## cyber adv

Advantage one is cyber

Cyber rules exist now but are classified --- secrecy and legal uncertainty ensures cyber escalation

Segal et al 13 (Adam Segal – Project Director of CFR Task Force and Maurice R. Greenberg Senior Fellow for China Studies, and CFR Independent Task Force, “Defending an Open, Global, Secure, and Resilient Internet” Independent Task Force Report No. 70, June 2013, Council on Foreign Relations Press)

Adopt a Greater Degree of Transparency

Although public officials have warned about the threat of a “cyber Pearl Harbor” or “digital 9/11,” the Task Force sees widespread cyber economic, political, and military espionage against defense, government, and privatesector networks as the most immediate threat to economic and national security interests. The capacity to launch a sudden strike that destroys or disrupts a large swath of critical infrastructure is most likely limited to a few nation-states. These actors should be deterred by the expectation that the United States could respond to a cyberattack through a combination of retaliatory cyber and kinetic attacks, as well as diplomatic and other measures.46

The U.S. government is more likely to be able to attribute a devastating attack to a specific state actor, especially if it comes during a geopolitical crisis, but the genesis of attacks at a lower threshold may remain unknown and will continue. These low-intensity attacks can have a long-term corrosive effect on the trust and integrity of the networks that are the foundation of the banking, transport, and communications systems. Furthermore, over time, the capability to conduct more damaging attacks will spread to states that may be harder to deter, as well as to extremists, lone wolves, criminal entities, and other nonstate actors.

It is widely assumed that offense has—and will continue to have in the foreseeable future—the advantage over defense in cyberspace. Improved defense and greater resiliency are necessary but not sufficient. The defense has to secure tens of millions of lines of code and billions of items of data across hundreds of networks and thousands of devices, which are often maintained by private actors and individuals. As a result, offensive capabilities are required to deter attacks, and, if deterrence fails, to impose costs on the attackers.

This offensive dominance, along with the problem of attribution and low barriers to entry, make cyberspace a highly unstable strategic environment. Given the speed of potential strikes, nation-states have strong incentive to strike first, to take out an adversary’s communication, electric, and transportation grids before it strikes. Former secretary of defense Leon Panetta recently said that the United States may also consider preemptive strikes if it detects “an imminent threat of attack that will cause significant physical destruction in the United States or kill American citizens.”47 The concept of imminence in the cyber realm, however, remains legally and doctrinally nebulous.48 This ambiguity makes coordination with allies more difficult since they may have a different legal interpretation of what is permissible. It increases the chances for miscalculation since legal boundaries can be useful for signaling and unclear ones can contribute to miscommunication, in addition to making it more difficult to predict international reactions to moves and countermoves in cyberspace.

After a long period in which U.S. officials hesitated to speak about offensive capabilities, over the last two years there have been a series of leaks to the press and public pronouncements on the development of cyber weapons. Reports in the New York Times and Washington Post have credited the United States and Israel with being behind Stuxnet, the malware designed to slow Iran’s nuclear program as part of a secret operation code-named Olympic Games.49

Arguments in support of Stuxnet or other covert operations are based in part on the alternatives. That is, an attempt to slow Iran’s nuclear program with malware that killed no one is politically and strategically preferable to commando raids, air strikes, or missile strikes that are likely to cause much greater physical damage and a number of deaths. Given the United States’ high degree of vulnerability to cyberattacks, there is concern that an operation like Stuxnet may create blowback or provide cover for an adversary to conduct a similar attack. Iran appears to have accelerated its cyber programs after the attack. There is also a negative impact on the United States’ ability to convince other states of the need for norms of peaceful conduct in cyberspace if they believe Washington has already used cyber weapons. But it is also true that many potential adversaries have been thinking about and developing offensive capabilities long before Stuxnet was ever developed, and the United States was no more vulnerable after Olympic Games was revealed than it was before. The public, however, is unable to fully participate in the debate on the merits of these types of uses of cyber weapons because of a high degree of secrecy. The Task Force calls for a more open public discussion and, where appropriate, the declassification of information.

Despite severe constraints in almost every other part of the defense budget, funding for computer network warfare is growing; the 2014 budget request includes $4.7 billion for cyberspace operations, a 20 percent increase from this year.50 U.S. Cyber Command is reportedly expanding by more than fivefold, from nine hundred to forty-nine hundred personnel, and creating three types of forces: national mission forces, to protect critical infrastructure and defend against nationallevel threats; combat mission forces, assigned to the operational control of individual combatant commanders, to plan and execute attacks; and cyber protection forces, to defend the Defense Department’s network. 51 Within the national mission forces, the Pentagon will reportedly create thirteen offensive teams by 2015 and twenty-seven within the combat mission forces to support the Pacific, Central, and other combatant commands as they plan offensive cyber operations.52

According to press reports, the Pentagon has developed classified rules of engagement for battle in cyberspace, which would guide commanders on when they could leave government networks to conduct offensive and defensive operations. In November 2012, President Obama reportedly signed Presidential Policy Directive 20, which “established principles and processes for the use of cyber operations,” including the offensive use of computer attacks.53 Offensive cyber operations outside a war zone are said to require presidential permission; even self-defense involving cyber operations outside military networks that could be construed as a use of force require presidential authorization. In addition, a legal review purportedly concluded that President Obama has the broad power to order a preemptive strike if the United States detects credible evidence of an imminent major cyberattack.54

This is progress compared with past reticence about offense, but U.S. government officials still publicly frame offensive military operations as defensive.55 The Task Force supports the U.S. government’s right to develop offensive capabilities, but calls for greater transparency about how and when such capabilities might be used. As the Defense Science Board argues, the United States needs to “clearly indicate that offensive cyber capabilities will be utilized (preemptively or in reaction, covertly or overtly), in combination with other instruments of national power, whenever the National Command Authority decides that it is appropriate.”56

These statements should be linked to and reinforced by the United States’ argument that the laws of war apply to cyberspace. State Department officials have said that that international humanitarian law can be extended to this new cyber domain, addressing the legal requirement of necessity in using force, what constitutes an act of force—“cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force”—as well as the principles of proportionality, neutrality, and distinction.57 But states like China question whether existing international laws apply to cyber and believe that cyberspace requires a new set of laws and treaties.

It is essential for the leading nations to agree on a set of norms for activity and engagement in cyberspace; **a failure to agree will be destabilizing, increasing the chances of misperception, misunderstanding, and escalation**. Perhaps even more disruptive to stability, nonstate actors frequently operate under the cover of a sovereign state. One country may see its action as permissible, the other as an act of war.

Lack of congressional consultation fuels uncertainty --- increases the risk

Dycus 10 (Stephen – Professor @ Vermont Law School, “Cybersecurity Symposium: National Leadership, Individual Responsibility: Congress's Role in Cyber Warfare” 2010, 4 J. Nat'l Security L. & Pol'y 155)

The important point here is that any use of cyber weapons, offensive or defensive, could have enormous consequences for the security and other interests of the United States. The effect of such use, actual or potential, matters more than the labels. And if the effect - on human life or property, for example, or diplomatic relations or compliance with the law of armed conflict - is substantial, Congress has a role to play in adopting policy for that use.

Congress has not thus far adopted measures suited to the regulation of cyber warfare. The War Powers Resolution, for example, is concerned with sending U.S. troops into harm's way, rather than with clicking a computer mouse to launch a cyber attack, although the strategic consequences might be similar. And the WPR's relatively relaxed timetable for executive notice and legislative response is unrealistic for war on a digital battlefield. Similarly, if cyber warfare is regarded as an intelligence activity, the intelligence oversight measures just described cannot, for reasons already indicated, ensure that Congress will be able to play a meaningful role. In the words of the National Research Council study cited above, "Today's policy and legal framework for guiding and regulating the use of cyberattack is ill-formed, undeveloped, and highly uncertain." n45

Our experience with nuclear weapons may point to needed reforms. Since the beginning of the Cold War, the United States has had a fairly clear nuclear policy (albeit one that deliberately includes an element of [\*163] ambiguity) - one known generally to Congress, the American public, and potential enemies. n46 Congress has approved or disapproved the purchase of the weapons and delivery systems. It has been briefed on the policy, and it has debated that policy vigorously. n47 While Congress has not articulated U.S. nuclear policy in any coherent form, it has collaborated closely with the executive branch in the development and execution of that policy.

Cyber weapons bear a striking resemblance to nuclear weapons in some important ways. An enemy's cyber attack would, like a nuclear strike, probably come without a clear warning. There are as yet no reliable defenses against either a cyber attack or a nuclear attack. Collateral damage from a nuclear attack would almost certainly be very extensive and would linger for an extended period. n48 The direct and indirect effects of a cyber attack, while different in kind and degree, still could be widespread and indiscriminate. n49

In other ways, cyber weapons are critically different from their nuclear counterparts. For one thing, the time frame for response to a cyber attack might be much narrower. A nuclear weapon delivered by a land-based ICBM could take 30 minutes to reach its target. An electronic attack would arrive instantaneously, and leave no time to consult with or even inform anyone outside the executive branch before launching a counterstrike, if that were U.S. policy.

What most distinguishes digital warfare, however, is the potential difficulty in identifying the source of a cyber attack. It is always possible, of course, that an enemy might covertly deliver a nuclear device to the U.S. homeland in a shipping container or a Cessna. But the apparent ease with which a cyber attack may be carried out without attribution could make it impossible to fight back at all. If an attacker made it appear that the source was an innocent neutral state or perhaps another enemy of the attacker, a misdirected U.S. response might provoke a wider conflict. The potential [\*164] difficulty in tracking the source also makes a policy of deterrence based on a threat of retaliation far less credible.

Given these characteristics of cyber warfare, and the continuing refinement of cyber weaponry, we approach a state of extreme strategic instability, with each nation on hair-trigger alert. The execution of an ill-conceived cyber war policy calling for a prompt response - or any response - to an attack or threatened attack could have disastrous, unanticipated consequences. It also might, depending on the circumstances, violate the law of armed conflict.

Congress accordingly needs to work closely with the executive branch in the development of a policy for this new kind of conflict. Such a policy ought to reflect the distinctive technology and strategy of digital warfare, and it should be reviewed constantly as the technology evolves. Like other regulations dealing with dynamic subjects, this policy should include general approaches that reflect this nation's broad strategic concerns and fundamental values. But the policy must also be crafted with enough flexibility to allow those charged with its execution to deal with future developments that cannot now be predicted. And it should set out a procedure for such adaptive use by identifying, for example, who must be consulted under what circumstances, and who will make the final critical decisions.

It is at least theoretically possible that Congress could play an active, real-time role in the implementation of whatever cyber warfare policy is adopted. The policy might, for example, like the War Powers Resolution, require consultation "in every possible circumstance." n50 But it seems more likely that a digital war would begin and end before any notice could ever reach Capitol Hill. Congress therefore needs to lay down clear guidelines, with as much flexibility as prudence requires, for executive branch officials to follow if consultation is not reasonably possible. And Congress should require a prompt and full account of every significant use of cyber weapons.

