenner that Rogers and his ilk fear would go too far in hamstringing the NSA. The USA Freedom Act would require the NSA to meet a tougher standard for the data searches and would limit other NSA programs, such as Internet surveillance of people overseas. Additionally, President Obama is expected to unveil his own plan to reform the controversial phone data collection program this week. According to The New York Times, Obama's proposal would also keep the database in the hands of the phone companies. His plan would have tougher judicial oversight than the House bill by requiring pre-approval from the court for every targeted phone number, the newspaper reported. But though the momentum has shifted and officials seem to be coalescing around a framework for overhauling the NSA program, the question is far from settled. Leahy and Sensenbrenner are not backing off from their USA Freedom Act, and outside groups will continue their policy push as well.

NSA reform key to the alliance

Dempsey 2/3/14

Judy Dempsey, senior associate, editor in chief of Strategic Europe, Carnegie Endowment for Peace, February 3, 2014, "Kerry’s Lost Opportunity for Transatlantic Relations", http://carnegieeurope.eu/strategiceurope/?fa=54408

When U.S. Secretary of State John Kerry flew into Berlin on January 31, expectations were high that the United States was finally taking seriously its allies’ anger about the National Security Agency’s pervasive spying.

U.S. snooping is an issue that is refusing to disappear from German newspaper headlines. Crucially, it is increasingly straining transatlantic relations—a situation that neither the Americans nor the Europeans can afford to ignore.

At a meeting with German Chancellor Angela Merkel, Kerry spoke casually of “bumps in the road.” Yet he gave absolutely no reassurance about the United States’ future policy on spying, neither during his Berlin meetings nor afterward at this year’s Munich Security Conference.

In fact, when he spoke to his audience of high-ranking politicians, diplomats, and foreign and security policy specialists in the Bavarian capital, he didn’t even mention the NSA. Nor did U.S. Defense Secretary Chuck Hagel bother to raise the issue publicly.

That was a mistake.

It is not only the German public that needs reassurances and explanations about the scope of the NSA’s reach. It is about restoring trust between the United States and all its European allies. Given the huge issues that governments on both sides of the Atlantic have to tackle, such trust is necessary more than ever.

If the administration of U.S. President Barack Obama wants to start rebuilding trust in the transatlantic relationship, it needs to embark on much more active public diplomacy. “And that means sending very senior people to European countries to do just that,” said Toomas Hendrik Ilves, the president of Estonia, who also took part in the Munich summit.

In that sense, Kerry and Hagel squandered the opportunity to use the high-level conference as a platform to reach out to German and European audiences. The pair did nothing to address the trend identified in a recent poll by German public television that only 57 percent of Germans believe that relations with the United States are good, down from 92 percent in 2012.

Instead, Kerry spent much of his speech recalling his childhood in Europe and stressing America’s commitment to NATO and to Europe. He and Hagel cited all the places and all the conflicts in which the United States was engaged, to prove that America was not turning in on itself. In short, conference participants were told that everything was just fine with the transatlantic relationship.

Yet the State of the Union address that Obama gave in Washington on January 28 presented a very different picture, causing genuine concern not only to European governments but also to U.S. foreign policy experts. In that speech, there was scant mention of Ukraine. There was little serious attention paid to Syria, and nothing about Russia or China. NATO and Europe received only passing references.

But at least Obama did mention that U.S. surveillance methods were being reviewed. That is exactly what Kerry and Hagel should have said in Munich. They should have acknowledged how much the NSA scandal has hurt transatlantic relations, and they should have explained what Washington plans to do about that.

An equally important dimension to the spying scandal is Russia. Vladimir Putin, the Russian president, must be having a field day. The more Edward Snowden, a former NSA official who has been given asylum in Russia, leaks classified information, the more those revelations weaken transatlantic ties. Putin must be delighted about the wedge being driven between the United States and its European allies, in particular Germany.

Neither Obama nor Merkel can afford to ignore this state of affairs. They both need each other more than ever, on issues ranging from the unrest in Ukraine to the negotiations on a new Transatlantic Trade and Investment Partnership. It would be so damaging for the United States and the EU if certain political parties and influential nongovernmental organizations in Europe were to exploit the NSA scandal to jeopardize those talks.

The United States must understand that its allies’ anger over being spied on won’t simply blow over. Ignoring that sentiment carries real costs in terms of influence and policies. Some plain talking from John Kerry and others is sorely needed.

Stops Eurasian nuclear war

Brzezinski, 3

(PhD-Poli Sci & Former National Security Advisor to President Carter, “Hegemonic quicksand,” Winter, http://nationalinterest.org/article/hegemonic-quicksand-563)

FOR THE next several decades, the most volatile and dangerous region of the world--with the **explosive potential to plunge the world into chaos**--will be the crucial swathe of Eurasia between Europe and the Far East. Heavily inhabited by Muslims, we might term this crucial subregion of Eurasia the new "Global Balkans." (1) It is here that America could slide into a collision with the world of Islam while American-European policy differences could even cause the Atlantic Alliance to come unhinged. The two eventualities together could then put the prevailing American global hegemony at risk. At the outset, it is essential to recognize that the ferment within the Muslim world must be viewed primarily in a regional rather than a global perspective, and through a geopolitical rather than a theological prism. The world of Islam is disunited, both politically and religiously. It is politically unstable and militarily weak, and likely to remain so for some time. Hostility toward the United States, while pervasive in some Muslim countries, originates more from specific political grievances--such as Iranian nationalist resentment over the U.S. backing of the Shah, Arab animus stimulated by U.S. support for Israel or Pakistani feelings that the United States has been partial to India-than from a generalized religious bias. The complexity of the challenge America now confronts dwarfs what it faced half a century ago in Western Europe. At that time, Europe's dividing line on the Elbe River was the strategically critical frontline of maximum danger, with the daily possibility that a clash in Berlin could unleash a nuclear war with the Soviet Union. Nevertheless, the United States recognized the stakes involved and committed itself to the defense, pacification, reconstruction and revitalization of a viable European community. In doing so, America gained natural allies with shared values. Following the end of the Cold War, the United States led the transformation of NATO from a defense alliance into an enlarging security alliance--gaining an enthusiastic new ally, Poland--and it has supported the expansion of the European Union (EU). For at least a generation, the major task facing the United States in the effort to promote global security will be the pacification and then the cooperative organization of a region that contains the world's greatest concentration of political injustice, social deprivation, demographic congestion and potential for high-intensity violence. But the region also contains most of the world's oil and natural gas. In 2002, the area designated as the Global Balkans contained 68 percent of the world's proven oil reserves and 41 percent of the world's proven natural gas reserves; it accounted for 32 percent of world oil production and 15 percent of world natural gas production. In 2020, the area is projected to produce roughly 42 million barrels of oil per day--39 percent of the global production total (107.8 million barrels per day). Three key regions-Europe, the United States and the Far East--collectively are projected to consume 60 percent of that global production (16 percent, 25 percent and 19 percent, respectively). The combination of oil and volatility gives the United States no choice. America faces an awesome challenge in helping to sustain some degree of stability among precarious states inhabited by increasingly politically restless, socially aroused and religiously inflamed peoples. It must undertake an even more daunting enterprise than it did in Europe more than half a century ago, given a terrain that is culturally alien, politically turbulent and ethnically complex. In the past, this remote region could have been left to its own devices. Until the middle of the last century, most of it was dominated by imperial and colonial powers. Today, to ignore its problems and underestimate its potential for global disruption would be tantamount to declaring an open season for **intensifying regional violence**, region-wide contamination by terrorist groups and the **competitive proliferation of w**eaponry of **m**ass **d**estruction. The United States thus faces a task of monumental scope and complexity. There are no self-evident answers to such basic questions as how and with whom America should be engaged in helping to stabilize the area, pacify it and eventually cooperatively organize it. Past remedies tested in Europe--like the Marshall Plan or NATO, both of which exploited an underlying transatlantic political-cultural solidarity--do not quite fit a region still rent by historical hatreds and cultural diversity. Nationalism in the region is still at an earlier and more emotional stage than it was in war-weary Europe (exhausted by two massive European civil wars fought within just three decades), and it is fueled by religious passions reminiscent of Europe's Catholic-Protestant forty-year war of almost four centuries ago. Furthermore, the area contains no natural allies bonded to America by history and culture, such as existed in Europe with Great Britain, France, Germany and, lately, even Poland. In essence, America has to navigate in uncertain and badly charted waters, setting its own course, making differentiated accommodations while not letting any one regional power dictate its direction and priorities. To Whom Can America Turn? TO BE SURE, several states in the area are often mentioned as America's potential key partners in reshaping the Global Balkans: Turkey, Israel, India and--on the region's periphery--Russia. Unfortunately, every one of them suffers serious handicaps in its capability to contribute to regional stability or has goals of its own that collide with America's wider interests in the region. Turkey has been America's ally for half a century. It earned America's trust and gratitude by its direct participation in the Korean War. It has proven to be NATO's solid and reliable southern anchor. With the fall of the Soviet Union, it became active in helping both Georgia and Azerbaijan consolidate their new independence, and it energetically promoted itself as a relevant model of political development and social modernization for those Central Asian states whose people largely fall within the radius of the Turkic cultural and linguistic traditions. In that respect, Turkey's significant strategic role has been complementary to America's policy of reinforcing the new independence of the region's post-Soviet states. Turkey's regional role, however, is limited by two major offsetting considerations stemming from its internal problems. The first pertains to the still uncertain status of Ataturk's legacy: Will Turkey succeed in transforming itself into a secular European state even though its population is overwhelmingly Muslim? That has been its goal since Ataturk set his reforms in motion in the early 1920s. Turkey has made remarkable progress since then, but to this day its future membership in the European Union (which it actively seeks) remains in doubt. If the EU were to close its doors to Turkey, the potential for an Islamic political-religious revival and consequently for Turkey's dramatic (and probably turbulent) international reorientation should not be underestimated. The Europeans have reluctantly favored Turkey's inclusion in the European Union, largely in order to avoid a serious regression in the country's political development. European leaders recognize that the transformation of Turkey from a state guided by Ataturk's vision of a European-type society into an increasingly theocratic Islamic one would adversely affect Europe's security. That consideration, however, is contested by the view, shared by many Europeans, that the construction of Europe should be based on its common Christian heritage. It is likely, therefore, that the European Union will delay for as long as it can a clear-cut commitment to open its doors to Turkey--but that prospect in turn will breed Turkish resentments, increasing the risks that Turkey might evolve into a resentful Islamic state, with potentially dire consequences for southeastern Europe. (2) The other major liability limiting Turkey's role is the Kurdistan issue. A significant proportion of Turkey's population of 70 million is composed of Kurds. The actual number is contested, as is the nature of the Turkish Kurds' national identity. The official Turkish view is that the Kurds in Turkey number no more than 10 million, and that they are essentially Turks. Kurdish nationalists claim a population of 20 million, which they say aspires to live in an independent Kurdistan that would unite all the Kurds (claimed to number 25-35 million) currently living under Turkish, Syrian, Iraqi and Iranian domination. Whatever the actual facts, the Kurdish ethnic problem and the potential Islamic religious issue tend to make Turkey-- notwithstanding its constructive role as a regional model--also very much a part of the region's basic dilemmas. Israel is another seemingly obvious candidate for the status of a pre-eminent regional ally. As a democracy as well as a cultural kin, it enjoys America's automatic affinity, not to mention intense political and financial support from the Jewish community in America. Initially a haven for the victims of the Holocaust, it enjoys American sympathy. As the object of Arab hostility, it triggered American preference for the underdog. It has been America's favorite client state since approximately the mid-1960s and has been the recipient of unprecedented American financial assistance ($80 billion since 1974). It has benefited from almost solitary American protection against UN disapprobation or sanctions. As the dominant military power in the Middle East, Israel has the potential, in the event of a major regional crisis, not only to be America's military base but also to make a significant contribution to any required U.S. military engagement. Yet American and Israeli interests in the region are not entirely congruent. America has major strategic and economic interests in the Middle East that are dictated by the region's vast energy supplies. Not only does America benefit economically from the relatively low costs of Middle Eastern oil, but America's security role in the region gives it indirect but politically critical leverage on the European and Asian economies that are also dependent on energy exports from the region. Hence good relations with Saudi Arabia and the United Arab Emirates--and their continued security reliance on America--is in the U.S. national interest. From Israel's standpoint, however, the resulting American-Arab ties are disadvantageous: they not only limit the degree to which the United States is prepared to back Israel's territorial aspirations, they also stimulate American sensitivity to Arab grievances against Israel. Among those grievances, the Palestinian issue is foremost. That the final status of the Palestinian people remains unresolved more than 35 years after Israel occupied the Gaza Strip and the West Bank--irrespective of whose fault that actually may be--intensifies and, in Arab eyes, legitimates the widespread Muslim hostility toward Israel. (3) It also perpetuates in the Arab mind the notion that Israel is an alien and temporary colonial imposition on the region. To the extent that the Arabs perceive America as sponsoring Israeli repression of the Palestinians, America's ability to pacify anti-American passions in the region is constrained. That impedes any joint and constructive American-Israeli initiative to promote multilateral political or economic cooperation in the region, and it limits any significant U.S. regional reliance on Israel's military potential. Since September 11, the notion of India as America's strategic regional partner has come to the forefront. India's credentials seem at least as credible as Turkey's or Israel's. Its sheer size and power make it regionally influential, while its democratic credentials make it ideologically attractive. It has managed to preserve its democracy since its inception as an independent state more than half a century ago. It has done so despite widespread poverty and social inequality, and despite considerable ethnic and religious diversity in a predominantly Hindu but formally secular state. India's prolonged conflict with its Islamic neighbor, Pakistan, involving violent confrontations with guerrillas and terrorist actions in Kashmir by Muslim extremists benefiting from Pakistan's benevolence, made India particularly eager to declare itself after September 11 as co-engaged with the United States in the war on terrorism. Nonetheless, any U.S.-Indian alliance in the region is likely to be limited in scope. Two major obstacles stand in the way. The first pertains to India's religious, ethnic and linguistic mosaic. Although India has striven to make its 1 billion culturally diverse people into a unified nation, it remains basically a Hindu state semi-encircled by Muslim neighbors while containing within its borders a large and potentially alienated Muslim minority of somewhere between 120-140 million. Here, religion and nationalism could inflame each other on a grand scale. So far, India has been remarkably successful in maintaining a common state structure and a democratic system--but much of its population has been essentially politically passive and (especially in the rural areas) illiterate. The risk is that a progressive rise in political consciousness and activism could be expressed through intensified ethnic and religious collisions. The recent rise in the political consciousness of both India's Hindu majority and its Muslim minority could jeopardize India's communal coexistence. Internal strains and frictions could become particularly difficult to contain if the war on terrorism were defined as primarily a struggle against Islam, which is how the more radical of the Hindu politicians tend to present it. Secondly, India's external concerns are focused on its neighbors, Pakistan and China. The former is seen not only as the main source of the continued conflict in Kashmir but ultimately--with Pakistan's national identity rooted in religious affirmation--as the very negation of India's self-definition. Pakistan's close ties to China intensify this sense of threat, given that India and China are unavoidable rivals for geopolitical primacy in Asia. Indian sensitivities are still rankled by the military defeat inflicted upon it by China in 1962, in the short but intense border clash that left China in possession of the disputed Aksai Chin territory. The United States cannot back India against either Pakistan or China without paying a prohibitive strategic price elsewhere: in Afghanistan if it were to opt against Pakistan, and in the Far East if it allied itself against China. These internal as well as external factors constrain the degree to which the United States can rely on India as an ally in any longer-term effort to foster--let alone impose--greater stability in the Global Balkans. Finally, there is the question of the degree to which Russia can become America's major strategic partner in coping with Eurasian regional turmoil. Russia clearly has the means and experience to be of help in such an effort. Although Russia, unlike the other contenders, is no longer truly part of the region--Russian colonial domination of Central Asia being a thing of the past--Moscow nevertheless exercises considerable influence on all of the countries to its immediate south, has close ties to India and Iran and contains some 15-20 million Muslims within its own territory. At the same time, Russia has come to see its Muslim neighbors as the source of a potentially explosive political and demographic threat, and the Russian political elite are increasingly susceptible to anti-Islamic religious and racist appeals. In these circumstances, the Kremlin eagerly seized upon the events of September 11 as an opportunity to engage America against Islam in the name of the "war on terrorism." Yet, as a potential partner, Russia is also handicapped by its past, even its very recent past. Afghanistan was devastated by a decade-long war waged by Russia, Chechnya is on the brink of genocidal extinction, and the newly independent Central Asian states increasingly define their modern history as a struggle for emancipation from Russian colonialism. With such historical resentments still vibrant in the region, and with increasingly frequent signals that Russia's current priority is to link itself with the West, Russia is being perceived in the region more and more as a former European colonial power and less and less as a Eurasian kin. Russia's present inability to offer much in the way of a social example also limits its role in any American-led international partnership for the purpose of stabilizing, developing and eventually democratizing the region. Ultimately, America can look to only one genuine partner in coping with the Global Balkans: **Europe**. Although it will need the help of leading East Asian states like Japan and China--and Japan will provide some, though limited, material assistance and some peacekeeping forces--neither is likely at this stage to become heavily engaged. **Only Europe**, increasingly organized as the European Union and militarily integrated through NATO, has the potential capability in the political, military and economic realms to pursue jointly with America the task of engaging the various Eurasian peoples--on a differentiated and flexible basis--in the promotion of regional stability and of progressively widening trans-Eurasian cooperation. And a supranational European Union linked to America would be less suspect in the region as a returning colonialist bent on consolidating or regaining its special economic interests.