That causes global nuclear escalation

Rothschild 13 (Matthew, author and editor in chief of Progressive magazine, appears frequently on Nightline, C-SPAN, The O'Reilly Factor, and NPR, and his newspaper commentaries have run in the Chicago Tribune, the L.A. Times, the Miami Herald, and a host of other newspapers, “The Dangers of Obama’s Cyber War Power Grab” February 4, 2013, The Progressive) \*we don’t defend gendered language in this card

When our founders were drafting the Constitution, they went out of their way to give warmaking powers to Congress, not the President.

They understood that if the President could make war on his own, he’d be no different than a king.

And they also understood, as James Madison said, that such power “would be too much temptation” for one man.

And so they vested that power in Congress.

 But since World War II, one President after another has usurped that power.

The latest usurper is President Obama, who did so in Libya, and with drones, and now is prepared to do so in cyberspace.

According to The New York Times, the Obama Administration has concluded that the President has the authority to launch preemptive cyberattacks.

This is a very dangerous, and very undemocratic power grab.

There are no checks or balances when the President, alone, decides when to engage in an act of war.

And this new aggressive stance will lead to a cyber arms race. The United States has evidently already used cyber weapons against Iran, and so many other countries will assume that cyber warfare is an acceptable tool and will try to use it themselves.

Most troubling, U.S. cybersupremacy—and that is Pentagon doctrine—will also raise fears among nuclear powers like Russia, China, and North Korea that the United States may use a cyberattack as the opening move in a nuclear attack.

For if the United States can knock out the command and control structure of an enemy’s nuclear arsenal, it can then launch an all-out nuclear attack on that enemy with impunity. This would make such nuclear powers more ready to launch their nuclear weapons preemptively for fear that they would be rendered useless. So we’ve just moved a little closer to midnight.

Now, I don’t think Obama would use cyberwafare as a first strike in a nuclear war. But our adversaries may not be so sure, either about Obama or his successors. They, too, worry about the temptations of a President.

And, extinction

Guterl, executive editor – Scientific American, 11/28/’12

(Fred, “Armageddon 2.0,” Bulletin of the Atomic Scientists)

The world lived for half a century with the constant specter of nuclear war and its potentially devastating consequences. The end of the Cold War took the potency out of this Armageddon scenario, yet the existential dangers have only multiplied.Today the technologies that pose some of the biggest problems are not so much military as commercial. They come from biology, energy production, and the information sciences -- and are the very technologies that have fueled our prodigious growth as a species. **They are far more seductive than nuclear weapons**, and more difficult to extricate ourselves from. The technologies we worry about today form the basis of our global civilization and are essential to our survival.The mistake many of us make about the darker aspects of our high-tech civilization is in thinking that we have plenty of time to address them. We may, if we're lucky. But it's more likely that we have less time than we think. There may be a limited window of opportunity for preventing catastrophes such as pandemics, runaway climate change, and cyber attacks on national power grids. Emerging diseases. The influenza pandemic of 2009 is a case in point. Because of rising prosperity and travel, the world has grown more conducive to a destructive flu virus in recent years, many public health officials believe. Most people probably remember 2009 as a time when health officials overreacted. But in truth, the 2009 virus came from nowhere, and by the time it reached the radar screens of health officials, it was already well on its way to spreading far and wide. "H1N1 caught us all with our pants down," says flu expert Robert G. Webster of St. Jude Children's Research Hospital in Memphis, Tennessee. Before it became apparent that the virus was a mild one, health officials must have felt as if they were staring into the abyss. If the virus had been as deadly as, say, the 1918 flu virus or some more recent strains of bird flu, the result would have rivaled what the planners of the 1950s expected from a nuclear war. It would have been a "total disaster," Webster says. "You wouldn't get the gasoline for your car, you wouldn't get the electricity for your power, you wouldn't get the medicines you need. Society as we know it would fall apart." Climate change. Climate is another potentially urgent risk. It's easy to think about greenhouse gases as a long-term problem, but the current rate of change in the Arctic has alarmed more and more scientists in recent years. Tim Lenton, a climate scientist at the University of Exeter in England, has looked at climate from the standpoint of tipping points -- sudden changes that are not reflected in current climate models. We may already have reached a tipping point -- a transition to a new state in which the Arctic is ice-free during the summer months. Perhaps the most alarming of Lenton's tipping points is the Indian summer monsoon. Smoke from household fires, and soot from automobiles and buses in crowded cities, rises into the atmosphere and drifts out over the Indian Ocean, changing the atmospheric dynamics upon which the monsoon depends -- keeping much of the sun's energy from reaching the surface, and lessening the power of storms. At the same time, the buildup of greenhouse gases -- emitted mainly from developed countries in the northern hemisphere -- has a very different effect on the Indian summer monsoon: It makes it stronger. These two opposite influences make the fate of the monsoon difficult to predict and subject to instability. A small influence -- a bit more carbon dioxide in the atmosphere, and a bit more brown haze -- could have an outsize effect. The Indian monsoon, Lenton believes, could be teetering on a knife's edge, ready to change abruptly in ways that are hard to predict. What happens then? More than a billion people depend on the monsoon's rains. Other tipping points may be in play, says Lenton. The West African monsoon is potentially near a tipping point. So are Greenland's glaciers, which hold enough water to raise sea levels by more than 20 feet; and the West Antarctic Ice Sheet, which has enough ice to raise sea levels by at least 10 feet. Regional tipping points could hasten the ill effects of climate change more quickly than currently projected by the Intergovernmental Panel on Climate Change. Computer hacking. The computer industry has already made it possible for computers to handle a variety of tasks without human intervention. Autonomous computers, using techniques formerly known as artificial intelligence, have begun to exert control in virtually every sphere of our lives. Cars, for instance, can now take action to avoid collisions. To do this, a car has to make decisions: When does it take control? How much braking power should be applied, and to which wheels? And when should the car allow its reflex-challenged driver to regain control? Cars that drive themselves, currently being field tested, could hit dealer showrooms in a few years. Autonomous computers can make our lives easier and safer, but they can also make them more dangerous. A case in point is **Stuxnet**, the computer worm designed by the US and Israel to attack Iran's nuclear fuel program. It **is a watershed** in the brief history of malware -- the Jason Bourne of computer code, designed for maximum autonomy and effectiveness. Stuxnet's creators gave their program the best training possible: they stocked it with detailed technical knowledge that would come in handy for whatever situation Stuxnet could conceivably encounter. Although the software included rendezvous procedures and communication codes for reporting back to headquarters, Stuxnet was built to survive and carry out its mission even if it found itself cut off. The uranium centrifuges that Stuxnet attacked are very similar in principle to the generators that power the US electrical grid. Both are monitored and controlled by programmable-logic computer chips. Stuxnet cleverly caused the uranium centrifuges to throw themselves off-balance, inflicting enough damage to set the Iranian nuclear industry back by 18 months or more. A similar piece of malware installed on the computers that control the generators at the base of the Grand Coulee Dam would likewise cause them to shake, rattle, and roll -- and eventually explode. If Stuxnet-like malware were to insinuate itself into a few hundred power generators in the United States and attack them all at once, the damage would be enough to cause blackouts on the East and West Coasts. With such widespread destruction, it could take many months to restore power to the grid. It seems incredible that this should be so, but the worldwide capacity to manufacture generator parts is limited. Generators generally last 30 years, sometimes 50, so normally there's little need for replacements. The main demand for generators is in China, India, and other parts of rapidly developing Asia. That's where the manufacturers are -- not in the United States. Even if the United States, in crisis mode, put full diplomatic pressure on supplier nations -- or launched a military invasion to take over manufacturing facilities -- **the capacity to ramp up production would be severely limited.** Worldwide production currently amounts to only a few hundred generators per year. The consequences of going without power for months, across a large swath of the United States, would be devastating. Backup electrical generators in hospitals and other vulnerable facilities would have to rely on fuel that would be in high demand. Diabetics would go without their insulin; heart attack victims would not have their defibrillators; and sick people would have no place to go. Businesses would run out of inventory and extra capacity. Grocery stores would run out of food, and deliveries of all sorts would virtually cease (no gasoline for trucks and airplanes, trains would be down). As we saw with the blackouts caused by Hurricane Sandy, gas stations couldn't pump gas from their tanks, and fuel-carrying trucks wouldn't be able to fill up at refueling stations. Without power, the economy would virtually cease, and if power failed over a large enough portion of the country, simply trucking in supplies from elsewhere would not be adequate to cover the needs of hundreds of millions of people. People would start to die by the thousands, then by the tens of thousands, and eventually the millions. The loss of the power grid would put nuclear plants on backup, but how many of those systems would fail, causing meltdowns, as we saw at Fukushima? The loss in human life would quickly reach, and perhaps exceed, the worst of the Cold War nuclear-exchange scenarios. After eight to 10 days, about 72 percent of all economic activity, as measured by GDP, would shut down, according to an analysis by Scott Borg, a cybersecurity expert.

Lack of norms fuel aggression with China – spills over to kinetic hostilities

Moss 13 (Trefor, independent journalist based in Hong Kong covering Asian politics, defence and security, and was Asia-Pacific Editor at Jane’s Defence Weekly until 2009, “Is Cyber War the New Cold War?” April 19, 2013, The Diplomat)

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

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

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

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

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

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

Air-Sea Battle incentivzes Chinese pre-emptive cyber attack – makes conflict likely

Gompert & Kelly 13 (David, senior fellow at RAND and professor at the U.S. Naval Academy. His most recent government position was as President Obama's principal deputy director of national intelligence, Terrence Kelly is a senior operations researcher at RAND and the director of the RAND Arroyo Center's Strategy and Resources program. “Escalation Cause: How the Pentagon’s new strategy could trigger war with China” August 8, 2013, China-US Focus)

As the threat to forward-deployed U.S. forces grows, particularly in East Asia, the Pentagon has been pursuing a strategy known as Air-Sea Battle. As Chief of Naval Operations Admiral Greenert and Chief of Staff of the Air Force General Welsh have outlined here in FP, the goal is to neutralize the ability of enemies to keep U.S. forces at bay with so-called anti-access and area-denial defenses.

But while the proponents of Air-Sea Battle are careful to say that the strategy isn't focused on one specific adversary, we shouldn't kid ourselves: The Chinese see it as aimed at them. Then-Secretary of Defense Leon Panetta said as much in the 2012 defense strategic guidance: "States such as **China** and Iran **will continue to pursue asymmetric means to counter our power projection capabilities**.... Accordingly, the U.S. military will invest as required to ensure its ability to operate effectively in anti-access and area denial (A2/AD) environments."

To do that, according to Air-Sea Battle, U.S. forces would launch physical attacks and cyberattacks against the enemy's "kill-chain" of sensors and weaponry in order to disrupt its command-and-control systems, wreck its launch platforms (including aircraft, ships, and missile sites), and finally defeat the weapons they actually fire. The sooner the kill-chain is broken, the less damage U.S. forces will suffer -- and the more damage they will be able to inflict on the enemy. Therein lies both the military attractiveness and the strategic risk of Air-Sea Battle.

Air-Sea Battle proponents are right to highlight the growing vulnerability of forward-deployed U.S. forces and right to enhance inter-service collaboration. But civilian and military leaders alike need to understand that Air-Sea Battle suggests the United States would strike China before China strikes U.S. forces. That could precipitate a spiraling, costly, and destabilizing arms race and make a crisis more likely to lead to hostilities. The United States needs options to facilitate crisis management, deter aggression, and protect U.S. forces that do not require early attacks on Chinese territory.

Here we suggest two: Shift toward a more survivable force posture in East Asia and improve the means to prevent China -- or any state -- from projecting force in an act of international aggression.

Akin to the Air-Land Battle plan of the 1980s -- meant to thwart Soviet aggression against NATO -- Air-Sea Battle responds to the declining viability of forward defense, combined with an aversion to nuclear escalation. As then, Air-Sea Battle is a joint effort by two services to align their capabilities and war plans to defeat a serious threat from a powerful adversary. (Then it was the Army and Air Force, now the Navy and Air Force.) And like Air-Land Battle, there is more to Air-Sea Battle than inter-service collaboration: namely a focus on deep, early strikes against enemy forces, infrastructure, command and control, and territory -- then Soviet, now Chinese.

Disrupting or destroying China's kill-chain is alluring. China has the resources to threaten U.S. forces in the Pacific. Failure to develop countermeasures would leave the United States with a declining ability to operate militarily, deter Chinese use of force, reassure and defend allies, and exert influence in a vital region. Yet this simple idea could have dire consequences: Air-Sea Battle's targets would have to be struck before they could do significant damage to U.S. forces. With the exception of ships at sea and satellites in orbit, the targets that comprise China's kill-chain -- air and naval bases, missile launchers, land-based sensors, command-and-control centers -- are in China itself.

Attacking Chinese territory would have serious geopolitical consequences. China isn't the menacing, isolated Soviet Union. It's a huge and integral part of the world economy, as well as a potential U.S. partner in managing world affairs. While the United States must maintain a strong military presence to balance the growth of Chinese power and prevent instability in East Asia, where the potential for conflict is greatest, at the same time it is trying to engage China in security cooperation from Korea to the Persian Gulf. Moreover, 2013 is not 1980: Information technologies -- for targeting, networking, and cyberwar -- are advancing rapidly, and China is more capable of competing technologically than the Soviet Union ever was.

Given all these concerns, what does Air-Sea Battle contribute to U.S. security? It could indeed present China's military with serious problems. The kill-chain on which its A2/AD strategy depends is complex, fragile, and vulnerable to physical attacks and cyberattacks. By disabling this chain, Air-Sea Battle could buy space, time, and security for the use of existing U.S. strike forces. Or, as the Chinese see it, Air-Sea Battle could render China extremely vulnerable to U.S attack.

At the same time, Air-Sea Battle does not solve the underlying problem of U.S. forces' growing vulnerability in the Western Pacific. That is the result of military-technological trends, geographic realities, and the limitations and costs of defending overseas deployments. Each factor favors A2/AD. **Air-Sea Battle** could provide a stopgap countermeasure until the United States can address its vulnerability. But it also **has the potential to** deepen Chinese fears **of U.S. intentions, cause the Chinese to re-double their A2/AD effort** -- which they see as essential for national defense -- **and** even make conflict more likely. Importantly, the advent of Air-Sea Battle should not divert the United States from developing other capabilities that could serve the same ends without destabilizing Sino-U.S. relations.

Because China is so critical, and because war with China could be so dangerous, we must think through the circumstances in which potentially escalatory attacks would be warranted. We must not lose sight of the fact that the Chinese regard U.S. forces in the Western Pacific -- especially air- and sea-based strike forces -- as threatening. While some such forces are needed to deter Chinese use of force in the region, plans for their use should take into account the fact that the Chinese see things differently, and for the most part defensively.

Air-Sea Battle increases the odds that a crisis will turn violent. Already, the Chinese People's Liberation Army (PLA) leans toward early strikes on U.S. forces if hostilities have begun or appear imminent (this inclination is a first premise of the Air-Sea Battle concept). Given that, to be most effective, Air-Sea Battle would need to take down Chinese targeting and strike capabilities before they could cause significant damage to U.S. forces and bases. It follows, and the Chinese fear, that such U.S. capabilities are best used early and first -- if not preemptively, then in preparation for further U.S. offensive action. After all, such U.S. strikes have been used to initiate conflict twice in Iraq. This perception will, in turn, increase the incentive for the PLA to attack preemptively, before Air-Sea Battle has degraded its ability to neutralize the U.S. strike threat. It could give the Chinese cause to launch large-scale preemptive cyber- and anti-satellite attacks **on our Air-Sea Battle assets**. Indeed, they might feel a need, out of self-defense, to launch such attacks even if they had not planned to start a war. It is a dangerous situation when both sides put a premium on early action.

In addition, there is no reason to think that the Chinese will be resigned to the disadvantages created for them by Air-Sea Battle. Indeed, Chinese commentators are already calling for China to intensify its efforts to respond in space and cyberspace -- since Air-Sea Battle depends critically on the computer networks and satellites that connect U.S. sensors, platforms, weapons, and command-and-control systems. It is not clear that U.S. military networks can be hardened enough to withstand the sort of major cyberattacks the Chinese will be able to conduct in the coming years. True, such attacks could occur in the event of a Sino-U.S. conflict, Air-Sea Battle or not. But whether they occur preemptively or with ample warning could affect the ability of U.S. forces to withstand them. Just as Air-Sea Battle calls for the United States to initiate cyberattacks against China in the event of a conflict, it will reinforce Chinese motivations to develop the means and plans to initiate cyberwar against the United States. This could disadvantage the United States: Although Chinese reliance on computer networks for military operations and other functions is growing, the United States is and will remain for some time more network-reliant, and thus more exposed in the event of cyberwar. We simply do not understand well enough how cyberwar with China would unfold and whether it could be contained. Strategies that encourage mutual restraint rather than early offensive action in this unfamiliar strategic domain may ultimately be advantageous to the United States.

US-China opacity increases the risk

Segal 13 (Adam, Maurice R. Greenberg Senior Fellow for China Studies, “Three Thoughts on Cyber and the Defense Department’s Report on the Chinese Military” May 7, 2013 , Council on Foreign Relations; Asia Unbound)

The Defense Department released its annual report to Congress on Military and Security Developments Involving the People’s Republic of China 2013. Besides being delivered relatively early compared to past editions and being almost twice as long as the 2012 version, this year’s version has at least three interesting points about Chinese cyber activities.

First, as many have noted, the sharpest break from the past is that the report directly ascribes blame for cyberattacks to the Chinese government and military, saying, “numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military.” The 2012 report, by contrast, speaks of attacks “which originated within China” and active and persistent “Chinese actors.” The 2011 report describes cyber intrusions, “some of which appear to have originated within the People’s Republic of China (PRC).” The 2010 report seemed to split the difference, stating it was “unclear if these intrusions were conducted by, or with the endorsement of, the People’s Liberation Army (PLA) or other elements of the PRC government.”

Second, as David Sanger notes in the New York Times, the report tries to describe Chinese thinking about offensive cyber operations by citing two works of military doctrine, “Science of Strategy” and “Science of Campaigns.” This is not new—the 2011 report mentions them by name, while the 2010 report uses the same phrase “authoritative PLA military writings.” Sanger uses the report’s claim that neither Chinese document “identifies specific criteria for employing computer network attack against an adversary” to turn the mirror back on its authors, and note that the Defense Department has also been opaque about the conditions under which it would employ offensive capabilities. This lack of transparency is extremely destabilizing; the military doctrine of both countries emphasizes the importance of early attacks to gain information dominance, creating intense pressure to “use it or lose it,” but there is little knowledge of the other sides’ red lines and how they might escalate.

That conflict goes nuclear – 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.

Biggest risk

**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.

Plan provides legal clarity and strengthens cyber doctrine

Lorber 13 (Eric, J.D. Candidate, University of Pennsylvania Law School, Ph.D Candidate, Duke University Department of Political Science, “COMMENT: Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?” January, 2013, 15 U. Pa. J. Const. L. 961)

While many in the public sphere have paid a great deal of attention to the legality of offensive cyber operations, far less attention has been devoted to how domestic law interacts with the United States' employment of these capabilities. Indeed, policymakers have repeatedly noted "the mismatch between our technical capabilities to conduct operations and the governing laws and policies." n71 Over the past few years, studies have suggested that the United States has not developed such a legal framework and that whether current U.S. law - such as the War Powers Resolution - can regulate OCOs remains under-analyzed. n72 While some argue that attempting to develop such a framework will severely hamper the United States' ability to effectively conduct offensive cyber operations in future conflicts, n73 most analysts agree that "today's policy and legal framework for guiding and regulating the U.S. use of cyberattack is ill-formed, undeveloped, and highly uncertain." n74 To this point, most of the debate as to the legality of these operations has remained behind government doors. n75 Indeed, until very recently, scholars [\*975] have not paid substantial attention to these issues. To date, only a few articles, n76 blog postings, n77 and a National Resource Council report n78 have delved into this issue in any detail.

This lack of attention creates a series of problems in determining whether and how to regulate these operations. Most notably, before even addressing whether a new framework should be developed, the question arises as to whether the current domestic legal framework can govern the employment of these capabilities. Although many policymakers have suggested the current framework cannot govern OCOs, this question remains to be closely examined and argued. Only if the existing framework is found inadequate should legal scholars and practitioners design a new legal framework. Indeed, if, as Matthew Waxman argues, "strategy is a ... driver of legal evolution," n79 then new legal mechanisms may be required to ensure proper limitations on the executive's war-making abilities.

Though a full accounting of the potential domestic legal mechanisms governing the use of offensive cyber weapons is beyond the scope of this Comment, a first step in determining whether the current legal framework can be effective, at least partially, in governing the uses of these new weapons is to examine whether an appropriate procedural system exists as to regulate when and how they are employed. Though not delving into specifics about the use of these weapons, an operative, procedural framework that allows other governmental branches to review, understand, and potentially check the uses of these weapons provides an initial move towards their effective regulation. Though it may not be sufficient to fully clarify when and how the use of offensive cyber weapons may be legal, such a system at least would allow for oversight and hold the promise of helping policymakers better understand the conditions under which they can lawfully use these tools.

 [\*976] To this end, this Comment examines the two primary statutory tools through which Congress has tried to regulate executive military action: the War Powers Resolution and the Intelligence Authorization Act. There are two reasons to focus on these statutes. First, they apply to instances in which offensive cyber weapons will most likely be employed outside of surveillance and espionage actions: covert actions to disable and disrupt adversary systems and capabilities, and overt actions taken in conjunction with kinetic operations to degrade an adversary's ability to effectively conduct combat operations. Second, they are the primary means through which Congress has attempted to constrain the President's exercise of his constitutional Commander-in-Chief function. n80 Historically, and particularly since 1970, Congress has been reluctant to use its primary power, the power of the purse, to defund military activities, utilizing it only a handful of times. n81 As recent controversies over funding for wars in Iraq and Afghanistan, as well as the intervention in Libya illustrate, threatening to defund ongoing military operations is politically delicate and many legislators prefer to avoid taking such action. n82 Before proceeding to analyze OCOs through the prism of these two statutes, however, sharpening our understanding of the different types of OCOs is necessary.