## 5

The executive branch of the United States should issue and enforce an executive order to cease the conduct of offensive cyber-attacks.

The Department of Defense should establish a new cyberwar doctrine codifying this policy, and the President should give a public address announcing this policy.  
The United States federal government should affirm the posse comitatus principle by clarifying that the military cannot operate drug interdiction and border duty missions.

The status quo is always an option – proving the CP worse does not justify the plan. Logical decision-making is the most portable skill.

And, presumption remains negative—the counterplan is less change and a tie goes to the runner.

It’s binding law that solves the aff.

Graham Dodds, Ph.D., Concordia professor of political science, 2013, Take Up Your Pen: Unilateral Presidential Directives in American Politics, p. 10

If executive orders, proclamations, memoranda, and other unilateral presidential directives merely expressed the president's view, then they would be important but not necessarily determinative. **However, these directives are not mere statements of presidential preferences; rather, they establish** binding policies and have the force of law**, ultimately** backed by the full coercive power of the state. In Armstrong v. United States, 80 U.S. (13 Wall.) 154 (1871), the Supreme Court considered the legal status of a proclamation and decided that such directives are public acts to which courts must “give effect.” In other words, in the eyes of the judiciary, unilateral presidential directives are just as binding as laws. In 1960, Senator Robert Byrd (D-WV) advised his colleagues, “Keep in mind that an executive order is not statutory law.” 46 Politically, that may be true, as unilateral presidential directives represent the will only of the chief executive and lack the direct endorsement of congressional majorities. But constitutionally and legally**, a unilateral presidential directive is** as authoritative and compulsory as a regular law, at least until such time as it is done away with by Congress, courts, or by a future unilateral presidential directive.

Executive speeches crystallize the CP’s legal position—locks-in durability and credible signal

Rebecca Ingber, Associate Research Scholar, Columbia Law School; 2011-2012 Council on Foreign Relations International Affairs Fellow and Hertog National Security Law Fellow, Columbia Law School, Summer 2013, Article: Interpretation Catalysts and Executive Branch Legal Decisionmaking, 38 Yale J. Int'l L. 359

The prior two sections discussed interpretation catalysts that are primarily driven by external factors. But internally-triggered events can also operate as compelling interpretation catalysts. Decisions to take a particular action or implement a policy can fall under this category, as can determinations to make a speech to express publicly the Administration's views on a given matter. Speechmaking is a particularly interesting interpretation catalyst as it can be provoked by a combination of internal and external factors. And as a somewhat more pliable tool than those that are more formally responsible to external [\*398] bodies like courts or treaty-reporting bodies, it can be employed strategically by officials within the government seeking to shape the decisionmaking process. n186 The decision to give a speech on a matter of international law and national security is rarely a decision made casually or unilaterally by the particular speechmaker herself, and the impetus to do so can be driven by a range of internal and external factors. There may exist external pressure, such as calls upon the executive - by media, Congress, or others - to explain its position in a given area. For example, there have been widespread calls in recent years for greater clarity from the Obama Administration regarding its legal position on targeting killing, which have resulted in a number of speeches by government officials explaining the policy and legal framework in ever greater detail. n187 Pressure to make public a set of legal views may also come from within the Administration, from actors who wish to explain the government's position in an effort to mollify criticism about either the substantive decisions or the lack of transparency about the decisionmaking process. n188 Speechmaking may simply reveal to the public the pre-existing legal rationale for executive policies or programs; it can also be an action-forcing mechanism driving the executive to crystallize and finally bind itself to a position on a matter. n189 As with other interpretation catalysts, speechmaking can shape the parameters of a particular decisional moment - its timing and the context in which the decision is made - and it can create greater leverage for the speechmaker and related officials at the decisionmaking table. There are numerous other means officials employ to create leverage, including strategic leaking and resignation threats, both of which are unilateral means to influence decisionmaking. Speechmaking is distinct in that it actually creates a different decisionmaking forum - the process of drafting and coordinating a position and language for the speech itself in a very specific context - and thus influences [\*399] substance by transforming the process, shaping the contextual pressures, and ensuring specific coordination. 1. Who Has the Pen? Unlike litigation and treaty-reporting, which are ongoing processes that may cross administrations and can be channeled to some degree by the career bureaucracy, speechmaking is inherently top-down, involving high-level, politically-appointed officials. Career officials may be involved but just as often it may be the political assistants surrounding the speechmaker who assist substantively in the process. Which official volunteers or is asked to take on a speech is critical because speechmaking - whether intended for this purpose or not - gives that official, and those working for her, the pen on the public representation of an issue, and it can thus be an opportunity for an official to gain inclusion in a matter to which she might otherwise not have access. n190 Speechmaking may grant to an official otherwise out of the loop not only a seat at the decisionmaking table, but also a place of significant influence. n191 Once a key administration official is slated to give a speech, her views cannot be disregarded. She cannot be left out of the speechwriting room. The words will be hers to say or to refuse to say, and this provides some degree of leverage over the position and over what will be made public. Going forward, these statements are generally taken to be the considered views of the U.S. government, and cannot easily be reversed. n192 Indeed, they are likely to be referred to in other contexts where U.S. officials are required to explain the government's position. n193 Of course, it is unlikely that speechmaking could be used to draw into the conversation an official who has no relevance to a particular area, but it may be effective in pulling up a critical chair to the table for an individual with both expertise and a structural connection to the matter at hand. The elevated seat at the table does not come cheaply for the speechmaker. The speechmaking-as-strategy process operates as a two-way street. By presenting the U.S. views on a topic in a public forum, the speechmaking official is sanctioning those views and signing on quite publicly to the U.S. position, in a way that will be difficult, if not impossible, to walk away from at a later date. n194 It is this legitimizing effect that the speechmaker often brings to the table in exchange for greater influence in the cultivation of the views that [\*400] will be presented. n195 This phenomenon may be most palpable in areas where an official may have greater legitimacy with a particular population that the Administration hopes to sway in large part because she is seen - rightly or wrongly - as potentially holding views in tension with the Administration's policies in that area. In such cases, the official both may desire greater leverage internally in order to influence decisionmaking, and may have an important legitimizing power in sanctioning the resulting views. Thus, both the speechmaking official and others in the Administration have something to gain in finding a compromise that permits the official to give a public speech on the matter. By way of example, State Department Legal Advisers - and even Secretaries of State n196 - have often been deployed to explain the U.S. government's legal position on matters affecting international law and national security, to both international and domestic audiences. Harold Koh's 2010 speech at the American Society of International Law, in which he discussed the Obama Administration's views toward targeting and detention in the conflict with al Qaeda, n197 received enormous public attention in part because of his stature as a leading human rights advocate. Thus, Koh's willingness to support the Administration's legal position was a boon to the Administration in facing criticism from the human rights community, and Koh presumably may have gained greater influence than he might otherwise have had in crafting the public statement of the Administration's position on wartime targeting and detention. Previously, under the Bush Administration, Legal Adviser John Bellinger gave a number of speeches explaining the U.S. government's understanding of its legal obligations under international law in the conflict with al Qaeda. n198 He publicly presented, explained, and defended the executive's positions - and in so doing worked toward trying to legitimize them - despite the fact that, as it is now widely known, he had had many disagreements with other Bush officials over many of the prevailing policies throughout the early years of the [\*401] Administration. n199 Considering the willingness of those other officials to cut the State Department out of the decisionmaking loop, as revealed years later by Legal Adviser Taft and others, n200 the ability to act as speechmaker and public face of the Administration's views of its authority likely elevated L's role in addressing these matters to some degree. At a bare minimum it ensured the State Department had a seat at the position-drafting table, which it might otherwise not have had.

The third plank solves the second adv without affecting cyber doctrine—their author

Matthew HAMMOND, attorney in the U.S. D.O.J., 1997 [“The Posse Comitatus Act: A Principle in Need of Renewal,” *Washington University Law Review*, Volume 75, Issue 2, 75 Wash. U. L. Q. 953, Lexis]

In response to the military presence in the Southern States during the Reconstruction Era, Congress passed the Posse Comitatus Act' ("PCA" or the "Act") to prohibit the use of the Army in civilian law enforcement. The Act embodies the traditional American principle of separating civilian and military authority and currently forbids the use of the Army and Air Force to enforce civilian laws.2 In the last fifteen years, Congress has deliberately eroded this principle by involving the military in drug interdiction at our borders This erosion will continue unless Congress renews the PCA's principle to preserve the necessary and traditional separation of civilian and military authority.¶ The need for reaffirmation of the PCA's principle is increasing because in recent years, Congress and the public have seen the military as a panacea for domestic problems.4 Within one week of the bombing of the federal building in Oklahoma City,' President Clinton proposed an exception to the PCA to allow the military to aid civilian authorities in investigations involving "weapons of mass destruction. ' In addition to this proposal Congress also considered legislation to directly involve federal troops in enforcing customs and immigration laws at the border.7 In the 1996 presidential campaign, candidate Bob Dole pledged to increase the role of the military in the drug war, and candidate Lamar Alexander even proposed replacing the Immigration and Naturalization Service and the Border Patrol with a new branch of the armed forces.'¶ The growing haste and ease with which the military is considered a panacea for domestic problems will quickly undermine the PCA if it remains unchecked. Minor exceptions to the PCA can quickly expand to become major exceptions. For example in 1981, Congress created an exception to the PCA to allow military involvement in drug interdiction at our borders.9 Then in 1989, Congress designated the Department of Defense as the "single lead agency" in drug interdiction efforts.'¶ The PCA criminalizes, effectively prohibiting, the use of the Army or the Air Force as a posse comitatus" to execute the laws of the United States. It reads:¶ Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.'2¶ Though a criminal law, the PCA has a more important role as a statement of policy that embodies "the traditional Anglo-American principle of separation of military and civilian spheres of authority, one of the fundamental precepts of our form of government."' 3 Major and minor exceptions to the PCA, which allow the use of the military in law enforcement roles, blur the line between military and civilian roles, undermine civilian control of the military, damage military readiness, and inefficiently solve the problems that they supposedly address.'4 Additionally, increasing the role of the military would strengthen the federal law enforcement apparatus that is currently under close scrutiny for overreaching its authority. 5 Although it seems benign, such an increase in military authority revives fears of past overreaching during the late 1960s.16¶ This Note argues that the principle embodied by the PCA should be renewed by rejecting exceptions to the Act and reaffirming the policy behind its inception. This renewal is necessary to preserve the historic division between civilian and military roles, to maintain civilian superiority over the military, to enhance military readiness, and to efficiently attack domestic problems. Part II reviews the historical traditional American fear of a standing army and the circumstances leading to the PCA's passage. Part III discusses the current scope of the PCA and the permissible roles of the military. Part IV explains how exceptions to the PCA endanger its underlying principle. The explanation covers the spectrum of possible exceptions to the PCA: drug interdiction, border duty, and biological and chemical weapons investigations. 7 Part V proposes legislative action to reaffirm the policy of the PCA and to limit to any further exceptions to it.¶

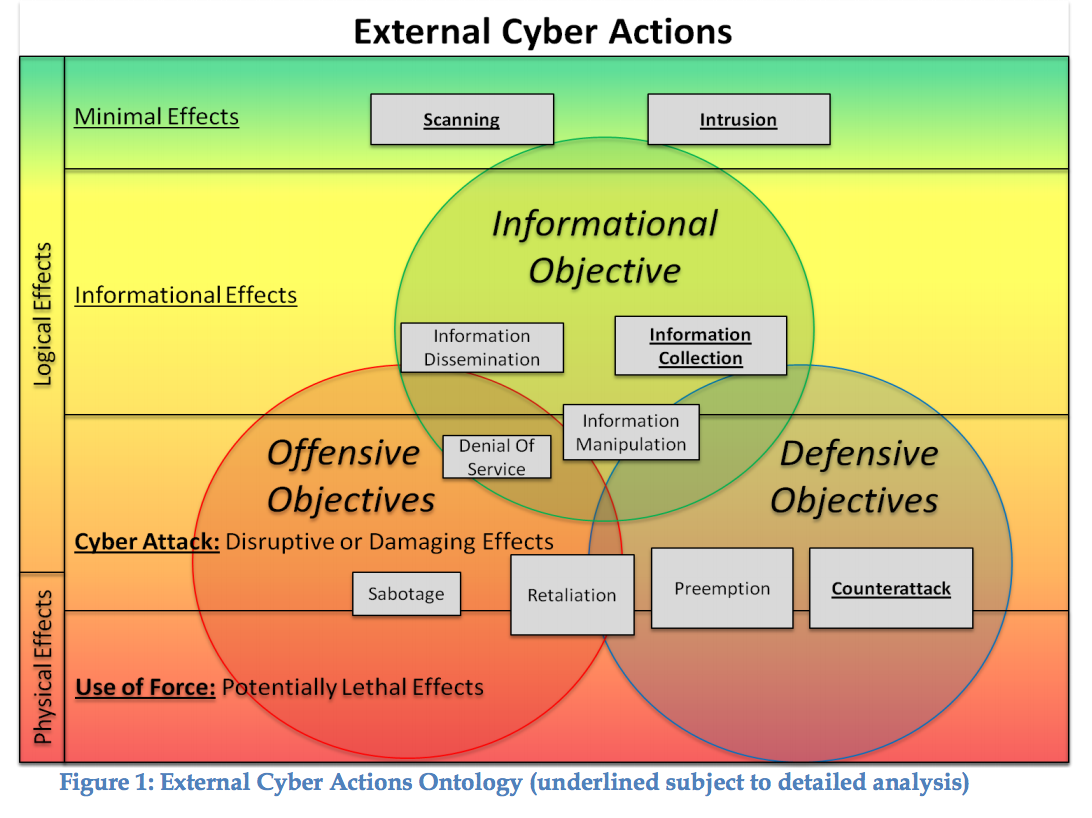
## 6

Interpretation and violation—“Offensive cyber operations” are attacks, sabotage, or retaliation – not information gathering or counterattacks.