II. Typologies, Employment, and Offensive Cyber Operations

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

Before moving to a discussion of what cyberattacks are, it is important to note what they are not. They are not cyberexploitation, that is, "the use of actions and operations ... to obtain information that would otherwise be kept confidential ... . Cyberexploitations are usually clandestine and conducted with the smallest possible intervention that still allows extraction of the information sought." n84 The core difference between attack and exploitation is in the cyber operation's purpose; cyberattacks are meant to be destructive whereas cyberexploitation acquires information nondestructively. n85 While the term offensive cyber operations usually encompasses both attack and exploitative elements, here "OCO" refers only to attacks. n86

At the most basic level, a cyberattack requires three elements: vulnerability; access; and payload. n87 A vulnerability is "an aspect of the system that can be used by the attacker to compromise" an adversary's network. n88 Given the increase in the number of complex systems employed by countries in the past two decades, many cyber defense analysts and computer experts agree that it is increasingly difficult to foresee and prevent vulnerability exploitation before attacks. n89 Access refers to the ability to deliver the payload into the target system such that it exploits the vulnerability. In particular, access to a target depends on whether the attack can be launched via remote access (e.g., by hacking into a computer network via the internet) n90 or close access (e.g., attacking a system through [\*978] the "local installation of hardware" via covert operatives). n91 The payload describes "the things that can be done once a vulnerability has been exploited. For example, once a software agent (such as a virus) has entered a given computer, it can be programmed to do many things - reproducing and retransmitting itself, destroying files on the system, or altering files." n92 Cyberattacks generally target a system's integrity (i.e., the system's ability to operate normally), n93 ability to discern proper authenticity (i.e., the system's ability to determine whether it should accept incoming data), n94 or its availability (i.e., whether users can properly access the system). n95 The resulting effects can be wide-ranging, including destroying data on networks, generating bogus network traffic, covertly altering data on the network, and degrading or denying service on the network. n96

Depending on whether the systems being attacked are remote or close access, a number of assault avenues exist. In an attack on a remote access system, botnets are one of the prominent means of assault. n97 In a botnet attack, which usually aims to deny users access to the system (such as a government website in a denial of service or distributed denial of service attack), bots install themselves on internet-connected computers and then, responding to commands from a master computer, attack the target by overloading it with numerous requests for information, such as e-mails, sometimes numbering in the millions. n98 Because the target cannot sufficiently process the information, it becomes inoperative. n99 Other ways to attack remote access systems include worms and viruses, which are generally used to install "trojan horse" systems on many computers that will render those computers inoperable. n100

Attacking close access systems may generally be more difficult given their lower degree of accessibility. However, one attack approach involves inserting malicious software into the supply chain of a system that will eventually become close access. n101 Such a strategy allows a compromised [\*979] machine or piece of software to enter into the close access system and then to be activated at a later point based on a variety of triggering mechanisms. Other attack routes include inserting compromised universal serial buses ("USBs") into close systems. Such an approach can be accomplished either by willing or unwilling insiders. n102

Hypothetically, scholars and practitioners have postulated a number of ways in which states might use cyberattacks in future combat scenarios, depending on a wide range of factors. n103 This process of categorization is not novel, as U.S. military planners have attempted to produce useful typologies since the mid-1990s. n104 While many potential categorization schemas exist, and many involve different types of adversaries, vulnerabilities, technologies underpinning the attacks, etc., most seem to focus on a primary element: the relationship of the cyberattack to other operations. In particular, the schemas differentiate based on whether the attack is part of a larger, kinetic offensive, or simply an attack launched independently of such operations. For example, Gregory Rattray and Jason Healey, in their recent work, suggest multiple ways in which a state could launch such an attack, but underpinning each is a discussion of whether the attack is part of a larger military operation or conducted independently. n105 [\*980] Likewise, William Owens, Kenneth Dam, and Herbert Lin differentiate between types of cyberattacks that directly support or are in conjunction with military operations, n106 and those conducted independently as covert action. n107

Further, the distinction between cyberattacks launched independently as opposed to part of a larger operation properly characterizes most known cyber operations to date. On the one hand, states have launched a number of attacks in recent years independent of kinetic operations. n108 For example, the actions in Estonia in 2007 - though potentially linked to the Russian government - were independent of any larger military assault. n109 More notably, the Stuxnet virus, which inflicted tremendous damage on the Iranian nuclear energy program by destroying its centrifuge cascades and much of its Uranium enrichment capability, was launched independent of military action. n110 Though no nation has taken responsibility for the virus, most analysts suggest that Israel, with the United States' help, designed and deployed the virus to hinder Iran's nuclear development. n111 On the other hand, because cyberattacks may make kinetic operations more effective, states have recently employed the two in conjunction. n112 For example, the alleged Israeli attack on Syria in 2007 n113 - as well as the alleged Russian attack on Georgia in 2008 n114 - both employed cyberattacks in conjunction with larger operations. In addition, U.S. war planning for Libya also included a cyber component, but only as part of a larger intervention. n115

 [\*981] Given the historical record of cyberattacks and that most of the theoretical literature categorizes such attacks based on their relationship to military actions, this Comment divides the attacks into binary categories: attacks waged independently of other military operations, and attacks waged as part of a larger military campaign. Though such a distinction may blur as states employ their capabilities in innovative ways, relying on that distinction now will aid both in understanding how different U.S. domestic laws apply to both general categories and in better preparing legal analysts in case of future cyber operations that do not neatly fit into them. Given this distinction, the analysis below examines whether current U.S. law effectively governs offensive cyber operations performed in conjunction with a military campaign or as a stand-alone operation.

III. The War Powers Resolution: Armed Forces, Hostilities, and Statutory Interpretation

Before proceeding to a discussion of either the War Powers Resolution or the Intelligence Authorization Act, one must acknowledge the inherent tension built into the relationship between Congress and the President over the power to wage war. Notably, the Constitution splits war-making authorities between the congressional and executive branches. n116 Proponents of executive power suggest that, because the President is the "Commander in Chief of the Army and Navy of the United States," n117 he is vested with the war-making power to determine when and how to deploy U.S. armed forces. n118 Conversely, Congress has the ability to "declare war," "raise and support Armies," "provide and maintain a Navy," and "provide for calling forth" and organizing and arming the militia. n119 Further, based on the Necessary and Proper Clause, some argue that Congress is empowered to pass legislation in accordance with its constitutional war-making authority specified above. n120 The debate over the extent of each branch's war-making [\*982] power has shadowed many conflicts in which the United States has been involved. n121

The intensity of this debate increased considerably during the Vietnam War, when Congress, uncomfortable with Presidents Johnson and Nixon's continuation of the conflict, attempted to rein in presidential power through a series of legislative acts. n122 The ineffectiveness of these early actions led a Senate committee to propose the War Powers Act in 1972. n123 After a period of extensive debates in which the language of the original Act was modified, n124 the House of Representatives concurred with the Senate bill and passed the Resolution on October 12, 1973. n125 On November 7, the House of Representatives overrode President Nixon's veto n126 of the War Powers Resolution. n127

Congress intended the War Powers Resolution ("WPR") n128 - passed in response to the Vietnam War when Presidents Kennedy, Johnson, and Nixon deployed large numbers of U.S. troops to Southeast Asia without a congressional declaration of war - to limit the President's power to send U.S. forces into combat without explicit congressional authorization. n129 However, given inherent questions about its constitutionality, n130 congressional unwillingness to invoke the authority granted to it under the [\*983] WPR under most circumstances, n131 and the likelihood that deploying offensive cyber activities does not constitute the introduction of armed forces into hostilities (if the hostilities threshold is even met), n132 the War Powers Resolution is a weak footing upon which to base congressional oversight of these activities.

The following section provides an overview of the provisions of the War Powers Resolution, paying particular attention to its reporting and withdrawal requirements. It then proceeds to discuss the debates over the Resolution's effectiveness and constitutionality, noting that while it has proven ineffective at times, it may not be fatally flawed or unconstitutional. Following, this section discusses the definitions of key terms, based both on how they have been interpreted in past historical instances of the Resolution's invocation and in the legislative history of the Act. Finally, this section argues that its terms likely do not cover offensive cyber operations launched independently or in conjunction with kinetic operations.

A. A Brief Overview of the War Powers Resolution

In the absence of congressional declaration of war, the WPR requires that:

The President shall submit within 48 hours to the Speaker of the House of Representatives and to the President pro tempore of the Senate a report, in writing, setting forth - (A) the circumstances necessitating the introduction of United States Armed Forces; (B) the constitutional and legislative authority under which such introduction took place; and (C) the estimated scope and duration of the hostilities or involvement. n133

Three circumstances trigger this reporting requirement. If United States armed forces are introduced: (1) "into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances;" n134 (2) if such forces are introduced "into the territory, airspace, or waters of a foreign nation, while equipped for combat, except for deployments which relate solely to supply, replacement, repair, or training of such forces;" n135 and (3) "in numbers which substantially enlarge United States Armed Forces equipped for combat already located in a [\*984] foreign nation." n136 Beyond requiring the President to submit a report to Congress within forty-eight hours of these specific triggering events, the WPR also directs the President to withdraw armed forces within sixty days after the report is submitted or is required to be submitted, unless Congress has declared war, extended the sixty-day period by law, or is physically unable to meet because of an armed attack against the United States. n137 The President can unilaterally extend this period for an additional thirty days. n138 In another controversial provision of the Act, Congress, by concurrent resolution, can order the President to remove U.S. armed forces if they are engaged in hostilities outside of the United States without a declaration of war or statutory authorization. n139 As discussed below, the constitutionality of this section (as well as the mandatory sixty-day removal requirement) is debatable, as the Supreme Court has ruled that legislative vetoes invalidating executive actions - which these sections arguably constitute - are unconstitutional. n140

As becomes evident, based on the text of the Resolution, determining the definitions of "U.S. armed forces," "hostilities," "imminent," and "into the territory ... while equipped for combat," is crucial for concluding whether the President must report U.S. military activities and remove U.S. forces after sixty days. Before analyzing whether such definitions might encompass offensive cyber operations, it is helpful to understand the primary arguments against the Act, including the routine assertion by Presidents that it is unconstitutional. n141

B. The Alleged Weaknesses of the War Powers Resolution

Critics of the War Powers Resolution assert two broad critiques: that it is ineffective in practice and that it is unconstitutional. n142 Regarding the first [\*985] claim, analysts suggest that Presidents simply order operations that successfully evade WPR reporting and withdrawal requirements, despite the fact that U.S. soldiers are deployed in situations likely imagined by the statute's drafters. n143 In particular, administrations continually argue that situations into which U.S. troops are deployed do not constitute hostilities. n144 Likewise, some suggest that macro-scale operations of the kind triggering the War Powers Resolution - where lengthy troop deployments are followed by crises and subsequent war - are antiquated and unlikely to occur in contemporary times. n145 Other analysts simply claim that Presidents have ignored the reporting requirements n146 and that members of Congress have been unwilling to stand up to potentially popular presidential uses of force, even if they clearly violate the WPR. n147 As a result, some analysts believe that other congressional mechanisms, such as its funding powers, provide the body with stronger oversight ability over executive action. n148 While many have critiqued the War Powers Resolution for its apparent ineffectiveness, this does not necessarily suggest it is has been futile; Presidents have actively submitted reports pursuant to its requirements and therefore have at least provided Congress with information about their activities. n149