Belk, naval aviator and politico-military fellow at the Harvard Kennedy School of Government, and Noyes, senior associate with the cybersecurity practice at Good Harbor Consulting, 3/20/2012

(Robert and Matthew, “On the Use of Offensive Cyber Capabilities,” http://belfercenter.ksg.harvard.edu/files/cybersecurity-pae-belk-noyes.pdf)

Current DoD definitions for Computer Network Operations (CNO) attempt to categorize cyber operations including nebulous definitions of Computer Network Attack (CNA) and Computer Network Defense (CND).3 This intent-based definition is internally inconsistent and **fails to provide useful distinctions for policy-making**. To rectify this issue, we have developed the following ontology based on a hierarchy of three criteria. 1) Target of the cyber operation: based on ownership of affected networks 2) Effect of the operation: by type (logical or physical) and degree (minimal to use of force) 3) Objective of the operation: whether **informational, offensive or defensive** Using this system, it is clear that **current classifications of offensive cyber operations are overly broad**, **applying actually to** **external cyber operations**. **Given this distinction**, **we provide a detailed examination of external cyber operations** as shown **in Figure 1**. Within this ontology, we have identified eleven types of external cyber actions, and have conducted detailed analyses of six: 1) Scanning, 2) Intrusion, 3) Information Collection, 4) Cyber Attack, 5) Counterattack, and 6) Cyber Force.



the plan mandates both of those – their 1ac author

Alan BUTLER, Appellate Advocacy Counsel, Electronic Privacy Information Center (EPIC); J.D. UCLA School of Law, 13 [June, 2013, “When Cyberweapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy,” American University Law Review, 62 Am. U.L. Rev. 1203, Lexis]

III. Applying the Third Amendment to Military Cyberoperations¶ The Third Amendment prohibitions govern military intrusions onto private property. Cyberoperations can affect private computers and networks, including innocent third-party systems. n169 As the U.S. military develops its strategy and begins to conduct cyberoperations, its actions affecting domestic systems must comply with Third Amendment principles.¶ Each category of cyberoperations has the potential to affect private systems in the United States. The use of a self-replicating virus or worm, such as Stuxnet, can result in widespread infection beyond the intended military target. Even more targeted cyberexploits, such as Flame or Red October, use intermediate networks and devices to gain access to their targets. Additionally, a retaliatory strike or hack-back may harm an innocent third-party system rather than the actual attacker. The Third Amendment governs all of these situations if the affected system belongs to someone under U.S. jurisdiction.¶ To determine whether the Third Amendment prohibits a given military cyberoperation, the relevant inquiry would be: (1) is the computer or network device property protected as part of "any house," and (2) does the military intrusion constitute "quartering" by a "Soldier"? If the network or device is protected, and the military intrusion constitutes quartering, then consent is required under the Third Amendment during times of peace and a formal legal enactment is required during times of war. [\*1228]¶ A. The Private Property Protected by the Third Amendment Includes Computer and Network Infrastructure¶ The first issue relevant to the Third Amendment analysis of military cyberoperations is whether civilian computers and networks are protected. The Third Amendment prohibits quartering "in any house." n170 This provision could be interpreted as protecting only residential buildings, as opposed to the "persons, houses, papers, and effects" protected by the Fourth Amendment. n171 However, the history of the Third Amendment indicates that it governs "quartering" on excludable private property generally, regardless of the specific structure or parcel used. n172 In respecting the "Owner['s]" right to exclude, the scope of the Third Amendment may in fact be broader than the Fourth Amendment. n173 The only federal court to fully analyze and apply the Third Amendment in a modern context took a similarly broad view of the protected property right. n174¶ The history surrounding the ratification of the Third Amendment also suggests that a broad view is appropriate. The English quartering statutes traditionally provided for quartering in "public houses" during wartime, n175 including the 1765 provision governing quartering in the Colonies. n176 These statutes specifically listed the types of structures that could be used for quartering. n177 This was even true of the Quartering Act of 1774, one of the "intolerable acts" that [\*1229] revolutionary colonists cited in the lead up to the war. n178 Notably, British soldiers "were not quartered in private colonial houses" during the pre-revolutionary period. n179 When the Third Amendment was enacted, however, Congress rejected an alternative proposal that would have allowed billeting of soldiers in public houses and inns. n180 Rather than provide specific rules based on the classification of property, Congress adopted a general prohibition governing "any house." n181¶ The Second Circuit adopted a broad view of the Third Amendment's property protections in Engblom. n182 There, the court analyzed the Third Amendment's application based on its role in assuring "a fundamental right to privacy," as noted by the Supreme Court in Griswold. n183 The Second Circuit rejected a rigid application of the term "Owner" because it "would be wholly anomalous when viewed, for example, alongside established Fourth Amendment doctrine" that protects tenants. n184 The court ultimately held that the Third Amendment's property-based privacy interests are not limited only to those "Owners" who possess a fee simple ownership of their residence but instead protect citizens who lawfully occupy or possess a residence. n185¶ In a more recent case, Custer County Action Ass'n v. Garvey, n186 the U.S. Court of Appeals for the Tenth Circuit rejected a claim under the Third Amendment based on the military use of airspace over a plaintiff's home. n187 The court reviewed the claim under the Engblom framework and found that the plaintiffs had no general right to exclude planes traversing the airspace over their property. n188 The Supreme Court had reached a similar conclusion under the Fifth [\*1230] Amendment Takings Clause years earlier in United States v. Causby. n189 Thus, the Tenth Circuit followed a similar analysis of the Third Amendment where "any home" was defined as a property area in which an individual has a right to exclude others. n190¶ When framed as a right to exclude the military from private property, it is clear that computers, networks, and other systems fall within the scope of the Third Amendment. The phrase "any house" encompasses all forms of property that fit within the typical paradigm. Rather than include or exclude certain types of property, the Framers opted for broad language. n191 Civilian networked devices will necessarily fall within this category because they are maintained within, and are a component of, private property. Hacking is analogous to a trespass, n192 and typical home and corporate systems can also rightfully be classified as private property. n193 Invasion of these systems is prohibited by comprehensive federal laws that recognize this general right to exclude. n194 [\*1231]¶

Vote negative for limits— they create a whole new topic area surrounding surveillance that was explicitly taken out of the res because it was too big

Precision is key – shapes NDT prep and research

## 7

The plan causes circumvention via PMCs—takes out the aff

Kruck ‘14

Andreas, Geschwister Scholl Institute for Political Science, University of Munich, “Theorising the use of private military and security companies: a synthetic perspective,” Journal of International Relations and Development, 2014, 17, (112–141)

In contrast with this functionalist view, the political-instrumentalist model conceives of privatisation as a strategy of governments to reduce **political costs** rather than enhance problem-solving effectiveness and economic costefficiency (Avant 2005: 60; Chesterman and Lehnardt 2007: 252–3; Avant and Sigelman 2010; Carmola 2010: 45–50, 90–91; Deitelhoff 2010: 198–9; Deitelhoff and Geis 2010). The use of PMSCs serves as an instrument for the **reduction of political costs** accruing to governments from warfare in the context of democratic politics. The political-instrumentalist model relies on the **principal-agent literature** on accountability-evasion, responsibility-shirking and blame-shifting as motives for delegation (Hood 2002; Flinders and Buller 2006; Bartling and Fischbacher 2012). According to this strand of principal-agent research, delegation may be a rational strategy for political cost-sensitive actors who seek to **avoid accountability** for (**potentially**) **controversial or unsuccessful policy decisions** and measures. The model also draws analogies from IR scholarship that has conceived of international cooperation through intergovernmental organisations as a ‘new raison d’e´tat’ (Wolf 1999), that is, **a deliberate strategy** that allows governments to enhance their autonomy **from parliamentary and societal actors** as the intergovernmental arena is largely insulated from effective political control. According to the political-instrumentalist model, governments are not mere transmitters of societally dominant interests but follow their own governmental interests and logics. They seek to keep or even expand their policy autonomy from other legislative and judiciary actors, as well as the broader public. From this perspective, the privatisation of security is a genuinely political and instrumentalist strategy of governments in **strong** and **democratic states** (Binder 2007: 307–8) that serves to **avoid politically costly parliamentary, civil society and media scrutiny,** **opposition and control in the area of security policies.** Democratic oversight and control mechanisms are politically costly because they increase transparency and reduce governments’ autonomy. They render decision-making and implementation more time-intense and cumbersome, less calculable and, ultimately, more risky for governmental actors. Moreover, research on the ‘Democratic Peace’ has shown that democratic electorates are casualty-sensitive (Scho¨ rnig 2008); that is, fallen soldiers can undermine electoral support for military operations and even for incumbent governments, which limits governments’ political leeway in matters of security policy. Failed and/or illegal **military interventions** can endanger incumbents’ re-election in democratic systems and may sometimes even force them to resign (Cockayne 2007: 206, 212; Carmola 2010: 45–60; Deitelhoff 2010: 198–9). By shifting security tasks from the public to the private sphere, governmental actors seek to **reduce (further**) the transparency of decision-making in the realm of security policy, **diffuse accountability**, circumvent democratic and legal control mechanisms and thus enhance their political autonomy in decisions concerning the use of military force. **The use of PMSCs thus increases the power of governments vis-a`-vis their parliaments** (Avant 2005: 60; Avant and Sigelman 2010; Deitelhoff and Geis 2010). Highly political security measures are ‘depoliticised’, that is, removed from contested and (at least somewhat) transparent parliamentary, civil society and media debates. **Transferring** the execution of **security functions to PMSCs** may **help governments** to **hide the origins, extent and consequences of unpopular decisions from other state organs** and broader constituencies (Cockayne 2007: 212). Thus, privatisation serves to cover or downplay the roles and responsibilities of governments. In extreme cases, the responsibility for controversial or unpopular policies is shifted to private actors — this may be attractive and succeed reasonably well if the appearance of a distance between the government and PMSCs can be upheld. PMSCs may then allow for covert foreign policy not approved of by the national public (Deitelhoff 2010: 198). Governmental actors profit from the lesser transparency, the weaker oversight and regulation, as well as the lower media profile of PMSCs compared with public armed forces (Chesterman and Lehnardt 2007; Schneiker 2007; Cutler 2010). In the absence of major scandals, PMSCs are still relatively low-key agents who fly under the radar of public scrutiny and are more or less insulated from intense public contestation and control. Their lack of transparency and accountability to parliaments and the broader public suits the governmental strategy of depoliticisation by delegation (Flinders and Buller 2006). Obviously, governments’ desire to reduce political costs through outsourcing would need to vary if it is to account for variation in the use of PMSCs. From a political-instrumentalist perspective, the crucial context variable that conditions governments’ desire to reduce political costs by delegation will be the anticipated political costliness of the decisions and measures that are to be taken, that is, their (un)popularity in the broader public. Thus, we can hypothesise from a political-instrumentalist perspective that **the less popular a military operation among the domestic audience**, **the greater will be the incentives of governmental actors to reduce political costs and the higher their propensity to rely on the security services of PMSCs.** States will first and foremost outsource politically and societally controversial tasks to PMSCs.

Destroys allied interoperability

Isenberg ‘9

David, researcher and leader of the Norwegian Initiative on Small Arms Transfers (NISAT) at the International Peace Research Institute, Oslo (PRIO), and the author of Shadow Force: Private Security Contractors in Iraq (Greenwood, 2009), “Private Military Contractors and U.S. Grand Strategy,” PRIO Report 1/2009

TODAY, THE U.S. GOVERNEMENT’S growing reliance on contractors constitutes an attempt to **circumvent** or evade **public skepticism** **about the U**nited **S**tates’ selfappointed role as global policeman. Viewing PMCs through a market framework focuses attention on questions of efficiency, at the expense of more fundamental considerations about the policy being pursued. The related question of whether force should be used – either by uniformed military personnel or else by private contractors – is often neglected. 69 In this respect, the low visibility and presumed low cost of private contractors appealed to those policy analysts who favor a global U.S. military presence, but fear that such a strategy cannot command public support. Max Boot, senior fellow for national security studies at the Council on Foreign Relations, has long championed the use of contractors on these grounds. Writing in The American Interest Boot explained: In a perfect world, Congress would bring the size of our armed forces into closer alignment with our massive defense commitments. But our legislature, like most democratic legislatures, is loath to spend what’s needed on defense, and it is even more reluctant to conscript its citizens... Just as Victorian parliaments stinted on the size of the British army, forcing reliance on regiments raised in India, so too our Congress will never provide enough uniformed personnel to address every perceived need... Thus, in all likelihood, we will continue to muddle along with a mixture of private and public providers of security services.70 Governments also rely on contractors in order to **shift responsibility and blame** for their actions. A state employing contractor personnel to advance its foreign policies faces **less international responsibility** in terms of attribution than would be the case if it relied on its own armed forces.71 But states bear responsibility for the actions of contractors they employ. They should not be allowed to evade responsibility, especially with respect to contractors functioning as the equivalent of the states’ armed forces. The United States is the world's leading user of private contractors because the U.S. government has assumed the role of guarantor of global stability at a time when the American public is unwilling to provide the resources necessary to support this strategy.72 Washington either has to use private contractors to fill the gap between goals and means or else change its goals, and policymakers have shown little interest in the latter. As the United States relies more heavily upon military contractors to support its role as world hegemon, it reinforces the tendency to **approach global crises in a unilateral**, as opposed to multilateral **manner**, further ensuring that the burdens will be carried disproportionately by U.S. taxpayers, and especially U.S. troops.73 Other states have not kept up with the ongoing qualitative changes in the United States military; their armed forces are not readily deployable **nor** easily **interoperable with American personnel and equipment.** In contrast, military contractors have not only geared themselves to serving the American marketplace, they have been instrumental in bringing about those changes within the U.S. military. The marketplace, in other words, can often more readily satisfy the United States’ operational requirements than can our allies and prospective regional partners. 74 The use of contractors has other deleterious effects, **including the weakening of our system of government.** Deborah Avant, a professor of political science at the University of California at Irvine and the Director of International Studies and the Center for Research on International and Global Studies, identifies three features that are common to democracies – constitutionalism, transparency and public consent, and concludes that the use of private security contractors in Iraq had “impeded constitutionalism and lowered transpar- ency.” She speculates that it had circumvented or impeded “effective public consent.” 75 Because Congress has less information about and control over the use of contractors than the use of troops, the White House and the Pentagon can rely on contractors to evade congressional (and, indirectly, public) opposition. 76 PMC employees usually remain outside the formal chain of command and are not allowed to take part in hostilities because they are regarded as civilians under International Humanitarian Law. However, in most of the military interventions today the distinction between frontline and hinterland blurs, bringing PMCs who are most active in logistics, site and convoy security and weapon maintenance ever closer to theater and to an active participation in hostilities. This not only increases risks that they will become a target of military attacks, it also calls upon the regular forces to extend their protection to these companies. Additionally, coordination is needed to prevent conflicts between the regular forces and the PMCs. The increase of so-called blue-on-white fire in Iraq — accidental attacks between U.S. forces and the contractors — indicates how difficult that is. 77 On a broader level, because the use of PMC receives less attention than the use of regular troops, **this reduces the political cost of using force**. Bluntly put, if someone is contributing to the war effort but is not on active duty in the U.S. military, nobody beyond his or her immediate family cares if they get killed. By contrast, the death of even a single infantryman or marine routinely winds up on the front page of the major papers.