 [\*986] In addition to critiquing its effectiveness, administrations and legal analysts have suggested that the WPR is unconstitutional or suffers from substantial legal problems. n150 These claims break down into four different assertions: that the War Powers Resolution infringes on the President's commander-in-chief function, based on an original understanding of these provisions by the Framers; n151 that the concurrent resolution constitutes a legislative veto of an executive action and is therefore unconstitutional under Immigration and Naturalization Services v. Chadha; n152 that members of Congress do not have standing to bring claims for presidential violations of the WPR; n153 and that enforcement of the WPR presents a non-justiciable claim. n154

While each of these claims has merit, none is sufficiently definitive as to whether the Resolution is constitutional or suffers from other fatal legal flaws. First, good evidence exists to support arguments that the Framers would have found the Resolution to be consistent with congressional war powers, n155 or conversely, that it infringes upon the Executive's commander-in-chief function. n156

Second, the War Powers Resolution may not constitute a "legislative veto" for the purposes of Chadha. n157 According to legal scholars, "the [\*987] Chadha decision is generally believed to have struck down section 5(c) of the War Powers Resolution, which permits the Congress to direct the President to remove the armed from a hostile situation by passage of a concurrent resolution." n158 In addition, some argue that Section 5(b) (requiring the removal of troops after the mandatory sixty-day period without congressional action, i.e., if only one chamber of Congress does not act) also represents a legislative veto. n159 In Chadha, the Supreme Court ruled that § 244(c)(2) of the Immigration and Nationality Act, which allowed Congress to pass a joint resolution forcing the Attorney General to cancel a deportation, was unconstitutional because it was a legislative veto of executive action. n160 Basing its decision on Article I, Section 7, Clauses 2 and 3 of the Constitution, the Supreme Court concluded that congressional action meant to have the effect of law must be approved by both houses of Congress and presented to the President for his approval (or disapproval). n161 In Chadha, "the Court held that § 244(c)(2) [was] unconstitutional because it authorized one house of Congress to change the legal status quo by action less than that required by the Constitution for a valid law." n162 As noted by Professor Sidney Buchanan however, substantial distinctions exist between § 244(c)(2) and the War Powers Resolution. For example, § 244(c)(2) allowed Congress to change the legal status quo by adjusting the legal status of the immigrant. n163 If, as some scholars argue, the War Powers Resolution is a codification of legally existing congressional war-making authority, then the War Powers Resolution does not change the legal status quo but merely fleshes out these powers. n164 Further, though scholars note that the War Powers Resolution may be unconstitutional because the action (of forcing the removal of troops) is not presented to the President for his approval, such presentment may not be required. n165 In Hollingsworth v. Virginia, the Supreme Court suggested that the presentment requirement applies only to [\*988] "ordinary" cases of legislation. n166 This assertion implies that there may exist cases where legislation does not require presentment before the President and it is likely that a concurrent resolution in the War Powers Resolution would be extraordinary enough to fall into such a category. n167 As a result, it is unclear whether the War Powers Resolution represents an impermissible legislative veto.

Third, courts have suggested that members of Congress may have standing to bring suit based on violations of the War Powers Resolution. n168 Federal courts have suggested that, if Congress were to pass a resolution requiring a particular presidential report under the War Powers Resolution, for example, non-compliance with this resolution would constitute a cognizable claim. n169 As a result, Congress could potentially use the courts to bring a successful claim for violation of the War Powers Resolution.

Fourth and finally, some federal courts have asserted that the issue of whether the President refuses to abide by the War Powers Resolution is a political, non-justiciable question, and therefore the courts cannot rule on the matter. n170 At the same time, however, courts have also asserted that if a majority of Congress agreed that the President must abide by the requirements of the War Powers Resolution in a given circumstance, such consensus would present a justiciable claim to the courts. n171

As this discussion illustrates, the War Powers Resolution is certainly flawed. However, it is not necessarily unconstitutional and may serve some [\*989] positive function by alerting Congress to activities undertaken by the President and giving them the potential opportunity to weigh in, albeit not likely force the removal of U.S. forces. Thus, it still may prove useful in helping Congress regulate the use of offensive cyber operations, if it applies to them.

C. The War Powers Resolution as Applied to Offensive Cyber Operations

As discussed above, critical to the application of the War Powers Resolution - especially in the context of an offensive cyber operation - are the definitions of key terms, particularly "armed forces," as the relevant provisions of the Act are only triggered if the President "introduc[es armed forces] into hostilities or into situations [of] imminent ... hostilities," n172 or if such forces are introduced "into the territory, airspace, or waters of a foreign nation, while equipped for combat, except for deployments which relate solely to supply, replacement, repair, or training of such forces." n173 The requirements may also be triggered if the United States deploys armed forces "in numbers which substantially enlarge United States Armed Forces equipped for combat already located in a foreign nation." n174 As is evident, the definition of "armed forces" is crucial to deciphering whether the WPR applies in a particular circumstance to provide congressional leverage over executive actions. The definition of "hostilities," which has garnered the majority of scholarly and political attention, n175 particularly in the recent Libyan conflict, n176 will be dealt with secondarily here because it only becomes important if "armed forces" exist in the situation.

As is evident from a textual analysis, n177 an examination of the legislative history, n178 and the broad policy purposes behind the creation of the Act, n179 [\*990] "armed forces" refers to U.S. soldiers and members of the armed forces, not weapon systems or capabilities such as offensive cyber weapons. Section 1547 does not specifically define "armed forces," but it states that "the term "introduction of United States Armed Forces' includes the assignment of members of such armed forces to command, coordinate, participate in the movement of, or accompany the regular or irregular military forces of any foreign country or government." n180 While this definition pertains to the broader phrase "introduction of armed forces," the clear implication is that only members of the armed forces count for the purposes of the definition under the WPR. Though not dispositive, the term "member" connotes a human individual who is part of an organization. n181 Thus, it appears that the term "armed forces" means human members of the United States armed forces. However, there exist two potential complications with this reading. First, the language of the statute states that "the term "introduction of United States Armed Forces' includes the assignment of members of such armed forces." n182 By using inclusionary - as opposed to exclusionary - language, one might argue that the term "armed forces" could include more than members. This argument is unconvincing however, given that a core principle of statutory interpretation, expressio unius, suggests that expression of one thing (i.e., members) implies the exclusion of others (such as non-members constituting armed forces). n183 Second, the term "member" does not explicitly reference "humans," and so could arguably refer to individual units and beings that are part of a larger whole (e.g., wolves can be members of a pack). As a result, though a textual analysis suggests that "armed forces" refers to human members of the armed forces, such a conclusion is not determinative.

An examination of the legislative history also suggests that Congress clearly conceptualized "armed forces" as human members of the armed forces. For example, disputes over the term "armed forces" revolved around who could be considered members of the armed forces, not what constituted a member. Senator Thomas Eagleton, one of the Resolution's architects, proposed an amendment during the process providing that the Resolution cover military officers on loan to a civilian agency (such as the Central [\*991] Intelligence Agency). n184 This amendment was dropped after encountering pushback, n185 but the debate revolved around whether those military individuals on loan to the civilian agency were still members of the armed forces for the purposes of the WPR, suggesting that Congress considered the term to apply only to soldiers in the armed forces. Further, during the congressional hearings, the question of deployment of "armed forces" centered primarily on past U.S. deployment of troops to combat zones, n186 suggesting that Congress conceptualized "armed forces" to mean U.S. combat troops.

The broad purpose of the Resolution aimed to prevent the large-scale but unauthorized deployments of U.S. troops into hostilities. n187 While examining the broad purpose of a legislative act is increasingly relied upon only after examining the text and legislative history, here it provides further support for those two alternate interpretive sources. n188 As one scholar has noted, "the War Powers Resolution, for example, is concerned with sending U.S. troops into harm's way." n189 The historical context of the War Powers Resolution is also important in determining its broad purpose; as the resolutions submitted during the Vietnam War and in the lead-up to the passage of the WPR suggest, Congress was concerned about its ability to effectively regulate the President's deployments of large numbers of U.S. troops to Southeast Asia, n190 as well as prevent the President from authorizing troop incursions into countries in that region. n191 The WPR was a reaction to the President's continued deployments of these troops into combat zones, and as such suggests that Congress's broad purpose was to prevent the unconstrained deployment of U.S. personnel, not weapons, into hostilities.

This analysis suggests that, when defining the term "armed forces," Congress meant members of the armed forces who would be placed in [\*992] harm's way (i.e., into hostilities or imminent hostilities). Applied to offensive cyber operations, such a definition leads to the conclusion that the War Powers Resolution likely does not cover such activities. Worms, viruses, and kill switches are clearly not U.S. troops. Therefore, the key question regarding whether the WPR can govern cyber operations is not whether the operation is conducted independently or as part of a kinetic military operation. Rather, the key question is the delivery mechanism. For example, if military forces were deployed to launch the cyberattack, such an activity, if it were related to imminent hostilities with a foreign country, could trigger the WPR. This seems unlikely, however, for two reasons. First, it is unclear whether small-scale deployments where the soldiers are not participating or under threat of harm constitute the introduction of armed forces into hostilities under the War Powers Resolution. n192 Thus, individual operators deployed to plant viruses in particular enemy systems may not constitute armed forces introduced into hostilities or imminent hostilities. Second, such a tactical approach seems unlikely. If the target system is remote access, the military can attack it without placing personnel in harm's way. n193 If it is close access, there exist many other effective ways to target such systems. n194 As a result, unless U.S. troops are introduced into hostilities or imminent hostilities while deploying offensive cyber capabilities - which is highly unlikely - such operations will not trigger the War Powers Resolution.