Allied interoperability prevents Hormuz closure and SCS conflict—overcomes Chinese regional A2/AD

Armitage ‘12

Richard, president of Armitage International and a trustee of CSIS. From 2001 to 2005, he served as U.S. deputy secretary of state., Joseph S. Nye, dean emeritus of the Kennedy School of Government at Harvard University and a trustee of CSIS. “The U.S.-Japan Alliance anchoring stability in asia,” CSIS August 2012 report

Japan can more fully exercise defense and military diplomacy through capacity building and bilateral and multilateral measures. A new roles and missions review should expand the scope of Japan’s responsibilities to include the defense of Japan and defense with the United States in regional contingencies. The most immediate challenge is in Japan’s own neighborhood. China’s **assertive claims** to most of the East China Sea and virtually all of the South China Sea and the **dramatic increase** in the operational tempo of the PLA and other maritime services, including repeated circumnavigation of Japan, reveal Beijing’s intention to assert greater strategic influence throughout the “First Island Chain” (Japan-Taiwan-Philippines) or what Beijing considers the “Near Sea.” In response to these kinds of anti-access/area denial (A2AD) challenges, the United States has begun work on new operational concepts such as Air Sea Battle and the Joint Operational Access Concept (JOAC). Japan has begun work on parallel concepts such as “dynamic defense.” While the U.S. Navy and the Japan Maritime Self-Defense Forces (JMSDF) have historically led in bilateral interoperability, the new environment requires **significantly greater jointness and interoperability** across services in both countries and bilaterally between the United States and Japan. This challenge should be at the core of the bilateral RMC dialogue and must be fully integrated and driven forward by senior leadership in the U.S. Departments of Defense and State together with the Japanese Ministries of Defense (MOD) and Foreign Affairs (MOFA). In a time of budgetary constraints, RMC cannot be addressed piecemeal or by lower-level officials. Two additional areas for potential increased alliance defense cooperation are in minesweeping in **the Persian Gulf** and joint surveillance of the South China Sea. The Persian Gulf is a **vital global trade and energy transit hub**. At the first rhetorical sign or indication of Iran’s intention to close the Strait of Hormuz, Japan should unilaterally send minesweepers to the region to counter this internationally illegal move. **Peace and stability in the South China Sea are** yet **another vital allied interest** **with** especially **profound salience for Japan**. With 88 percent of Japan’s supplies, including vital energy resources, transiting through the South China Sea, it is in Japan’s interest to increase surveillance in collaboration with the United States to ensure stability and continued freedom of navigation. The distinction between the “Defense of Japan” and regional security is thin. A sealed-off Strait of Hormuz or a military contingency in the South China Sea will have severe implications for the security and stability of Japan. The once-touted sword and shield analogy oversimplifies current security dynamics and glosses over the fact that Japan requires offensive responsibilities to provide for the defense of the nation. Both allies require **more robust**, shared, and **interoperable** Intelligence, Surveillance, and Reconnaissance (ISR) **capabilities** and operations that extend well beyond Japanese territory. For their part, U.S. Forces in Japan (USFJ) should have specific roles assigned in the defense of Japan. With the goal of operational competency and eventual USFJ-JSDF joint task force capability in mind, the United States should allocate greater responsibility and sense of mission to the USFJ. Amidst looming budget cuts and fiscal austerity in both Washington and Tokyo, **smarter** use of resources is essential to maintain capabilities. A primary manifestation of smarter resource implementation is interoperability. Interoperability is not a code word for buying U.S. equipment. At its core, it **is the fundamental ability to work together**. The U.S. Navy and JMSDF have demonstrated this ability for decades. The U.S. Air Force and Japan Air Self-Defense Force (JASDF) are making progress; but U.S. Army/Marine Corps cooperation with the Japan Ground Self-Defense Force (JGSDF) has been limited due to a contrast in focus. The United States has concentrated its efforts on fighting ground wars in the Middle East, while Japan has conducted peacekeeping and disaster relief operations.

SCS conflict causes extinction

Wittner 11 (Lawrence S. Wittner, Emeritus Professor of History at the State University of New York/Albany, Wittner is the author of eight books, the editor or co-editor of another four, and the author of over 250 published articles and book reviews. From 1984 to 1987, he edited Peace & Change, a journal of peace research., 11/28/2011, "Is a Nuclear War With China Possible?", [www.huntingtonnews.net/14446](http://www.huntingtonnews.net/14446))

While nuclear weapons exist, there remains a danger that they will be used. After all, for centuries national conflicts have led to wars, with nations employing their deadliest weapons. The current deterioration of U.S. relations with China might end up providing us with yet another example of this phenomenon. The gathering tension between the United States and China is clear enough. Disturbed by China’s growing economic and military strength, the U.S. government recently challenged China’s claims in the South China Sea, increased the U.S. military presence in Australia, and deepened U.S. military ties with other nations in the Pacific region. According to Secretary of State Hillary Clinton, the United States was “asserting our own position as a Pacific power.” But need this lead to nuclear war? Not necessarily. And yet, there are signs that it could. After all, both the United States and China possess large numbers of nuclear weapons. The U.S. government threatened to attack China with nuclear weapons during the Korean War and, later, during the conflict over the future of China’s offshore islands, Quemoy and Matsu. In the midst of the latter confrontation, President Dwight Eisenhower declared publicly, and chillingly, that U.S. nuclear weapons would “be used just exactly as you would use a bullet or anything else.” Of course, China didn’t have nuclear weapons then. Now that it does, perhaps the behavior of national leaders will be more temperate. But the loose nuclear threats of U.S. and Soviet government officials during the Cold War, when both nations had vast nuclear arsenals, should convince us that, even as the military ante is raised, nuclear saber-rattling persists. Some pundits argue that nuclear weapons prevent wars between nuclear-armed nations; and, admittedly, there haven’t been very many—at least not yet. But the Kargil War of 1999, between nuclear-armed India and nuclear-armed Pakistan, should convince us that such wars can occur. Indeed, in that case, the conflict almost slipped into a nuclear war. Pakistan’s foreign secretary threatened that, if the war escalated, his country felt free to use “any weapon” in its arsenal. During the conflict, Pakistan did move nuclear weapons toward its border, while India, it is claimed, readied its own nuclear missiles for an attack on Pakistan. At the least, though, don’t nuclear weapons deter a nuclear attack? Do they? Obviously, NATO leaders didn’t feel deterred, for, throughout the Cold War, NATO’s strategy was to respond to a Soviet conventional military attack on Western Europe by launching a Western nuclear attack on the nuclear-armed Soviet Union. Furthermore, if U.S. government officials really believed that nuclear deterrence worked, they would not have resorted to championing “Star Wars” and its modern variant, national missile defense. Why are these vastly expensive—and probably unworkable—military defense systems needed if other nuclear powers are deterred from attacking by U.S. nuclear might? Of course, the bottom line for those Americans convinced that nuclear weapons safeguard them from a Chinese nuclear attack might be that the U.S. nuclear arsenal is far greater than its Chinese counterpart. Today, it is estimated that the U.S. government possesses over five thousand nuclear warheads, while the Chinese government has a total inventory of roughly three hundred. Moreover, only about forty of these Chinese nuclear weapons can reach the United States. Surely the United States would “win” any nuclear war with China. But what would that “victory” entail? A nuclear attack by China would immediately slaughter at least 10 million Americans in a great storm of blast and fire, while leaving many more dying horribly of sickness and radiation poisoning. The Chinese death toll in a nuclear war would be far higher. Both nations would be reduced to smoldering, radioactive wastelands. Also, radioactive debris sent aloft by the nuclear explosions would blot out the sun and bring on a “nuclear winter” around the globe—destroying agriculture, creating worldwide famine, and generating chaos and destruction.

## Preemption

Obama circumvents the plan

Wolfgang 1/16/14

Ben, White House Correspondent for the Washington Times, “Little change expected in U.S. surveillance policy,” http://www.washingtontimes.com/news/2014/jan/16/little-change-expected-in-us-surveillance-policy/

If the skeptics are correct, President Obama is about to **embrace** and endorse many of the controversial national-security tools and tactics introduced by his predecessor, despite railing against those policies while campaigning for the Oval Office in 2008. Expectations for Friday's long-awaited address, in which Mr. Obama will outline changes to U.S. spying, surveillance and data-collection efforts, are exceedingly low among privacy advocates and others. They expect the president, while paying **lip service** to the notion of privacy protections and limited government power, to continue the practices first established by the Bush administration in the aftermath of the Sept. 11, 2001, terrorist attacks. Mr. Obama's shift shouldn't come as a surprise, political analysts say, and can be partly attributed to the fact that **it's simply difficult for a president to ever give up authority,** **especially if that authority is meant to protect American lives.** It also may come from the fact that the president fears being viewed by history as the commander in chief who curtailed intelligence-gathering only to see a terrorist attack occur, said William Howell, a politics professor at the University of Chicago who has written extensively on presidential power. "When you're running for office, you may espouse the benefits of a limited executive, but when you assume office, there are **profound pressures** **to claim** and nurture **and exercise authority** at every turn **and not** to **relinquish** the **powers available to you**," Mr. Howell said. Leading up to and during his 2008 presidential campaign, Mr. Obama made it a point to separate himself from Mr. Bush on the national security front, but there remain many **notable similarities**. Guantanamo Bay still is operational, despite repeated pledges from the president that he'd close the U.S. detentional facility in Cuba and house enemy combatants elsewhere. Mr. Obama has dramatically **increased** the use of drones to target terrorists abroad — a step the administration vehemently defends as being quicker, more effective and far less dangerous to American personnel than sending in ground troops. U.S. surveillance efforts, rather than having been reined in, have in some ways **expanded**. In the process, they have caused Mr. Obama significant foreign policy headaches.

Obama will signing statement the aff—hollows the restriction out

Jeffrey Crouch, assistant professor of American politics at American University, Mark J. Rozell, acting dean and a professor of public policy at George Mason University, and Mitchel A. Sollenberger, associate professor of political science at the University of Michigan-Dearborn, December 2013, The Law: President Obama's Signing Statements and the Expansion of Executive Power, Presidential Studies Quarterly 43.4

In a January 2013 signing statement, President Barack Obama stated that his constitutional powers as president limited him to signing or vetoing a law outright and that he lacked the authority to reject legislative provisions “one by one.” Yet he then proceeded in a nearly 1,200 word statement to pick the law apart, section by section, and to effectively challenge many provisions by declaring that they violated his constitutional powers as commander in chief. According to his signing statement, a provision restricting the president's authority to transfer detainees to foreign countries “hinders the Executive's ability to carry out its military, national security, and foreign relations activities and would, under certain circumstances, violate constitutional separation of powers principles” (Obama 2013). Obama did not mention, however, that Congress specifically authorized transfers to foreign countries as long as the secretary of defense, with the concurrence of the secretary of state and in consultation with the director of national intelligence, certified that the foreign government receiving the detainees was not a designated state sponsor of terrorism and possessed control over the facility the individual would be housed (P.L. 112-239; see Fisher 2013). Obama also objected to a number of provisions that he claimed would violate his “constitutional duty to supervise the executive branch” and several others that he said could encroach upon his “constitutional authority to recommend such measures to the Congress as I ‘judge necessary and expedient.’ My Administration will interpret and implement these provisions in a manner that does not interfere with my constitutional authority” (Obama 2013). What the president could not block or modify through concessions or veto threats during budget negotiations with members of Congress, he decided he could unilaterally strip from a signed bill. Similar to his predecessor, George W. Bush, Obama suggested that he was the ultimate “decider” on what is constitutional and proper. Few acts by occupants of the White House so completely embody the unchecked presidency. Candidate Obama on Signing Statements President Obama's actions have been surprising given that he proclaimed while first running for his office that he would not issue signing statements that modify or nullify acts of Congress (YouTube 2013 2013). In a December 2007 response to the Boston Globe, presidential candidate Obama provided a detailed explanation for his thinking: “I will not use signing statements to nullify or undermine congressional instructions as enacted into law. The problem with [the George W. Bush] administration is that it has attached signing statements to legislation in an effort to change the meaning of the legislation, to avoid enforcing certain provisions of the legislation that the President does not like, and to raise implausible or dubious constitutional objections to the legislation” (Savage 2007a). Candidate Obama's objection to President Bush's actions centered on one of the three varieties of signing statement, in this case, a “constitutional” signing statement. In a “constitutional” signing statement, a president not only points out flaws in a bill, but also declares—in often vague language—his intent not to enforce certain provisions. Such statements may be different than ones that are “political” in nature. In “political” signing statements, a president gives executive branch agencies guidance on how to apply the law.1 Finally, the most common type of signing statements are “rhetorical,” whereby the intent of the president is to focus attention on one or more provisions for political gain (Kelley 2003, 45-50). President Obama's Policy on Signing Statements At the start of his term, it seemed that President Obama would honor his campaign commitments and break with his predecessor when he issued a memorandum to heads of executive branch departments and agencies regarding his policy on signing statements. In this memorandum, he wrote, “there is no doubt that the practice of issuing [signing] statements can be abused.” He objected to the use of signing statements where a president disregards “statutory requirements on the basis of policy disagreements.” Only when signing statements are “based on well-founded constitutional objections” do they become legitimate. Therefore, “in appropriately limited circumstances, they represent an exercise of the President's constitutional obligation to take care that the laws be faithfully executed, and they promote a healthy dialogue between the executive branch and the Congress.” President Obama proceeded to list four key principles he would follow when issuing signing statements: (1) Congress shall be informed, “whenever practicable,” of the president's constitutional objections; (2) the president “will act with caution and restraint” when issuing statements that are based on “well-founded” constitutional interpretations; (3) there will be “sufficient specificity” in each statement “to make clear the nature and basis of the constitutional objection”; and finally, (4) the president would “construe a statutory provision in a manner that avoids a constitutional problem only if that construction is a legitimate one” (Obama 2009a). Media coverage praised President Obama's action. The Boston Globe declared, “Obama reins in signing statements” (Editorial 2009). David Jackson of USA Today reported, “Obama tried to overturn his predecessor again on Monday, saying he will not use bill signing statements to tell his aides to ignore provisions of laws passed by Congress that he doesn't like” (Jackson 2009). Another reporter noted, President Obama “signaled that, unlike Bush, he would not use signing statements to do end runs around Congress” (James 2009). Any expectations for a shift in the exercise of signing statements ultimately were misplaced, as President Obama, like his predecessor, has used signing statements in ways that attempt to increase presidential power. In this article, we first describe and analyze the continuity of policy and action between Barack Obama and George W. Bush. Second, we address why signing statements—at least one type of them—can not only be unconstitutional abuses of presidential power, but may also be unproductive tools for promoting interbranch dialogue and cooperation. Third, we show that signing statements are a natural result of expanding power in the modern presidency and that they have come to be used as a means of unilateral executive action. Finally, we provide a possible corrective to some of the more aggressive forms of constitutional signing statements that impact appropriations.