IV. The Intelligence Authorization Act: Covert Actions and the Traditional Military Activities Exemption

Stemming from similar tension noted in the constitutional division of war-making authority noted above, congressional oversight of covert actions beyond intelligence collection has often proved a point of contention between the executive and legislative branches. n195 Presidents have "inferred authority [to conduct covert actions] from such places as the Vesting Clause, the Commander-in-Chief Clause, the Treaty Clause, and from an implied executive privilege." n196

 [\*993] Likewise, Congress attempted to rein in the President's ability to conduct covert operations without oversight by implementing a series of laws that required the President to get approval before undertaking such activities. n197 If the President did not provide such notification, Congress could decline to fund that particular covert activity. n198 Following the revelation that widespread, unreported covert actions were undertaken during the Vietnam War, Congress moved for stricter control of executive power, both by forcing the executive to account for the money it was spending as part of annual authorization bills n199 and by streamlining its own oversight capability by tasking two primary committees, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, with oversight. n200

While Congress designed this legislation to rein in the President's power to conduct covert activities without oversight, events in the 1980s clearly showed that its efforts had been ineffective. n201 In particular, the Iran-Contra affair illustrated that Congress needed to substantially reform oversight legislation to ensure that it could properly monitor executive covert action. n202 As a result, in 1990, Congress began drafting a new oversight bill, [\*994] the Intelligence Authorization Act of 1991, which grants Congress oversight of covert activities. n203 Section 413b of the Intelligence Authorization Act provides,

To the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the Director of Central Intelligence and the heads of all departments, agencies, and entities of the United States Government involved in a covert action ... shall keep the [congressional] intelligence committees fully and currently informed of all covert actions ... . n204

The Act further provides that the President must ensure that any covert action that falls under the scope of the Act is reported to Congress "as soon as possible after such approval and before the initiation of the covert action" n205 unless "the President determines that it is essential to limit access to the finding to meet extraordinary circumstances affecting vital interests of the United States." n206 Moreover, if the President does not fully inform the intelligence committees prior to the action, he or she "shall fully inform the [congressional] intelligence committees in a timely fashion and shall provide a statement of the reasons for not giving prior notice." n207

Congress, recognizing that the power of the statute turned - to a substantial degree - on the definition of covert action, provided guidance both in the legislation and the committee reports as to what the term meant. According to the statute, "the term "covert action' means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly." n208 Congress also provided a list of exceptions to the term, however, specifically noting that, inter alia, "activities the primary purpose of [\*995] which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities," as well as "traditional diplomatic or military activities or routine support to such activities," do not constitute covert action. n209

While an initial textual reading of these exceptions - especially traditional military activities ("TMAs") - suggests that they are extremely broad, an examination of the Act's legislative history suggests that they are narrower than they first appear. In particular, as University of Texas law professor Robert Chesney notes, the Senate Select Committee on Intelligence's ("SSCI") committee report associated with the legislation,

went on to make clear that the SSCI assumed that U.S. government responsibility "would be apparent or acknowledged at the time of the military operation.' When that was not the case - i.e. when "military elements not identifiable to the United States [are] used to carry out an operation abroad without ever being acknowledged by the United States" - the operation would not constitute TMA. n210

This original understanding led to an odd result, whereby "the TMA exemption did no work, as the definition of covert action already excluded operations in which the U.S. role was intended to be acknowledged." n211 To remedy this issue, the committees proposed, and President Bush ultimately accepted, n212 a compromise whereby an unacknowledged operation could fall under the traditional military activities exemption by meeting two requirements: n213 first, the TMA must be commanded and executed by military personnel; and second, the TMA must take place in a context in which overt hostilities are either ongoing or anticipated, meaning approval has been given by the National Command Authority (which consists of the President and the Secretary of Defense) for the activities and for the operational planning for hostilities. n214 Further, according to Chesney, "operational planning can and normally will begin far earlier than the eve of conflict or even the eve of a deployment in anticipation of combat... . The "operational planning' standard ... is not nearly as restrictive ... as the casual reader might assume." n215

 [\*996]

A. The Intelligence Authorization Act as Applied to Offensive Cyber Operations

Given the language of the statute and the elaboration on its language provided by the legislative history, would offensive cyber operations - either used independently or in conjunction with a military campaign - trigger the notification requirements of the Intelligence Authorization Act? Looking first at cyber operations used prior to - or in conjunction with - military campaigns, the President would not need to report these to Congress under § 413b. Interestingly, depending on how the United States decides to conduct its offensive cyber operations, they may not even constitute covert actions under 413b, before even reaching the question of whether they fall under the exemptions. The statute's definition of covert actions requires that the United States not intend its role be "apparent or acknowledged publicly." n216 If, for example, the United States were to launch an attack using proxy forces - similar to the alleged Russian attack against Georgia in the 2008 war - it would likely constitute a covert action because the United States would be attempting to hide its role. Conversely, in the Israeli case, Israel likely did not intend for its computer attack against Syrian air defenses to remain hidden; indeed, by the overall attack's public nature, it seemed likely that information about the cyberattack preceding the military strike would be revealed. Likewise, if the United States in the lead-up to the Libya intervention had launched a cyberattack against the Libyan air defense network, it might also have failed to constitute covert action because of the likelihood that the third party observers would understand that a cyberattack occurred. Further, in the Israeli case and the Libya hypothetical, Israel and the United States clearly did not intend to hide their roles, as they followed the cyberattacks (or considered attacks) by openly striking targets within those countries.

If the United States did intend to hide a cyberattack, even though it was part of a larger military operation, such an attack would likely fall into the "traditional diplomatic or military activities or routine support to such activities" exception provided in the statute. n217 To qualify as a traditional military activity, the TMA must be commanded and executed by military personnel and take place in a context in which overt hostilities are either ongoing or anticipated, meaning approval has been given by the National Command Authority for the activities and for the operational planning for hostilities. n218 Given that the National Security Agency, responsible for the development and deployment of U.S. cyber capabilities, is co-housed and [\*997] extensively shares personnel with U.S. Cyber Command, the military command tasked with launching cyberattacks against adversaries, it seems likely that any such attack will satisfy the first prong of the test. n219

Regarding the second prong, cyber operations conducted prior to, or in conjunction with, military operations may also take place in a context in which overt hostilities are either ongoing or anticipated. First, using the Russian activities in the 2008 war with Georgia as the basis for a factual hypothetical, if the United States were to conduct similar operations parallel to kinetic operations, such activity would be taking place in the context of overt hostilities. Though the level of hostilities is important in determining whether "overt hostilities" exist, n220 a Georgian-style conflict would likely trigger this exception. n221 Though one might argue, as the Obama administration did in the 2011 Libyan intervention, that its actions did not constitute hostilities (and therefore did not trigger the War Powers Resolution's reporting requirement), that argument does not hold force here because the Obama Administration was referring to the period after United States airmen were engaging in direct strikes against Libyan ground forces (and after all of Libya's air defenses were effectively destroyed). n222 By inference, the period in which U.S. forces were striking Libyan targets did constitute hostilities. Therefore, these cyber operations, used in conjunction with military operations, would likely fall under the TMA exception.

If the cyberattacks were used prior to the commencement of hostilities (for example if the United States launched OCOs to disable Libya's air defense network), they would also likely fall under the language of the exception because the National Command Authority would have given approval both for the activities and operational planning for the hostilities. While this might seem like a high burden, National Command Authority consists only of the President and the Secretary of Defense. n223 Thus the [\*998] President and the Secretary of Defense must only approve the activities in anticipation of overt hostilities. Further, because operational planning can simply constitute planning for a "situation that likely would involve military forces in response to natural and man-made disasters, terrorists, subversives, military operations by foreign powers, or other situations as directed by the President or SecDef," n224 National Command Authority for operational planning does not require the President and the Secretary of Defense to prepare to commence overt hostilities, but rather they can simply conduct contingency planning for a wide range of scenarios. Further, in a circumstance where the United States is prepared to actively intervene in another country, such as Libya, it would be clear that overt hostilities are anticipated, even in circumstances where overt hostilities are not imminent. In such a scenario, the President is merely considering future action and planning accordingly, and thus such offensive cyber operations would likely fall under the Traditional Military Activities exception.

Offensive cyber operations might also be exempt under the routine support exception. If the activity is "routine support" to "traditional diplomatic or military activities," it does not constitute covert action. n225 Though the legislation does not define "routine," the Senate committee suggested it involved a subjective element and that providing pertinent examples might be useful. n226 According to the committee, the term "would include various forms of logistical support that might be useful in placing personnel inside a denied area and enabling them to act without detection, including false documents, communications gear, safe houses, transportation, and information." n227 Interestingly, these examples seem to reference support to covert activities, not necessarily traditional military activities (i.e. helping to facilitate individuals to act without detection). However, if these activities are meant to support traditional military activities, then the language seems likely to encompass cyberattacks in preparation for military attacks against a target. For example, if the United States had launched OCOs against Libya to disable its air defense network in preparation of an allied air attack, this might be similar to aiding personnel in gaining access to a denied area (in this case, the personnel would be U.S. aircraft and the associated crewmen and the denied area would be airspace denied because of the defenses protecting it). While ambiguity certainly exists as to whether such a cyber operation would constitute routine support, [\*999] offensive cyber operations conducted prior to - or in conjunction with - kinetic operations likely do fall under the covert action exemption.

Likewise, offensive cyber operations conducted independently of military operations, though likely constituting covert action, are also likely exempt under the Traditional Military Activities exception. Imagine, for example, that the United States launched the Stuxnet worm that attacked Iran's nuclear enrichment capabilities without Israeli involvement. Further imagine that all other facts in the case were the same as they are in reality (i.e. the United States denied its involvement in the attack). In such a case, the attack seems to constitute a covert action that requires reporting to the congressional intelligence committees because it was an activity to influence political conditions (i.e. the Iranian ability or decision to develop its nuclear program) or military conditions (i.e. preventing the Iranians from moving forward with the development of a nuclear weapon, which could substantially bolster their military capability) abroad. n228 Further, the United States did not intend for its role to be apparent or publicly acknowledged. n229

Despite falling into this category, however, such an offensive operation, for the reasons discussed above, likely satisfies the congressional test for a traditional military activity. First, because General Alexander is the commander of both CYBERCOM and the head of the National Security Agency and because many of the personnel are dual-hatted at the respective organizations, any offensive cyber operation conducted independently of a kinetic assault will be commanded and executed by military personnel. n230 Second, because the President can launch offensive cyber operations without congressional notification if they are in anticipation of hostilities, n231 he also has great flexibility in deciding whether to report his activities. For example, if the President were to order the launch of a Stuxnet-style attack against Iran to degrade its nuclear enrichment capability, such an activity would - assuming it was done with the Secretary of Defense's consent - necessarily constitute approval by the National Command Authority. In addition, because the definition of operational planning - another element required in fulfilling the TMA exception to the definition of covert action - is so broad, such an attack would likely fall within its purview. The President would simply argue that approval has been given for operational planning of future combat operations with Iran (which it almost certainly has in the U.S. military) n232 and therefore the activity was taking place in the context where [\*1000] overt hostilities are anticipated. Indeed, only in a situation where no contingency planning has occurred - such as with an ally or a country that the United States takes little interest - would this exception not apply.

As a result, it becomes evident that even a Stuxnet-type of attack likely will not trigger the requirements set forth in the Intelligence Authorization Act. Given the dual-hatted nature of many NSA and CYBERCOM personnel, as well as the fact that action approved by the President and the Secretary of Defense necessarily constitutes approval by the National Command Authority, all the executive branch must realistically show is that it undertook the operation in a context where operational planning had occurred for potential hostilities at some undefined point in the future. This hurdle is very low and the executive should have little problem clearing it.

These limited requirements suggest that the executive can easily argue that offensive cyber operations conducted both as independent actions and in conjunction with kinetic operations likely fall under the Traditional Military Activity exception to the definition of covert action as provided by the Intelligence Authorization Act. As a result, the President is likely not statutorily required to report any offensive cyberattacks under the Act.

V. A Middle Ground of Legal Oversight

This analysis suggests that, given inherent weaknesses in the underlying statutory schemes, excluding offensive cyber operations from their scope does not substantially shift the balance of war-making authority between the President and Congress. This exclusion does, however, provide the President additional, powerful means by which to conduct military action without congressional oversight.