Can’t operationalize restrictions—no definitional clarity makes the aff incoherent

Brown, senior legal advisor – U.S. Cyber Command, and Metcalf, senior legal advisor – U.S. Marine Corps Forces Cyberspace Command, ‘14

(Gary D. and Andrew O., “Easier Said Than Done: Legal Reviews of Cyber Weapons,” *Journal of National Security Law & Policy* Vol. 7)

The terms “cyber attack” or “cyber warfare” imply the employment of cyber weapons. But the uncertainty in the term “cyber warfare” leads to equal uncertainty in identifying cyber weapons, and great confusion about when the use of a “cyber weapon” is a “cyber attack” that creates a state of “cyber warfare.” There have been some excellent attempts to define “cyber weapon” with specificity and to use that discussion to gain a better understanding of cyber war.3 These discussions are intellectually stimulating, but the purpose of this paper is to highlight the difficulty in transforming these broad topics of academic discussion into practical legal advice for those few practitioners advising commanders on the impact of cyber law on operations. Military attorneys must translate academic and deeply theoretical discussions into concrete legal advice. That experience informs this article, which offers examples of how the practicalities of cyber war may collide with the academic discourse, in the hope of informing and shaping the debate. The actual examples of cyber capabilities and operations offered here highlight the practical issues involved in cyberspace operations, where attorneys are called upon to analyze cyber operations under the existing legal regime regarding weapons, and the means and methods of war. Ultimately, this article concludes that treating all cyber techniques as weapons is impractical. Rather, an assessment focusing on how a capability will be used in context, especially of the primary purpose of the capability, is more effective and consonant with international law. This approach will more clearly delineate cyber attacks, and permit a separate discussion of the great majority of cyber events – those that fall below the level of attack. What this paper does not do is discuss the difference between state-sponsored cyber operations, including cyber warfare and cyber espionage, and cyber crimes. Distinguishing between state uses of cyberspace, and the operations of criminal groups by examining the technical details of cyber incidents is usually not possible. Ultimately, this can only be determined by learning and assessing the motivation of the responsible party, and issues of agency and attribution may make this a near-impossible task. Agency is a particularly thorny problem. The keyboard operator may think he is merely part of a criminal enterprise stealing intellectual property or assisting in an extortion scheme, but the entity paying the bills could as easily be a government pursuing a national security agenda. Conversely, agents of foreign intelligence services may occasionally moonlight as cyber criminals for a few extra bucks. In the end, it is the effect of the action that matters. If all the money is disappearing from a bank, it makes little difference to the bank and its customers whether the malevolent actor is a criminal or a spy – they just want the theft to stop. I. ESPIONAGE VS. OPERATIONS One of the first practical issues confronting a cyber operations lawyer is the artificial distinction between espionage and operations. While it’s true there is a long-standing (and cynically named) “gentleman’s agreement” between nations to ignore espionage in international law, determining exactly which cyber actions constitute espionage and not something of a different nature presents a real challenge. Despite the similarities between cyber-spying and more aggres-sive activity in this operations space, cyber experts and policymakers seem intent on excluding espionage from the same consideration that other cyber operations receive.4 While this firm distinction may have been workable in the age of microfilm, cameras and spies, there are significant challenges in applying this old paradigm to cyber operations. First, espionage used to be a lot more difficult. Cold Warriors did not anticipate the wholesale plunder of our industrial secrets. Second, the techniques of cyber espionage and cyber attack are often identical, and cyber espionage is usually a necessary prerequisite for cyber attack. On the receiving end, there may be little or no ability to distinguish between cyber techniques used for espionage and those used for warfare. Once an adversary takes control of a computer, he can do what he wants. Initial actions might involve stealing information, but the adversary can use the same access to disrupt or destroy the system, as well. The treatment of espionage in international law may have made some sense prior to the advent of cyber espionage, but looks increasingly ill-suited for the modern world. Cyber espionage, far from being simply the copying of information from a system, ordinarily requires some form of cyber maneuvering that makes it possible to exfiltrate information.5 That maneuvering, or “enabling” as it is sometimes called, requires the same techniques as an operation that is intended solely to disrupt. Enabling operations themselves can – deliberately or accidentally – also be just as disruptive to a computer system as an action undertaken for the specific purpose of disrupting the system. For example, an enabling operation could set out to weaken encryption or disable a cyber capability to force the target into using an alternate system that provides easier access to his communications. And, once a system is compromised, the new “owner” of the system can take whatever action he chooses on the compromised system, from manipulating data, to destroying the software, to, in some cases, actually physically breaking the hardware. From the victim’s perspective, if this unauthorized access is discovered prior to being used, there is no way to tell from mere observation whether the unauthorized user will choose to engage in espionage, system disruption or destruction. Often, the only difference between military cyber operations intended to collect intelligence and those designed to deliver cyber effects is the intent – intelligence activities are done with the intent of collecting intelligence, while other military activities are done in support of operational planning or execution. The military regularly conducts a broad range of activities outside of cyber that support its ability to execute traditional military operational plans. Some of the support is direct, such as collecting intelligence on areas of interest and strategically pre-positioning forces or supplies so they are available during future crises. Other support is indirect, such as training partner nation militaries or entering into mutual support agreements with friendly countries. Most support activities outside the cyber realm are non-controversial from a legal perspective, though they may be conducted clandestinely and without the consent of the nation where they are being conducted. This unnatural dichotomy in cyberspace activities makes providing legal advice a different and much more challenging activity than it is in traditional military operations. An activity in cyberspace may be entirely uncontroversial when the primary articulated purpose is intelligence, while the identical activity, conducted for a purpose other than collecting intelligence, may be defined as an “attack” with a “weapon” that requires an extensive analysis involving every branch of government.6 As set out below, providing a proper definition of “cyber weapon” may provide a basis for a more objective determination of the nature of activities in cyberspace.

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).

## PC

Drug interdiction and border duty are bigger internal links to their advantage that they can’t solve – their 1ac evidence sets the bar super low for spillover so it takes out the impact – and its from 97 so err neg

Matthew HAMMOND, attorney in the U.S. D.O.J., 1997 [“The Posse Comitatus Act: A Principle in Need of Renewal,” *Washington University Law Review*, Volume 75, Issue 2, 75 Wash. U. L. Q. 953, Lexis]

In response to the military presence in the Southern States during the Reconstruction Era, Congress passed the Posse Comitatus Act' ("PCA" or the "Act") to prohibit the use of the Army in civilian law enforcement. The Act embodies the traditional American principle of separating civilian and military authority and currently forbids the use of the Army and Air Force to enforce civilian laws.2 In the last fifteen years, Congress has deliberately eroded this principle by involving the military in drug interdiction at our borders This erosion will continue unless Congress renews the PCA's principle to preserve the necessary and traditional separation of civilian and military authority.¶ The need for reaffirmation of the PCA's principle is increasing because in recent years, Congress and the public have seen the military as a panacea for domestic problems.4 Within one week of the bombing of the federal building in Oklahoma City,' President Clinton proposed an exception to the PCA to allow the military to aid civilian authorities in investigations involving "weapons of mass destruction. ' In addition to this proposal Congress also considered legislation to directly involve federal troops in enforcing customs and immigration laws at the border.7 In the 1996 presidential campaign, candidate Bob Dole pledged to increase the role of the military in the drug war, and candidate Lamar Alexander even proposed replacing the Immigration and Naturalization Service and the Border Patrol with a new branch of the armed forces.'¶ The growing haste and ease with which the military is considered a panacea for domestic problems will quickly undermine the PCA if it remains unchecked. Minor exceptions to the PCA can quickly expand to become major exceptions. For example in 1981, Congress created an exception to the PCA to allow military involvement in drug interdiction at our borders.9 Then in 1989, Congress designated the Department of Defense as the "single lead agency" in drug interdiction efforts.'¶ The PCA criminalizes, effectively prohibiting, the use of the Army or the Air Force as a posse comitatus" to execute the laws of the United States. It reads:¶ Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.'2¶ Though a criminal law, the PCA has a more important role as a statement of policy that embodies "the traditional Anglo-American principle of separation of military and civilian spheres of authority, one of the fundamental precepts of our form of government."' 3 Major and minor exceptions to the PCA, which allow the use of the military in law enforcement roles, blur the line between military and civilian roles, undermine civilian control of the military, damage military readiness, and inefficiently solve the problems that they supposedly address.'4 Additionally, increasing the role of the military would strengthen the federal law enforcement apparatus that is currently under close scrutiny for overreaching its authority. 5 Although it seems benign, such an increase in military authority revives fears of past overreaching during the late 1960s.16¶ This Note argues that the principle embodied by the PCA should be renewed by rejecting exceptions to the Act and reaffirming the policy behind its inception. This renewal is necessary to preserve the historic division between civilian and military roles, to maintain civilian superiority over the military, to enhance military readiness, and to efficiently attack domestic problems. Part II reviews the historical traditional American fear of a standing army and the circumstances leading to the PCA's passage. Part III discusses the current scope of the PCA and the permissible roles of the military. Part IV explains how exceptions to the PCA endanger its underlying principle. The explanation covers the spectrum of possible exceptions to the PCA: drug interdiction, border duty, and biological and chemical weapons investigations. 7 Part V proposes legislative action to reaffirm the policy of the PCA and to limit to any further exceptions to it.¶

Healy says Katrina wrecked readiness

AND

It’s about using soldiers as police officers

Gene HEALY, senior editor at the Cato Institute, 5 [September 27, 2005, “Domestic Militarization: A Disaster in the Making,” http://www.cato.org/publications/commentary/domestic-militarization-disaster-making]

Having already wrecked a legendary American city, Hurricane Katrina may now be invoked to undermine a fundamental principle of American law; that principle, enshrined in the Posse Comitatus Act, is that when it comes to domestic policing, the military should be a last resort, not a first responder.¶ In his televised address on September 15, President Bush declared that “It is now clear that a challenge on this scale requires greater federal authority and a broader role for the armed forces—the institution of our government most capable of massive logistical operations on a moment’s notice.” Senator John Warner (R-Va.), chair of the Armed Services Committee, goes further. In the wake of Katrina, he’s suggested weakening Posse Comitatus, the longstanding federal law that restricts the government’s ability to use the U.S. military as a police force. Pentagon spokesman Lawrence Di Rita called Posse Comitatus a “very archaic” law that hampers the president’s ability to respond to a crisis.¶ Not so. The Posse Comitatus Act is no barrier to federal troops providing logistical support during natural disasters. Nor does it prohibit the president from using the army to restore order in extraordinary circumstances—even over the objection of a state governor.¶ What it does is set a high bar for the use of federal troops in a policing role. That reflects America’s traditional distrust of using standing armies to enforce order at home, a distrust that’s well-justified.¶ There are very good reasons to resist any push toward domestic militarization. As one federal court has explained, “military personnel must be trained to operate under circumstances where the protection of constitutional freedoms cannot receive the consideration needed in order to assure their preservation. The Posse Comitatus statute is intended to meet that danger.” Army Lt. Gen. Russell Honore, commander of the federal troops helping out in New Orleans, seemed to recognize that danger when he ordered his soldiers to keep their guns pointed down: “This isn’t Iraq,” he growled.¶ Soldiers are trained to be warriors, not peace officers—which is as it should be. But putting full-time warriors into a civilian policing situation can result in serious collateral damage to American life and liberty.¶ It can also undermine military readiness, because when soldiers are forced into the role of police officers, their war-fighting skills degrade. That’s what the General Accounting Office concluded in a 2003 report looking at some of the homeland security missions the military was required to carry out after September 11, 2001. According to the report, “While on domestic military missions, combat units are unable to maintain proficiency because these missions provide less opportunity to practice the varied skills required for combat and consequently offer little training value.” GAO also concluded that such missions put a serious strain on a military already heavily committed abroad.¶ American law calls for civilian peace officers to keep the peace, or, failing that, National Guardsmen under the command of their state governors. So perhaps we should stop treating the National Guard as if it’s no different than the Army Reserve. As Katrina made landfall, there were 7,000 guardsmen from Louisiana and Mississippi deployed in Iraq. Among them were 3,700 members of Louisiana’s 256th Mechanized Infantry Brigade, who took with them high-water vehicles and other equipment that could have been put to better use in New Orleans. The guardsmen here at home had only one satellite phone for the entire Mississippi coast, when Katrina initially hit—because the others were in Iraq. Lt. Gen. Steven Blum, chief of the National Guard Bureau, noted that had the Louisiana Guardsmen “been at home and not in Iraq, their expertise and capabilities could have been brought to bear.” Disaster relief and responding to civil disturbances are core missions for the Guard; attempting to establish democracy in the Middle East is not.¶ The Katrina tragedy ought to be an occasion for rethinking a number of federal policies, including our promiscuous use of the Guard abroad. Instead, Washington seems poised to embrace further centralization and militarization at home. That has the makings of a policy disaster that would dwarf Hurricane Katrina.

# 2nc

## \*\*\*pmcs da

## ov

Asian wars most likely and deadly

**Campbell et al 8** (Kurt M, Assistant Secretary of State for East Asian and Pacific Affairs, Dr. Campbell served in several capacities in government, including as Deputy Assistant Secretary of Defense for Asia and the Pacific, Director on theNational Security Council Staff, previously the Chief Executive Officer and co-founder of the Center for a New American Security (CNAS), served as Director of the Aspen Strategy Group and the Chairman of the Editorial Board of the Washington Quarterly, and was the founder and Principal of StratAsia, a strategic advisory company focused on Asia, rior to co-founding CNAS, he served as Senior Vice President, Director of the International Security Program, and the Henry A. Kissinger Chair in National Security Policy at the Center for Strategic and International Studies, doctorate in International Relation Theory from Oxford, former associate professor of public policy and international relations at the John F. Kennedy School of Government and Assistant Director of the Center for Science and International Affairs at Harvard University, member of Council on Foreign Relations and  International Institute for Strategic Studies, “The Power of Balance: America in iAsia” June 2008, <http://www.cnas.org/files/documents/publications/CampbellPatelSingh_iAsia_June08.pdf>)

Asian *investment* is also at record levels. Asian countries lead the world with unprecedented infra­structure projects. With over $3 trillion in foreign currency reserves, Asian nations and businesses are starting to shape global economic activity. Indian firms are purchasing industrial giants such as Arcelor Steel, as well as iconic brands of its once-colonial ruler, such as Jaguar and Range Rover. China’s Lenovo bought IBM’s personal computer We call the transformations across the Asia-Pacific the emergence of “iAsia” to reflect the adoption by countries across Asia of fundamentally new stra­tegic approaches to their neighbors and the world. Asian nations are pursuing their interests with real power in a period of both tremendous potential and great uncertainty. iAsia is: *Integrating:* iAsia includes increasing economic interdependence and a flowering of multinational forums to deal with trade, cultural exchange, and, to some degree, security. *Innovating:* iAsia boasts the world’s most successful manufacturing and technology sectors and could start taking the lead in everything from finance to nanotech to green tech. *Investing:* Asian nations are developing infrastruc­ture and human capital at unprecedented rates. But the continent remains plagued by: Insecurity: Great-power rivalry is alive in Asia. Massive military investments along with historic suspicions and contemporary territorial and other conflicts make war in Asia plausible. Instability: From environmental degradation to violent extremism to trafficking in drugs, people, and weapons, Asian nations have much to worry about. *Inequality:* Within nations and between them, inequality in Asia is more stark than anywhere else in the world. Impoverished minorities in countries like India and China, and the gap in governance and capacity within countries, whether as back­ward as Burma or as advanced as Singapore, present unique challenges. A traditional approach to Asia will not suffice if the United States is to both protect American interests and help iAsia realize its potential and avoid pitfalls. business and the Chinese government, along with other Asian financial players, injected billions in capital to help steady U.S. investment banks such as Merrill Lynch as the American subprime mortgage collapse unfolded. Chinese investment funds regional industrialization, which in turn creates new markets for global products. Asia now accounts for over 40 percent of global consumption of steel 4 and China is consuming almost half of world’s available concrete. 5 Natural resources from soy to copper to oil are being used by China and India at astonishing rates, driving up commodity prices and setting off alarm bells in Washington and other Western capitals. Yet Asia is not a theater at peace. On average, between 15 and 50 people die every day from causes tied to conflict, and suspicions rooted in rivalry and nationalism run deep. The continent harbors every traditional and non-traditional challenge of our age: it is a cauldron of religious and ethnic tension; a source of terror and extrem­ism; an accelerating driver of the insatiable global appetite for energy; the place where the most people will suffer the adverse effects of global climate change; the primary source of nuclear proliferation; and the most likely theater on Earth for a major conventional confrontation and even a nuclear conflict. Coexisting with the optimism of iAsia are the ingredients for internal strife, non-traditional threats like terrorism, and traditional interstate conflict, which are all magnified by the risk of miscalculation or poor decision-making.

## turns case

PMCs will take over cyber—drives aggression and turns case

Nair ‘12

Srijith, PhD computer science, fellow of Cyber Strategy Studies at The Takshashila Institution, Principal Researcher at Security Futures Practice of BT Innovate & Design, “Use of private companies in cyber operations,” http://vyuha.nationalinterest.in/use-of-private-companies-in-cyber-operations/

US Homeland Security Secretary Janet Napolitano’s recent comment that the administration **has and will consider** the participation of private companies in “**proactive” cyber “counterattacks**” has received its share of attention: In discussing the private partnerships she is promoting to combat cyberattacks, Napolitano was asked if instead of just taking defensive measures, the government and companies should be launching proactive counterattacks against foreign-based culprits. “Should there be some aspect that is in a way proactive instead of reactive?” she responded, and then answered her own question with “yes.” She added, “it is not something that we haven’t been thinking about,” noting someone else had raised the subject with her earlier Monday. Before analysing this development and the concept in general, it needs to be stated that there seems to be some ambiguity, at least in my mind, about the statement(s) by Napolitano. Napolitano’s use of “proactive” and “counterattack” together, as reported by San Jose Mercury News, seems confusing since “proactive” is a term that is used usually along with the concept of “defense.” In risk management lingo ‘proactive’ denotes the act of taking initiative by acting rather than reacting to threat events, while ‘reactive’ actions respond to past event(s) rather than predicting and acting before these perceived event. Thus “proactive” gels well together with “defense”, which in military literature refers to the art of preventing an attack, to mean the act of defending against an imminent attack by taking action before the act of attack has happened. This flies completely against the concept of counter-attack which is about, duh, countering an attack that has happened, something that automatically classifies the act as being reactive. My guess is that Ms. Napolitano did mean counter-attack but by “proactive” she was trying to emphasis the fact that **the reaction from the US will not be limited to acts of defense but will include counter offensive moves**. Either way, I did end up smiling when I read the double negative that Ms. Napolitano used: “Should there be some aspect that is in a way proactive instead of reactive?” she responded, and then answered her own question with “yes.” She added, “it is not something that we haven’t been thinking about,” (…) Now that my confusion regarding the use of “proactive counterattack” is out in the open, let us get to the main point of discussion – **use of private companies in proactive cyber attacks by nation states**. In traditional military engagement, private military companies have long been used to supplement the operational capability of the nation state’s army. In recent years the role has increasingly moved from support of military personnels in areas like security of the military base, protecting the convoy etc., to a more traditional role played by active military personnels as part of an active war operation. The case of Academi (previously Blackwater) is a prime example of such private military companies. The reasons have been numerous, the cost being the obvious but **not the main one,** which is to avoid scrutiny, including Congressional oversight in the US, that seems to be reserved for the military personnels of the nation-state. A similar reasoning can be used within the cyberspace as well. Private companies engaged in cyber operations, **regardless of its nature** (defensive, offensive, counter-attack, proactive), **can be set up to evade deep scrutiny and congressional oversight**. **This gives them the flexibility to** be a lot more liberal about the means and mechanisms usedwithout having to worry about repercussions. The practice also provides a good means to exploit the attribution problem, which has so far been an issue rather than a way out for the US (pdf). By engaging private civilian companies it becomes harder for the subject of the attacks to concretely state that they were indeed targeted by the US. Even if they did, the fact that the attacks cannot be tracked back to have been originated from the networks of the US military complex gives the US **enough excuses** to assert that **they were not aware of nor authorised such attacks.** Such a setup has been used with good results by the Chinese and the Russians. In the narrower context of counter-attacks, the domain of cyber differs from the rest of the domain of land, sea, air and space in a crucial way in that the conduits/medium that are used for the attacks, the networks consisting of the backbone of routers, cables and other physical and software based systems, are owned by private companies. The four traditional domains differ from cyber domain in that in each of the four cases, the conduit of attack (land, sea, air and space respectively) are usually owned, at least in the extended sense of the word, by the nation states that is attacking or being attacked. This makes it easier for constructing a case for involving private companies since after all they are direct front line causalities in the event of an attack. Another reason is of course the simple practical fact that the talent pool of experts expands drastically if private companies are also considered as part of the “recruitment” space. Cyber is the only domain in the list of five where the private sector holds a big pie of capable, qualified individuals who can provide service in these operations. Public-private partnerships just makes sense. The wholesale hiring of “ethical hackers” by NTRO, as reported by news outlets provides a seemingly similar setup in India with the crucial disadvantage that these “hired helps” are still directly associated with NTRO and hence NTRO can and will be held accountable for their actions, negating some of the crucial advantages of using private companies/individuals. What is needed is a deeper and longer term relationship between the government and private companies that makes defending the infrastructures that they both rely on as the central theme and working on means to do that, be it defensive postures or offensive gestures. There are of course **risks involved**. **Command structure gets blurred when the military structure merges with the private sector** and without one, controlling these private parties becomes a risky process that cannotbe taken for granted. This has been seen **again and again** in cases related to Blackwater. What if an unapproved action from the part of the private contractor is judged as an act of war by the other party and leads to a **confrontational situation?** A similar situation can arise when wrong magnitude of (counter)attack force is applied accidentally or otherwise by these third parties. All these point to fact that use of private companies in cyber operations is tactically a good move and some would argue, a necessity. However it cannot be done at the drop of a hat since the “rules of engagement” is bound to be fickle in such symbiotic associations.

Turns readiness and CMR

Singer ‘5

Peter, Senior Fellow and Director of the Project on U.S. Policy Towards the Islamic World at the Saban Center for Middle East Policy at the Brookings Institution, “Outsourcing War.” Foreign Affairs, Vol. 84, No. 2 (Mar. - Apr., 2005), pp. 119-132

The final dilemma raised by the extensive use of private contractors involves the future of the military itself. The armed services have long seen themselves as engaged in a unique profession, set apart from the rest of civilian society, which they are entrusted with securing. The introduction of PMFS, and their recruiting from within the military itself, challenges that uniqueness; the military's professional identity and monopoly on certain activities is being encroached on by the regular civilian marketplace. Most soldiers thus have a deeply ambivalent attitude toward PMFS. On the one hand, they are grateful to have someone help them bear their burden, which, thanks to military overstretch in Iraq, feels particularly onerous at the moment. Even though the job of the U.S. armed services has grown, the force has shrunk by 35 percent since its Cold War high; the British military, meanwhile, is at its smallest since the Napoleonic wars. PMFS help fill the gap as well as offer retired soldiers the potential for a second career in a field they know and love. Some in the military worry, on the other hand, that the PMF boom could endanger the health of their profession and resent the way these firms exploit skills learned at public expense for private profit. They also fear that the expanding PMF marketplace **will hurt the military's ability to retain talented soldiers**. Contractors in the PMF industry can make anywhere from two to ten times what they make in the regular military; in Iraq, former special forces troops can earn as much as $i,ooo a day. Certain service members, such as pilots, have always had the option of seeking work in the civilian marketplace. But the PMF industry marks a significant change, since it keeps its employees within the military, and thus the public, sphere. More important, PMFS compete directly with the government. Not only do they draw their employees from the military, they do so to play military roles, thus shrinking the military's purview. PMFS use public funds to offer soldiers higher pay, and **then charge the government at an even higher rate,** all for services provided by the human capital that the military itself originally helped build. The overall process may be brilliant from a business standpoint, but it is **self-defeating from the military's perspective.**

This issue has become **especially pointed** **for special forces** units, which have the most skills and are thus the most marketable. **Elite force commanders** in Australia, New Zealand, the United King dom, and the United States have all expressed deep concern over the poaching of their numbers by PMFS. One U.S. special forces officer described the issue of retention among his most experienced troops as being "at a tipping point." So far, the U.S. government has failed to respond adequately to this challenge. Some militaries now allow their soldiers to take a year's leave of absence, in the hope that they will make their money quickly and then return, rather than be lost to the service forever. But Washington has failed to take even this step; it has only created a special working group to explore the issue.

## link

The plan causes a PMC shift—the executive uses them to continue operations after Congress issues regulations—that’s Kruck

Best studies prove the link

Kruck ‘14

Andreas, Geschwister Scholl Institute for Political Science, University of Munich, “Theorising the use of private military and security companies: a synthetic perspective,” Journal of International Relations and Development, 2014, 17, (112–141)

The political-instrumentalist model is supported by **numerous studies** that find indications that the use of PMSCs is indeed harmful for the transparency, accountability and parliamentary control of military operations and that governments are at the very least aware of this (Avant 2005; Deitelhoff 2010; Dunigan 2011: 100). The use of PMSCs allowed the US government to **circumvent troop ceilings ordered** **by** the US **Congress** in the Balkans conflict and again in its Plan Colombia (Deitelhoff and Geis 2010). The governmentdominated practices in the negotiation and oversight of PMSCs’ contracts in Iraq have also demonstrated that outsourcing makes **parliamentary oversight** over the defence budget and, ultimately, the use of force more difficult (Deitelhoff 2010). As Avant and Sigelman (2010) have empirically shown, parliamentary organs and the broader public have less information on PMSCs than on public armed forces, and access to this information is more difficult. Although the broader public may be just as sensitive to the deaths of private forces as it is to the military personnel’s deaths, it is simply less likely to know about them (ibid.: 230). PMSC casualties are not listed in official casualty statistics. Thus, public debates about more than 1,000 PSMC casualties in Iraq **have** largely **been absent**. Governments’ reluctance to increase monitoring and clarify liabilities of PMSCs via stricter regulation also correspond nicely to the political-instrumentalist model’s main arguments (Deitelhoff 2010: 198).

## \*\*\*cp

## overview

There’s no possible solvency deficit.

Graham Dodds, Ph.D., Concordia professor of political science, 2013, Take Up Your Pen: Unilateral Presidential Directives in American Politics, p. 243-4

As for the legislature, Congress has at times protested unilateral presidential directives, but **it has not done so consistently or successfully**. 58 Congress could speak out against a particular unilateral presidential directive, it could use its power of the purse to block the implementation of a directive, it could reverse or nullify a directive, and it could even pass legislation to curtail executive unilateralism more generally. Additionally, Congress could pass legislation to clarify the many different types of presidential documents and require their regular publication, thereby possibly preventing executive obfuscation by using memoranda and other directives in lieu of executive orders and proclamations. A Senate report of 1974 noted that “the fundamental ambiguity and arbitrariness in the use of Executive orders remains one of the most troubling problems of public administration yet to be resolved by Congress.” 59 In terms of the practice of presidents using different unilateral tools instead of executive orders, the report stated that “remedial legislation to correct this recent practice of public administration should be a priority for Congress.” 60 Nearly four decades later, Congress has yet to act on this priority. And **it does not appear that Congress will stand up to the president** anytime soon. 61 Consider the following account by the renowned author Joan Didion of a congressional hearing during George W. Bush's first term: when a former longtime member of the House of Representatives, Lee Hamilton, suggested at a hearing of the Senate Governmental Affairs Committee that recommendations of the 9/ 11 Commission could be put in effect by “executive order,” [there was] not only no polarization but virtually no response, no discussion of why someone who had long resisted the expansion of executive power now seemed willing to suggest that a major restructuring of the government proceed on the basis of the president's signature alone. “And usually, given my background, you'd expect me to say it's better to have a statute in back of it,” he said. Was he suggesting a way to shortcut the process on only minor points? Or, since he seemed to be talking about major changes, was he simply trying to guide the Senate to the urgency of the matter? Such questions did not enter the discourse. There was only silence, general acquiescence, as if any lingering memory of a separation of powers had been obliterated. 62 This clearly demonstrates the fact that Congress is simply not interested in reining in unilateral executive policymaking. The more recent examples of Congress's reactions to George W. Bush's controversial directives for detainment and domestic spying underscore the point, as **Congress** initially expressed outrage, then **became silent, and eventually** passed legislation essentially to endorse the president's action. As Senator Sheldon Whitehouse (D-RI) said in late 2007 regarding Bush's order for domestic spying, “When the Congress of the United States is willing to roll over for an unprincipled President, this is where you end up.” 63

# 1nr

## 2nc impact

Solves every threat – specifically nuke terror

Royal ‘11

John-Paul, Institute of World Politics, Class of 2011 Valedictorian, “War Powers and the Age of Terrorism,” <http://www.thepresidency.org/storage/Fellows2011/Royal-_Final_Paper.pdf>