Based on analysis of the War Powers Resolution, the lack of oversight for OCOs does not radically shift the balance between the legislative and executive branches' war-making authority. Most notably, because the War Powers Resolution itself has proven ineffective in providing Congress with a powerful tool to govern presidential use of force, bringing OCOs under the War Powers Resolution's statutory umbrella likely would not provide the possibility of such oversight. However, insofar as the President has increasingly turned to covert action since the passage of the War Powers Resolution to avoid its reporting requirements, n233 offensive cyber operations [\*1001] provide the President another means by which to continue this trend. OCOs therefore may give the President substantially more flexibility than he already has under the War Powers Resolution by adding what will become an increasingly frequent tool of warfare to his option-set.

The lack of congressional oversight of offensive cyber operations under the Intelligence Authorization Act also likely does not seriously shift the balance between congressional and executive war-making powers. The reason is inherent in the limitations of the legislation itself: the Intelligence Authorization Act specifies reporting requirements, but does not require the non-use or withdrawal of forces. n234 Further, these reports must be made in a "timely" fashion (the definition of which is undefined) and only to a small number of Congressmen (at most eight). n235 Thus even if the President had to report offensive cyber operations to Congress, it is unclear he would have to do so in a way that gave Congress an effective check, as these reports would be made only to a small group of Congressmen (who would not be able to share the information, because of its classified nature, with other members of the legislature) and could be done well after the employment of these capabilities. The resulting picture is one of increased presidential flexibility; the War Powers Resolution and the Intelligence Authorization Act - while arguably ineffective in many circumstances - provide increased congressional oversight of presidential war-making actions such as troop deployments and covert actions. Yet these statutes do not cover offensive cyber operations, giving the President an increasingly powerful foreign policy tool outside congressional reach.

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.

These **competing arguments** - one for limiting any oversight and one for increasing it - **suggest a** middle ground **that will avoid drawing red lines but will still provide useful** congressional insight into the doctrinal and legal development **of offensive cyber operations**. Such an approach would include new legislation, similar to the Intelligence Authorization Act, explicitly requiring the President to report its use of covert cyber activities to the heads of Senate and House intelligence committees (i.e. the Gang of Eight). n238 Congress would not have the ability to veto such actions, however it would be able to raise potential legal issues with the executive branch, as well as provide policy advice as to the wisdom of employing these capabilities in such circumstances. As a result, while the heads of these committees would not have the ability to draw red lines themselves, they would be able to consult with the executive branch - as the branch employs these capabilities - to determine their likely legality and wisdom. While the President could ignore this advice, such an approach would at the very least keep Congress informed of the developing capabilities and their employment. With such an approach, Congress could play a meaningful role in the shifting and uncertain legal and policy realms of offensive cyber operations, which will undoubtedly become increasingly important as the United States and other nations develop and employ these capabilities with ever-greater frequency.

That builds deterrence regimes – promotes international attention to implement norms

Lieberthal & Singer 12 (Kenneth G. Lieberthal - Director @ John L. Thornton China Center & Senior Fellow of Foreign Policy and Global Economy and Development @ Brookings Peter W. Singer -- Director @ 21st Century Defense Initiative & Senior Fellow of Foreign Policy @ Brookings, “ Cybersecurity and U.S.-China Relations” February 23, 2012, Brookings Institution)

Cyber war, like cyber crime, is a realm in which there may be real gains for all players to come to agreement on what actions might risk gen erating a wider conflict. This is useful not only for each side to know, so as to avoid investing in and using capabilities that would unintentionally escalate a crisis, but also to try to generate certain norms and implementing mechanisms to take such risky actions “off the table.” Any such agreements—and even the process of negotiating them— can increase mutual understanding, decrease distrust, and make each country less inclined to react precipitously to any indication of danger.

The Cold War provides examples of the problem of lack of clarity in such “red lines” of behavior. In 1962, the U.S. and USSR had not effectively communicated to each other their red lines on where nuclear weapons might be located and what behavior would trigger escalation. That is, neither side was happy about the other developing such capabilities, but each side unintentionally deployed them in a manner (the U.S. putting missiles into Turkey and the Soviets into Cuba) that raised the level of tension and provoked a reaction well past what they expected. The outcome was the Cuban Missile Crisis, where competition moved into destabilization and near thermonuclear war.

Today, the U.S. and Chinese doctrines in cyber space are quite similar in their deliberate vagueness and, indeed, quite parallel to the situation in the late 1950s and 60s. For example, the U.S. Defense Department cyber strategy published in 2011 announced a new doctrine, arguing that harmful action within the cyber domain can be met with a parallel response in another domain. 73 This has come to be known as “equiva lence.” 74 Aiming for such flexibility is certainly sensible from one angle, but problems emerge when it is weighed through the lens of a competition between two states. Substitute the words “conventional” and “nuclear” for “cyber” and “kinetic” and the new doctrine is fundamentally similar to the 1960s nuclear deterrence doctrine of “flexible response” that possibly helped lead to the Cuban crisis. The Chinese cyber strategy is even more opaque, much like the Soviet nuclear strategy was to U.S. leaders at the time.

Coming to such agreements on red lines of behavior is surprisingly possible even in the most contentious realms. For example, much of the pernicious state-sponsored activity in the cyber realm today is related in some way to espionage. But even at the height of the Cold War, the CIA and KGB were able to come to an informal set of agreements to avoid certain types of behavior. Neither side liked the other stealing secrets from it, but the two agencies were able to communicate a set of activities and targets that were to be avoided by both in order to keep their competition in the espionage realm from escalating into some thing more serious. 75

In short, no one should expect all disagreements to be easily resolved or the two sides to give up their core interests or values, nor that certain codes of conduct won’t change as situations evolve. Rather, the goal is to communicate one’s interests and values effectively. Many believe that this will actually be in each party’s own interest, as it will aid their respective deterrence strategies. As General James Cartwright (ret.), former Vice Chairman of the Joint Chiefs of Staff, and one of the key figures in the development of U.S. cybersecurity strategy, notes, “You can’t have something that’s a secret be a deterrent. Because if you don’t know it’s there, it doesn’t scare you.” 76

Most importantly, it will clarify to each side the paths of behavior that will be viewed as egregious and provoke serious tension and responses that neither side wishes to see happen. That is, even if no formal agreement is possible, there is great value in having serious discussion to start the process of communicating each side’s “red lines,” what they would view as unacceptable behavior in the cyber realm that could lead rapidly to a crisis. This discussion is important in that it will inform the policymakers that there are legitimate concerns on each side and potentially provide some clarity on prospective escalation paths that can then be avoided.

There is also a critical potential side benefit of such a discussion about red lines and escalation paths. It can also promote healthy attention to the issue within each government. It will allow leaders to better under stand not just what the other side is thinking but also what their own agencies and related non-state entities might be doing and the potential consequences. This is something that most senior policymakers on both sides are not sufficiently focused on at present.

Plans consistent legal standards ensure successful norms while retaining policy flexibility

Bradbury 11 (Stephen, Partner, Dechert, LLP, “KEYNOTE ADDRESS: The Developing Legal Framework for Defensive and Offensive Cyber Operations” 2011, Harvard National Security Journal Symposium, Cybersecurity: Law, Privacy, and Warfare in a Digital World, 2 Harv. Nat'l Sec. J. 591)

Evolving customary law. This approach also accommodates the reality that how the U.S. chooses to use its armed forces will significantly influence the development of customary international law.

As the label implies, customary law can evolve depending on the accepted conduct of major nations like the United States. **The real-world practice of the U**nited **S**tates **in adapting the use of its military to** the new challenges raised by **computer warfare will** (and should) help **clarify the accepted customs of war in areas where the limits are not clearly established today.**

And if you just review the literature on cyber war, you quickly see that that's where we are: precisely how the laws and customs of war should apply to offensive cyber operations is not yet crystallized in key respects.

For example, there aren't always bright lines to tell us when a cyber attack on computer systems constitutes an "armed attack" or a "use of force" that justifies a nation in launching a responsive military strike under Article 51 of the U.N. Charter.

Some questions are easy: Hacking into a sensitive government computer system to steal information is an act of espionage, not an armed attack. It's clearly not prohibited by the laws and customs of war.

On the other hand, if the cyber intrusion inflicts significant physical destruction or loss of life by causing the failure of critical infrastructure, like a dam or water supply system, then it obviously would constitute an armed attack under the law of war and would justify a full military response if it could be attributed to a foreign power. Where committed as an offensive act of aggression, such an attack may violate international law.

 [\*608] If significant enough, the effect of the attack will determine its treatment, not necessarily whether the attack is delivered through computer lines as opposed to conventional weapons systems. In these cases, the laws and customs of war provide a clear rule to apply.

But there will be gray areas in the middle. Thus, it's far less clear that a computer assault that's limited to deleting or corrupting data or temporarily disabling or disrupting a computer network or some specific equipment associated with the network in a way that's not life threatening or widely destructive should be considered a use of force justifying military retaliation, even if the network belongs to the military or another government agency.

This was the case with the "distributed denial of service" attacks experienced by Estonia in 2007, which severely disrupted the country's banking and communications systems. Suspecting that Russia was behind it, Estonia suggested that NATO declare that Estonia's sovereignty had been attacked, which would have triggered the collective self-defense article of the NATO Treaty, but that suggestion was rebuffed on the ground that a cyber attack is not a clear military action. n12

There's an echo of that reasoning in Article 41 of the U.N. Charter, which says that a "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communications" is not a "measure . . . involving armed force."

And what about Stuxnet? As I understand it from public reports, Stuxnet was a computer worm that found its way into the systems controlling Iran's nuclear program and gave faulty commands causing the destruction of the centrifuges used for enriching uranium. Suppose President Ahmadinejad claimed that Israel was behind the Stuxnet worm and claimed that Stuxnet constituted an armed attack on Iran that justified a military response against Israel. I suspect the United States would disagree.

At the same time, when it comes to a cyber attack directed against U.S. computer systems, I certainly want the President to have leeway in determining whether or not to treat the attack as a use of force that supports [\*609] military retaliation. Making such judgments is a traditional power exercised by the President, and I think he retains that leeway.

Similarly, I submit, it's not clearly established that a cyber attack aimed at disrupting a server or Web site located in a neutral country or in a country outside a theater of open hostilities would be a violation of that country's neutrality.

The server might be a valid military target because it's being used for the communications or command and control of the enemy fighters in the area of hostilities (after all, al Qaeda regularly uses the Internet in planning and ordering operations). The server might have no connection to the host country's military, government, or critical infrastructure, and it might be readily targeted for a computer attack without inflicting widespread damage on unrelated systems used for civilian purposes.

Such a focused cyber operation -- with little physical impact beyond the destruction of data or the crippling of a server -- is very different from the kind of physical violation of territory -- such as a conventional troop incursion or a kinetic bombing raid -- that we ordinarily think of as constituting an affront to neutrality. n13

Although every server has a physical location, the Internet is not segmented along national borders, and the enemy may gain greater tactical advantage from a server hosted half way around the world than from one located right in the middle of hostilities.