The international system itself and national security challenges to the United States in particular, underwent rapid and significant change in the first decade of the twenty-first century. War can no longer be thought about strictly in the terms of the system and tradition created by the Treaty of Westphalia over three and a half centuries ago. Non-state actors now possess a level of destructiveness formerly enjoyed only by nation states. Global terrorism, coupled with the threat of weapons of mass destruction developed organically or obtained from rogue regimes, presents new challenges to U.S. national security and place innovative demands on the Constitution’s system of making war. In the past, as summarized in the 9/11 Commission Report, threats emerged due to hostile actions taken by enemy states and their ability to muster large enough forces to wage war: “Threats emerged slowly, often visibly, as weapons were forged, armies conscripted, and units trained and moved into place. Because large states were more powerful, they also had more to lose. They could be deterred" (National Commission 2004, 362). This mindset assumed that peace was the default state for American national security. Today however, we know that threats can emerge quickly. Terrorist organizations half-way around the world are able to wield weapons of unparalleled destructive power. These attacks are more **difficult to detect** and deter due to their unconventional and asymmetrical nature. In light of these new asymmetric threats and the resultant changes to the international system, peace can no longer be considered the default state of American national security. Many have argued that the Constitution permits the president to use unilateral action only in response to an imminent direct attack on the United States. In the emerging security environment described above, pre-emptive action taken by the executive branch may be needed more often than when nation-states were the principal threat to American national interests. Here again, the 9/11 Commission Report is instructive as it considers the possibility of pre-emptive force utilized over large geographic areas due to the diffuse nature of terrorist networks: In this sense, 9/11 has taught us that terrorism against American interests “over there” should be regarded just as we regard terrorism against America “over here.” In this sense, the American homeland is the planet (National Commission 2004, 362). Furthermore, the report explicitly describes the global nature of the threat and the global mission that must take place to address it. Its first strategic policy recommendation against terrorism states that the: U.S. government must identify and prioritize actual or potential terrorist sanctuaries. For each, it should have a realistic strategy to keep possible terrorists insecure and on the run, using all elements of national power (National Commission 2004, 367). Thus, fighting continues against terrorists in Afghanistan, Yemen, Iraq, Pakistan, the Philippines, and beyond, as we approach the tenth anniversary of the September 11, 2001 attacks. Proliferation of weapons of mass destruction (WMD), especially nuclear weapons, into the hands of these terrorists is the most dangerous threat to the United States. We know from the 9/11 Commission Report that Al Qaeda has attempted to make and obtain nuclear weapons for at least the past fifteen years. Al Qaeda considers the acquisition of weapons of mass destruction to be a religious obligation while “more than two dozen other terrorist groups are pursing CBRN [chemical, biological, radiological, and nuclear] materials” (National Commission 2004, 397). Considering these statements, rogue regimes that are openly hostile to the United States and have or seek to develop nuclear weapons capability such as North Korea and Iran, or extremely unstable nuclear countries such as Pakistan, pose a special threat to American national security interests. These nations were not necessarily a direct threat to the United States in the past. Now, however, due to proliferation of nuclear weapons and missile technology, they can inflict damage at considerably higher levels and magnitudes than in the past. In addition, these regimes may pursue proliferation of nuclear weapons and missile technology to other nations and to allied terrorist organizations. The United States must pursue condign punishment and appropriate, rapid action against hostile terrorist organizations, rogue nation states, and nuclear weapons proliferation threats in order to protect American interests both at home and abroad. Combating these threats are the “top national security priority for the United States…with the full support of Congress, both major political parties, the media, and the American people” (National Commission 2004, 361). Operations may take the form of pre-emptive and sustained action against those who have expressed hostility or declared war on the United States. Only the executive branch can effectively execute this mission, authorized by the 2001 AUMF. If the national consensus or the nature of the threat changes, Congress possesses the intrinsic power to rescind and limit these powers.

Extinction

Hellman 8 (Martin E. Hellman, emeritus prof of engineering @ Stanford, “Risk Analysis of Nuclear Deterrence” SPRING 2008 THE BENT OF TAU BETA PI, <http://www.nuclearrisk.org/paper.pdf>)

The threat of nuclear terrorism looms much larger in the public’s mind than the threat of a full-scale nuclear war, yet this article focuses primarily on the latter. An explanation is therefore in order before proceeding. A terrorist attack involving a nuclear weapon would be a catastrophe of immense proportions: “A 10-kiloton bomb detonated at Grand Central Station on a typical work day would likely kill some half a million people, and inflict over a trillion dollars in direct economic damage. America and its way of life would be changed forever.” [Bunn 2003, pages viii-ix]. The likelihood of such an attack is also significant. Former Secretary of Defense William Perry has estimated the chance of a nuclear terrorist incident within the next decade to be roughly 50 percent [Bunn 2007, page 15]. David Albright, a former weapons inspector in Iraq, estimates those odds at less than one percent, but notes, “We would never accept a situation where the chance of a major nuclear accident like Chernobyl would be anywhere near 1% .... A nuclear terrorism attack is a low-probability event, but we can’t live in a world where it’s anything but extremely low-probability.” [Hegland 2005]. In a survey of 85 national security experts, Senator Richard Lugar found a median estimate of 20 percent for the “probability of an attack involving a nuclear explosion occurring somewhere in the world in the next 10 years,” with 79 percent of the respondents believing “it more likely to be carried out by terrorists” than by a government [Lugar 2005, pp. 14-15]. I support increased efforts to reduce the threat of nuclear terrorism, but that is not inconsistent with the approach of this article. Because terrorism is one of the potential trigger mechanisms for a full-scale nuclear war, the risk analyses proposed herein will include estimating the risk of nuclear terrorism as one component of the overall risk. If that risk, the overall risk, or both are found to be unacceptable, then the proposed remedies would be directed to reduce which- ever risk(s) warrant attention. Similar remarks apply to a number of other threats (e.g., nuclear war between the U.S. and China over Taiwan). his article would be incomplete if it only dealt with the threat of nuclear terrorism and neglected the threat of full- scale nuclear war. If both risks are unacceptable, an effort to reduce only the terrorist component would leave humanity in great peril. In fact, society’s almost total neglect of the threat of full-scale nuclear war makes studying that risk all the more important. The cosT of World War iii The danger associated with nuclear deterrence depends on both the cost of a failure and the failure rate.3 This section explores the cost of a failure of nuclear deterrence, and the next section is concerned with the failure rate. While other definitions are possible, this article defines a failure of deterrence to mean a full-scale exchange of all nuclear weapons available to the U.S. and Russia, an event that will be termed World War III. Approximately 20 million people died as a result of the first World War. World War II’s fatalities were double or triple that number—chaos prevented a more precise deter- mination. In both cases humanity recovered, and the world today bears few scars that attest to the horror of those two wars. Many people therefore implicitly believe that a third World War would be horrible but survivable, an extrapola- tion of the effects of the first two global wars. In that view, World War III, while horrible, is something that humanity may just have to face and from which it will then have to recover. In contrast, some of those most qualified to assess the situation hold a very different view. In a 1961 speech to a joint session of the Philippine Con- gress, General Douglas MacArthur, stated, “Global war has become a Frankenstein to destroy both sides. … If you lose, you are annihilated. If you win, you stand only to lose. No longer does it possess even the chance of the winner of a duel. It contains now only the germs of double suicide.” Former Secretary of Defense Robert McNamara ex- pressed a similar view: “If deterrence fails and conflict develops, the present U.S. and NATO strategy carries with it a high risk that Western civilization will be destroyed” [McNamara 1986, page 6]. More recently, George Shultz, William Perry, Henry Kissinger, and Sam Nunn4 echoed those concerns when they quoted President Reagan’s belief that nuclear weapons were “totally irrational, totally inhu- mane, good for nothing but killing, possibly destructive of life on earth and civilization.” [Shultz 2007] Official studies, while couched in less emotional terms, still convey the horrendous toll that World War III would exact: “The resulting deaths would be far beyond any precedent. Executive branch calculations show a range of U.S. deaths from 35 to 77 percent (i.e., 79-160 million dead) … a change in targeting could kill somewhere between 20 million and 30 million additional people on each side .... These calculations reflect only deaths during the first 30 days. Additional millions would be injured, and many would eventually die from lack of adequate medical care … millions of people might starve or freeze during the follow- ing winter, but it is not possible to estimate how many. … further millions … might eventually die of latent radiation effects.” [OTA 1979, page 8] This OTA report also noted the possibility of serious ecological damage [OTA 1979, page 9], a concern that as- sumed a new potentiality when the TTAPS report [TTAPS 1983] proposed that the ash and dust from so many nearly simultaneous nuclear explosions and their resultant fire- storms could usher in a nuclear winter that might erase homo sapiens from the face of the earth, much as many scientists now believe the K-T Extinction that wiped out the dinosaurs resulted from an impact winter caused by ash and dust from a large asteroid or comet striking Earth. The TTAPS report produced a heated debate, and there is still no scientific consensus on whether a nuclear winter would follow a full-scale nuclear war. Recent work [Robock 2007, Toon 2007] suggests that even a limited nuclear exchange or one between newer nuclear-weapon states, such as India and Pakistan, could have devastating long-lasting climatic consequences due to the large volumes of smoke that would be generated by fires in modern megacities. While it is uncertain how destructive World War III would be, prudence dictates that we apply the same engi- neering conservatism that saved the Golden Gate Bridge from collapsing on its 50th anniversary and assume that preventing World War III is a necessity—not an option.

## 2nc turns case—circumvention

Lack of crisis containment turns the case – makes cyber lashout more likely

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.

.

## Bio T

Executive primacy prevents 4th gen warfare

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.

## 2nc war power spillover

Plan empowers Congress --- undermines all war powers

Heder ’10

(Adam, J.D., magna cum laude , J. Reuben Clark Law School, Brigham Young University, “THE POWER TO END WAR: THE EXTENT AND LIMITS OF CONGRESSIONAL POWER,” St. Mary’s Law Journal Vol. 41 No. 3, <http://www.stmaryslawjournal.org/pdfs/Hederreadytogo.pdf>)

This constitutional silence invokes Justice Rehnquist’s oftquoted language from the landmark “political question” case, Goldwater v. Carter . 121 In Goldwater , a group of senators challenged President Carter’s termination, without Senate approval, of the United States ’ Mutual Defense Treaty with Taiwan. 122 A plurality of the Court held, 123 in an opinion authored by Justice Rehnquist, that this was a nonjusticiable political question. 124 He wrote: “In light of the absence of any constitutional provision governing the termination of a treaty, . . . the instant case in my view also ‘must surely be controlled by political standards.’” 125 Notably, Justice Rehnquist relied on the fact that there was no constitutional provision on point. Likewise, there is **no constitutional provision** on whether Congress has the legislative power to **limit, end, or otherwise redefine the scope of a war**. Though Justice Powell argues in Goldwater that the Treaty Clause and Article VI of the Constitution “add support to the view that the text of the Constitution does not unquestionably commit the power to terminate treaties to the President alone,” 126 **the same cannot be said about Congress’s legislative authority** to terminate or limit a war in a way that goes beyond its explicitly enumerated powers. There are no such similar provisions that would suggest Congress may decline to exercise its appropriation power but nonetheless legally order the President to cease all military operations. Thus, the case for deference to the political branches on this issue is even greater than it was in the Goldwater context. Finally, the Constitution does not imply any additional powers for Congress to end, limit, or redefine a war. The textual and historical evidence suggests the Framers purposefully **declined to grant Congress such powers**. And as this Article argues, granting Congress this power would be **inconsistent with the general war powers structure of the Constitution.** Such a reading of the Constitution would **unnecessarily empower Congress** and **tilt the scales heavily in its favor**. More over, it would strip the President of his Commander in Chief authority to direct the movement of troops at a time **when the Executive’s expertise is needed.** 127 And fears that the President will grow too powerful are unfounded, given the reasons noted above. 128 In short, the Constitution does not impliedly afford Congress any authority to prematurely terminate a war above what it explicitly grants. 129 Declaring these issues nonjusticiable political questions would be the most practical means of balancing the textual and historical demands, the structural demands, and the practical demands that complex modern warfare brings . Adjudicating these matters would only lead the courts to engage in impermissible line drawing — lines that would both confus e the issue and add layers to the text of the Constitution in an area where the Framers themselves declined to give such guidance.

Causes future encroachment – corrodes presidential power

Colella 88 (Frank, JD – Brooklyn Law, “BEYOND INSTITUTIONAL COMPETENCE: CONGRESSIONAL EFFORTS TO LEGISLATE UNITED STATES FOREIGN POLICY TOWARD NICARAGUA -- THE BOLAND AMENDMENTS.” SPRING, 1988, 54 Brooklyn L. Rev. 131)

Traditionally, the president has exercised greater control over foreign policy-making than has Congress. n28 Since the earliest days of the Republic, that office has been responsible for communicating with other governments on behalf of the United States. n29 Continuous contacts with other nations generated innumerable issues for resolution. n30 As a result of the President's continuous participation in the daily matters affecting foreign affairs, his position as chief spokesperson was established.

The role did not emerge from any constitutionally inherent superiority he possessed, **but rather from the practical necessity of having to make decisions.** **Decisions on day-to-day matters were often made "on the spot" by the executive branch personnel.** n31 When larger issues were involved, the president articulated the United States position, again, for practical reasons. He was always in session and Congress was not. Congress could only be specially convened with difficulty. n32 Moreover, the **president's access to the facts**, and the advice of subordinates, **permitted quick action** if required by the circumstances. n33

In addition, Congress may be said to have permitted the expansion of executive authority without challenge. "[Congress] did not equip itself with expertise, so as to acquire a dominant authority in foreign relations, or even a continuous, informed participation." n34 It might even be said that Congress facilitated [\*140] the expansion of presidential power over foreign affairs by providing him large "grants of power with only general lines of guidance." n35 In effect, the executive branch obtained a large degree of discretion to formulate and implement policy. n36

The expansion of presidential authority over foreign policy-making continued well into the twentieth century, with the period between 1940 and 1970, principally because of the Second World War and its aftermath, seeing the greatest rise in the president's authority over foreign affairs. n37 The exigencies of participating in that War, and the United States' position immediately following it, permitted this expansion. n38

Later, however, this country's growing dissatisfaction with its involvement in Vietnam, and a president weakened by the Watergate affair, set the stage for a dramatic confrontation between Congress and the executive over which branch would control the direction of foreign policy-making. n39 Some have termed this confrontation over the means necessary to achieve a policy goal a revolution -- with Congress entitled to claim victory. n40

Congress denied the president statutory authorization and the necessary funding to maintain United States support for the South Vietnamese. n41 Unfortunately, the legislation hastened the [\*141] overthrow of the South Vietnamese government "[b]y using the public legislative process to prohibit the president from using force, the legislators signaled Hanoi that the South could now be plucked with impunity." n42

These prohibitions on the use of force also confronted President Ford during the 1975 fall of Saigon. n43 As North Vietnamese troops overran Saigon, President Ford faced the choice of either "breaking the law" by airlifting the United States soldiers and pro-American Vietnamese out of Vietnam, or following the law thereby permitting them to be captured or killed. n44 President Ford did authorize the airlift. n45 Yet even as the airlift proceeded, Congress debated for two weeks the passage of a resolution that would have authorized this action. n46 This legislation was originally proposed to prevent President Nixon from continuing the war, however, as enacted it also applied to President Ford and the airlift, a situation Congress did not, and could not have [\*142] foreseen. n47

Congressional efforts to **limit the scope** of executive foreign policy-making via legislation have carried over into the 1980's. Along with it, the tension between the executive and legislative branches has been exacerbated. While the executive seeks broader discretion, the legislature seeks to foreclose discretion by statutory command. This conflict can degenerate into a foreign policy driven by questions of statutory interpretation. n48 **The need for flexibility and discretion is axiomatic in foreign policy-making.** n49 Therefore, legislative commands tend to receive narrow interpretation. n50 **However, this** narrowing **process is** corrosive **"because it leads inexorably to** more legislation**, more efforts to interpret it away, and so on in an inextricable,** self-generating circle**."** n51 As long as **the circle continues to generate more legislation and narrow constructions**, executive/legislative tensions will exist and continue to thwart a meaningful cooperation between the branches. Unfortunately, this is precisely what resulted from the numerous enactments **seeking to** micromanage the president's policy toward Nicaragua and Central America.

Congressional restriction is key --- sets a precedent

Caldwell 13 (Leigh, CNN correspondent, “Is Obama setting bad precedent for future presidents?” September 4, 2013, CNN; Politics)

President Barack Obama's abrupt change of course and decision to ask Congress to authorize a strike on Syria won praise from some who have bitterly opposed his foreign policy. But in his surprise decision, did Obama cede presidential power?

Over the last 50 years, presidents have successfully consolidated power when it comes to foreign affairs, especially when use of the U.S. military is concerned. Some say the concession to Congress sets a new precedent **that bodes well for future Congresses and not so well for future presidents.**

"**This** is a big deal and **will tie the hands of future presidents**," said Peter Spiro, law professor at Temple University.

Spiro said this is the first time a president has sought authorization from Congress for a limited military mission. He said it will limit the flexibility of future presidents to make quick decisions, potentially putting U.S. national security at risk.

Draft resolution on Syria would limit strike to 60 days

"That kind of decision-making doesn't work when you have 535 Monday morning quarterbacks," Spiro said, referring to the number of lawmakers who will have a vote on Syria intervention as early as next week.

Obama maintains, however, that he is not ceding his authority, but made the decision because "the country will be stronger" if Congress is on board. **Obama** insists he **still has the authority to act unilaterally**. "[I] believe I have the authority to carry out this military action **without specific congressional authorization**," he said Saturday when he announced he would seek Congress' support.

Obama and unilateralism

Other legal analysts disagree, however, with Spiro's assessment that the president is diluting the power of the office.

On the legal blog Lawfare, Harvard Law professor Jack Goldsmith wrote: "What would have been unprecedented, and a huge development for separation of powers, is a unilateral strike in Syria."

Oona Hathaway, a Yale Law School professor, agreed. She argued that the president had to seek Congress' approval because he didn't have support from the United Nations Security Council.

Obama looks to Congress to bolster legal case for Syria strike

"Going to war under these circumstances (without congressional or Security Council support) would have put him out on a limb politically and legally," Hathaway said.

Ari Fleischer, who was press secretary for President George W. Bush, sided with Obama. He said on CNN's "New Day" that this is "a voluntary exercise where the executive has said to the legislature, 'I want you to act.' "

A return to precedent?

Presidential historian Robert Dallek said the president "returned to a central part of the country's history" of power-sharing that has "a complicated history."

He said Presidents Woodrow Wilson and Franklin Delano Roosevelt would never have considered sidestepping Congress in the lead-up to World War I or World War II respectively.

Presidents moved away from asking Congress' permission in the 1950s, starting with the Korean War, when President Harry Truman declined to seek congressional authorization. Library of Congress historian Louis Fisher called the move "the single most important precedent for the executive use of military force without Congressional authority." Instead, Truman gained support from the U.N. Security Council and Congress did not object.

President John F. Kennedy further consolidated power by authorizing the CIA to carry out the Bay of Pigs invasion of Cuba and by his actions in the 1962 standoff with the Soviet Union over the U.S. blockade of Cuba. President Lyndon B. Johnson boxed out Congress with the 1964 Gulf of Tonkin Resolution, which gave Johnson broad authority without forcing him to declare war. He used the law to unilaterally decide to commit 100,000 troops in the first stage of the war against North Vietnam.

As a result, Congress passed the War Powers Resolution of 1973 to rein in presidents' war declarations. The law says the president must "consult" with Congress before U.S. forces are committed in an overseas conflict or within 60 days of U.S. involvement.

Congress' use of the War Powers Act is mixed, however. While President George W. Bush sought congressional approval for wars in Iraq and Afghanistan, presidents have often failed to ask Congress for support for smaller incursions. President Ronald Reagan didn't seek authorization for Grenada and Panama, President Bill Clinton avoided Congress over military action in Haiti and Kosovo, and Obama sidestepped the legislative branch for an expanded war in Afghanistan and intervention in Libya.

What if Congress turns down the president?

**The** most immediate **risk for the president is that the** Congress says no, as Great Britain's Parliament did to Prime Minister David Cameron last week. Fleischer warned that Obama "has to prevail on the vote."

Dallek said it would be "rare" that Congress would not defer to the president on an issue of war. He pointed to one instance in 1939, in the lead-up to World War II, when the president failed to gain Congress' support to aid the British and French against Nazi Germany. Shortly after, Congress reversed course and gave Roosevelt the resources he wanted.

Syria war resolution faces tough challenge in Congress

While Obama's decision will be debated for years, Congress' response could be the real precedent-setter.

During testimony before the Senate Foreign Relations Committee on Tuesday, Secretary of State John Kerry said congressional rejection **would harm U.S. standing among its allies while emboldening its enemies.**

As of now, Congress isn't completely sold on intervention in Syria. If a failed vote falls along party lines, Hathaway said "partisan squabbling would make future presidents nervous" about seeking congressional authority.

Dallek quoted Dutch historian Pieter Geyl, who said, "History is an argument without end." In other words, **future Congresses and presidents** (**and observers**) **are likely to use** Obama's action and **Congress' response as evidence bolstering a position.**

## 2nc OCO link

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.

## \*Preempt

Nuclear system aren’t vulnerable

Slocombe 9

Walt Slocombe, Former Under Secretary of Defense for Policy, June 2009, De-Alerting: Diagnoses, Prescriptions, and Side-Effects, http://www.ewi.info/system/files/Slocombe.pdf

Whatever other problems the current nuclear posture of the US nuclear force may present, it cannot reasonably be said to be on a “hair trigger.” Since the 1960s the US has taken a series of measures to insure that US nuclear weapons cannot be detonated without the receipt of both external information and properly authenticated authorization to use that information. These devices – generically Permissive Action Links or “PALs” – are in effect combination locks that keep the weapons locked and incapable of detonation unless and until the weapons’ firing mechanisms have been unlocked following receipt of a series of numbers communicated to the operators from higher authority. Equally important in the context of a military organization, launch of nuclear weapons (including insertion of the combinations) is permitted only where properly authorized by an authenticated order. This combination of reliance on discipline and procedure and on receipt of an unlocking code not held by the military personnel in charge of the launch operation is designed to insure that the system **is** “fail safe,” i.e., that **whatever mistakes occur, the** result will not be a nuclear explosion. Moreover, in recent years, both the US and Russia, as well as Britain and China, have modified their procedures so that even if a nuclear-armed missile were launched, it would go not to a “real” target in another country but – at least in the US case - to empty ocean. In addition to the basic advantage of insuring against a nuclear detonation in a populated area, the fact that a missile launched in error would be on flight path that diverged from a plausible attacking trajectory should be detectable by either the US or the Russian warning systems, reducing the possibility of the accident being perceived as a deliberate attack. De-targeting, therefore, provides a significant protection against technical error.5

Russia and China can’t cyberattack the US – they only use it to crack down on their own populations

**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)

"The West Is Falling Behind Russia and China." Yes, but not how you think. Russia and China are busy sharpening their cyberweapons and are already well steeped in using them. The Russian military clandestinely crippled Estonia's economy in 2007 and Georgia's government and banks in 2008. The People's Liberation Army's numerous Chinese cyberwarriors have long inserted "logic bombs" and "trapdoors" into America's critical infrastructure, lying dormant and ready to wreak havoc on the country's grid and bourse in case of a crisis. Both countries have access to technology, cash, and talent -- and have more room for malicious maneuvers than law-abiding Western democracies poised to fight cyberwar with one hand tied behind their backs. Or so the alarmists tell us. Reality looks quite different. Stuxnet, by far the most sophisticated cyberattack on record, was most likely a U.S.-Israeli operation. Yes, Russia and China have demonstrated significant skills in cyberespionage, but the fierceness of Eastern cyberwarriors and their coded weaponry is almost certainly overrated. When it comes to military-grade offensive attacks, America and Israel seem to be well ahead of the curve. Ironically, it's a different kind of cybersecurity that Russia and China may be more worried about. Why is it that those countries, along with such beacons of liberal democracy as Uzbekistan, have suggested that the United Nations establish an "international code of conduct" for cybersecurity? Cyberespionage was elegantly ignored in the suggested wording for the convention, as virtual break-ins at the Pentagon and Google remain a favorite official and corporate pastime of both countries. But what Western democracies see as constitutionally protected free speech in cyberspace, Moscow and Beijing regard as a new threat to their ability to control their citizens. Cybersecurity has a broader meaning in non-democracies: For them, the worst-case scenario is not collapsing power plants, but collapsing political power.b The social media-fueled Arab Spring has provided dictators with a case study in the need to patrol cyberspace not only for subversive code, but also for subversive ideas. The fall of Egypt's Hosni Mubarak and Libya's Muammar al-Qaddafi surely sent shivers down the spines of officials in Russia and China. No wonder the two countries asked for a code of conduct that helps combat activities that use communications technologies -- "including networks" (read: social networks) -- to undermine "political, economic and social stability." So Russia and China are ahead of the United States, but mostly in defining cybersecurity as the fight against subversive behavior. This is the true cyberwar they are fighting.

China's program is too weak

Lu 13

Dr. Lu Jinghua is a Research Fellow for the Center on China-America Defense Relations at the PLA Academy of Military Science, China US Focus, June 7, 2013, "China’s Cyber Threat: Real or Imaginary?", http://www.chinausfocus.com/peace-security/chinas-cyber-threat-real-or-imaginary/

It is the first time for the United States to directly condemn the Chinese government and military for cyber activities in an official document. However, not all these accusations are new. We can find similar arguments in previous reports and some newest reports such as the IP Commission Report. They have reflected the US concerns that its military superiority, economic prosperity and diplomatic influence would be undermined because of China’s cyber activities. Undoubtedly, China has enhanced its cyber capabilities. But would these advancements really be threatening America’s national interests?

According to some American scholars, the development of Chinese strategy in the domain of cyber warfare can be traced to the early 1990s. Pursuit of information dominance is given highest priority in the PLA not only because cyberspace is an emerging and critical domain for military competition, but also because cyber warfare strategy is in accordance with Sun Tzu's notion of “subduing the enemy without fighting.” That is, China enjoys “unique cultural advantages” in developing and using cyber capabilities. However, after two decades of development, the PLA is still aiming to “attain major progress in informationzation” while “bearing in mind the primary goal of accomplishing mechanization.” It is obvious that the PLA is still in the early process of informationization. In contrast with China, the US has a military with most IT applications and is the first one to establish a Cyber Command. Also, America is widely recognized as the main researcher, developer and user of Stuxnet, which is the only well-known computer network malware to cause significant damages to physical infrastructure. Through an in-depth analysis of this case, we can draw the conclusion that cyberspace is not an asymmetric domain for weaker actors to achieve unexpected advantages. Rather, it can only widen current gaps between strong countries and weak ones. In this sense, is it necessary for the strongest military power to feel afraid of a weak one?

Retaliation would be controlled

NBC 11

NBC News, May 31, 2011, "Sources: US decides cyber attack can be 'act of war'", http://www.nbcnews.com/id/43224451/ns/us\_news-security/t/sources-us-decides-cyber-attack-can-be-act-war/#.UiS6OJLVCSo

In its first formal cyber strategy, the Pentagon has concluded that computer sabotage by another country could constitute an act of war, administration and military sources told NBC News on Tuesday, confirming a report in the Wall Street Journal.

The officials emphasize, however, that not every attack would lead to retaliation. Such a cyber attack would have to be so serious it would threaten American lives, commerce, infrastructure or worse, and there would have to be indisputable evidence leading to the nation state involved, NBC Pentagon correspondent Jim Miklaszewski said.

Unclassified parts of the 30-page strategy are expected to become public in June, the Wall Street Journal reported, attributing the disclosure to three defense sources who had read the report.

A military source described the strategy to the Journal this way: "If you shut down our power grid, maybe we will put a missile down one of your smokestacks."

Pentagon officials and others in Washington are still debating what would constitute an act of war, the Journal stated, though one idea gaining traction is that of "equivalence" — military retaliation would be triggered by a cyber attack that causes the kind of death, damage or high-level disruption that a traditional military attack would cause.

Reject their ev - it's exaggerated and financially biased

Rid 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, PhD in political science from Humboldt University of Berlin, OC Register, March 15, 2013, "Thomas Rid: Hype, fear-mongering hurts cyberwar", http://www.ocregister.com/articles/systems-499977-cyber-control.html

LONDON – The White House likes a bit of threat. In his State of the Union address, Barack Obama wanted to nudge Congress yet again into passing meaningful legislation. The president emphasized that America's enemies are "seeking the ability to sabotage our power grid, our financial institutions and our air traffic control systems." After two failed attempts to pass a cybersecurity act in the past two years, he added swiftly: "We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."

Fair enough. A bit of threat to prompt needed action is one thing. Fear-mongering is something else: counterproductive. Yet too many a participant in the cybersecurity debate reckon that puffery pays off.

The Pentagon, no doubt, is the master of razzmatazz. Leon Panetta set the tone by warning again and again of an impending "cyber Pearl Harbor." Just before he left the Pentagon, the Defense Science Board delivered a remarkable report, "Resilient Military Systems and the Advanced Cyber Threat." The paper seemed obsessed with making yet more drastic historical comparisons: "The cyber threat is serious," the task force wrote, "with potential consequences similar to the nuclear threat of the Cold War." The manifestations of an all-out nuclear war would be different from cyberattack, the Pentagon scientists helpfully acknowledged. But then they added, gravely, that "in the end, the existential impact on the United States is the same."A reminder is in order: The world has yet to witness a single casualty, let alone fatality, as a result of a computer attack. Such statements are a plain insult to survivors of Hiroshima. After all, a bit of fear helps to claim – or keep – scarce resources when austerity and cutting seems out-of-control. The report recommended allocating the stout sum of $2.5 billion for its top two priorities alone, protecting nuclear weapons against cyberattacks and determining the mix of weapons necessary to punish all-out cyber-aggressors.

Then there are private computer security companies. Such firms, naturally, are keen to pocket some of the government's money earmarked for cybersecurity. And hype is the means to that end. Which leads to the next point: The media want to sell copy through threat inflation. "In Cyberspace, New Cold War," the headline writers at the Times intoned in late February. "The U.S. is not ready for a cyberwar," shrieked the Washington Post earlier this week. Instead of calling out the above-mentioned Pentagon report, the paper actually published two supportive articles on it and pointed out that a major offensive cyber capability now seemed essential "in a world awash in cyber-espionage, theft and disruption."

The Post should have reminded its readers that the only military-style cyberattack that has actually created physical damage – Stuxnet – was actually executed by the United States government.

Finally, the intelligence community tags along with the hype because the NSA and CIA are still traumatized by missing 9/11. Missing a "cyber 9/11" would be truly catastrophic for America's spies, so erring on the side of caution seems the rational choice.

This means that the quality of the public debate suffers, as experts as well as journalists have no choice but to rely on industry reports of sometimes questionable quality or anonymous informants whose veracity is hard to assess.