The targeting of a server in a third country may well raise significant diplomatic difficulties (and I wouldn't minimize those), **but I don't think the law-of-war principle of neutrality** categorically **precludes the President from authorizing such an operation by an execute order to Cyber Command**.

Conclusion. So here's my thesis: To my view, the lack of clarity on certain of these issues under international law means that with respect to those issues, the President is free to decide, as a policy matter, where and [\*610] how the lines should be drawn on the limits of traditional military power in the sphere of cyberspace. For example, that means that within certain parameters, the President could decide when and to what extent military cyber operations may target computers located outside areas of hot fighting that the enemy is using for military advantage. And when a cyber attack is directed at us, the President can decide, as a matter of national policy, whether and when to treat it as an act of war.

The corollary to all this is that in situations where the customs of war, in fact, are not crystallized, the lawyers at the State Department and the Justice Department shouldn't make up new red lines -- out of some aspirational sense of what they think international law ought to be -- that end up putting dangerous limitations on the options available to the United States. Certainly, the advice of lawyers is always important, especially so where the legal lines are established or firmly suggested. No one would contend that the laws of war have no application to cyber operations or that cyberspace is a law-free zone. But it's not the role of the lawyers to make up new lines that don't yet exist in a way that preempts the development of policy. n14

In the face of this lack of clarity on key questions, some advocate for the negotiation of a new international convention on cyberwarfare -- perhaps a kind of arms control agreement for cyber weapons. I believe there is no foreseeable prospect that that will happen. Instead, the outlines of [\*611] accepted norms and limitations in this area will develop through the practice of leading nations. And **the policy decisions made by the U**nited **S**tates in response to particular events will have great influence in shaping those international norms. I think that's the way we should want it to work.

One final admonition I'll offer on the topic of offensive cyber operations: In cases where the President shapes new policy by choosing military action over covert action for a cyber operation, or vice versa, I would strongly urge that the President fully brief both sets of committees in Congress -- the Intelligence Committees and the Armed Services Committees -- and explain the basis for the choice. It's inevitable the committees will find out anyway when a jurisdictional marker is crossed, and it will help smooth the development of consistent policies and standards for the committee members and staff to understand and appreciate the choices made on both sides of the question.

## convergence adv

Advantage two is convergence

Congressional oversight gaps cause confusion and executive fights --- hampers cyber counterterror

Brennan 12 (Lt Colonel John – US Army, “United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?” 15 March 2012, Civilian Research Project; U.S. Army War College)

Although indentifying international terrorists in cyberspace is critical to successful counterterrorism operations, it is only half of the battle in bringing them to justice. Monitoring terrorists’ electronic communications is extremely important, but further work is required by the CT community to isolate, and eventually kill or capture the terrorists overseas. Manipulation or disruption of a terrorist organization’s computer networks is a potential means to this end, and it is also a possible tactic that is employed to preempt a cyber or kinetic terrorist attack.37 The laws that govern the actual manipulation of terrorists’ electronic accounts and devices in order to make them more targetable, are not explicit or simply do not exist. The primary document that gives the President of the United States the authority to conduct offensive CT cyber operations overseas is the 2001 Authorization of the Use of Military Force, which gives the president the authority to “use all necessary and appropriate force” to protect the country for further attacks.38 The extrapolation of this authority which permits the targeting of al-Qa’ida and its adherents, was employed in order to legally kill Anwar al Awlaki (an American citizen) in Yemen, and was invoked in permitting the planned (but not executed) computer network attack against his online magazine, Inspire.39

Regardless of these authorities, General Keith B. Alexander, the Commander of U. S. Cyber Command, has expressed similar misgivings as Mr. O’Connell in response to Congressional inquiries concerning the efficacy of cyber laws. During his confirmation hearings that resulted in his appointment to the post of the commander of U. S. Cyber Command in 2010, General Alexander stated that there is a, “mismatch between our technical capabilities to conduct operations and the governing laws and policies.”40

When he assumed the mantle of command of this first-ever joint and interagency cyber unit, General Alexander retained his title and position as the Director of the National Security Agency (DIRNSA). This dual command role placed him in the unique position to not only locate and intercept enemy internet communications, but to also conduct computer network attacks on the terrorists’ networks as well.41 The essence of this new command permits a more efficient cyber warfare capability which can theoretically operate seamlessly under both Titles 10 and 50 of the U. S. Code.42

With over 1.8 billion Internet users and 4.6 billion cellular phone subscribers who generate approximately 90 trillion emails per annum, the establishment of U. S. Cyber Command from within the NSA was an extremely useful beginning.43 A subordinate command to the United States Strategic Command (USSTRATCOM), Cyber Command was delegated Title 10 authority over military operations in cyberspace.44 On the other hand, Cyber Command also possesses the ability to conduct covert actions within cyber space under Title 50.45 This duplicitous legal framework is a result of current cyber policies and can create confusion over who is permitted to actually authorize a cyber operation.46 In the end, this policy friction can translate into delays while the required approvals are garnered, and could result in missing a fleeting opportunity to kill or capture a terrorist.

U. S. Computer Network Operations Policy

As a matter of current U. S. policy, the decision to label a computer network operation (CNO) as a traditional military activity (TMA), thereby falling under the purview of Title 10 of the United States Code (USC), or as a covert action under Title 50 of the USC, has spurred a great deal of discussion at the highest levels of the U. S. Government.47 Although cyber warfare is only one aspect of the overall current Title 10/50 debate that is raging within Congress and the various departments within the executive branch, one cannot legitimately discuss the policies that govern the approvals to conduct CNOs without touching upon this current source of friction.48 Much of the policy concerning the details of computer network operations is classified, but is gaining in importance such that many policy experts are speaking about it, some albeit from under the cloak of anonymity.49 As Andru E. Wall suggests, the confusion over Title 10 and Title 50 authorities appears to have, “…more to do with congressional oversight and its attendant internecine power struggles than with operational or statutory authorities,” despite the fact that by design, Title 10 and 50 authorities are mutually supporting and were not intended to be competing.50 Retired Admiral Dennis C. Blair (former ODNI) proclaimed that, “This infuriating business about who’s in charge and who gets to call the shots is just making us look muscle-bound.” ADM Blair went on to bemoan the “over-legalistic” approach to CT cyber--despite the fact that current cyber laws are woefully inadequate to address the, …”complexity of the global information network.”51(Wall 2011101)

Current media reports indicate that the use of specially-designed cyber tools in order to target states or non-state actors requires presidential approval. An example of this approval policy was seen last year when media reports indicated that the Stuxnet cyber-worm was allegedly implanted in an Iranian nuclear facility, an act that American military cyber warriors will not publicly confirm.52 This computer virus subtly attacked the computers that controlled the enormous Iranian nuclear centrifuges and caused them to self-destruct. Although the Stuxnet infestation in Natanz was a major attack with immense international political consequences, media reporting suggests that less contentious operations against terrorists’ computer networks have taken on a similarly hierarchical approval process, even though these computer network operations support the local war fighters in Afghanistan or Iraq.53 For instance, in the early years of the Iraq war, numerous attempts to hack into terrorists’ email accounts and send erroneous information from them, in order to expose other members of AQI or cause potential organizational rifts was strictly forbidden without the approval of the CENTCOM Commander.54

The reasoning behind this elevated approval policy centers upon the fact that terrorists frequently use American or allied internet service providers (ISPs) to access and manipulate the internet during the conduct of their own cyber operations.55 The consequences of this arrangement, which could ultimately involve the U. S. Government manipulating an American or allied server network in order affect a terrorist organization, makes many national leaders leery of employing the capability in the first place.56

The ongoing debate between elements of the DoD, who feel that certain cyber operations are a traditional military activity and should be governed by the laws of armed conflict and Title 10 of the U.S. Code, and leaders within the Intelligence Community (IC) who contend that any and all cyber operations are inherently covert and should be under the purview of Title 50, shows no signs of abating. An example of this conundrum occurred in June, 2010 when the U. S. was allegedly contemplating a cyber attack on Insipire Magazine.57 The U. K.’s GCHQ Intelligence Service actually conducted an attack, dubbed “Operation Cupcake” while the CIA and Cyber Command were reportedly still haggling over whether attacking the site was a traditional military activity (TMA), thereby considered a Title 10 action, or a covert action under Title 50.58 Although this operation had little kinetic effect, it was disruptive as GCHQ managed to effectively replace the bomb-making recipes on the Inspire site with actual cupcake baking recipes.59 The delay caused by the policy debate within the executive branch ultimately led to a missed opportunity. The effect of a potential delay could have been much more significant had the stakes been higher, particularly if the purpose of the proposed CT cyber operation was to thwart an impending attack.60

Another potential genesis for the policy debate is the inconsistent verbiage used between the Military and the IC when categorizing operations in cyberspace. For example, if any data within an enemy computer network is modified, then the operation is labeled a Computer Network Attack (CNA) by the military.61 The IC considers data manipulation as an Offensive Cyber Operation (OCO), a title which is much more palatable to CT lawyers than the term Computer Network Attack, even though the intent and outcome of the operations are identical.62 The differences between these labels are frequently referenced in policy debates, which ultimately slow down the process of finding and interdicting terrorists.

Effective cyber CT key to prevent multiple scenarios for terrorism

Brennan 12 (Lt Colonel John – US Army, “United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?” 15 March 2012, Civilian Research Project; U.S. Army War College)

As Al-Qa’ida and its affiliates and adherents have evolved into much more technically savvy terrorist organizations, their ability to threaten to U. S. National Security has likewise increased. The divergence between American national strategies, laws, and policies that govern counterterrorism (CT) operations within cyberspace has hampered the efforts of U. S. CT professionals to keep pace with the transformation of transnational terrorist organizations into more cyber-enabled threats.

Counterterrorism is defined as, “Actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks.”2 Due to terrorists’ heavy reliance on cyberspace, it is an operational environment which CT professionals must simultaneously dominate, and effectively deny to these shadowy groups in order to defeat them. CT cyber strategies, law, and policies provide the framework through which CT cyber professionals execute their assigned operations.

Of considerable concern is the fact that current U. S. CT cyber policies are not necessarily completely sourced in domestic or international law, and they inhibit American CT professionals from efficiently implementing the very strategies which they are charged to execute. **These restrictive and hierarchical CT cyber policies clearly hinder the ability of** strategic and operational-level military **commanders who are deployed** in support of Overseas Contingency Operations (OCO) **to manipulate cyberspace to their greatest advantage**.

In 2010 General David Petraeus, then Commander of United States Central Command (USCENTCOM) accurately described the degree to which al-Qa’ida was operating with impunity in cyberspace to finance, command, and recruit its forces.3 The tactical and operational commanders subordinate to General Petraeus in Iraq and Afghanistan often lamented that they were permitted to drop two-thousand pound bombs on terrorists’ homes, but were forced to request from USCENTCOM Headquarters, or even the Secretary of Defense, the approval to attack or manipulate terrorists’ computer networks.4 This dichotomous situation flies in the face of logic and is caused by a trifurcated divergence between: what is expected of military CT professionals in order kill or capture terrorists; what is permissible under current CT cyber law; and the current policies that actually govern offensive CT operations in cyberspace.

This work will analyze the current threat posed by international terrorist organizations from within cyberspace, as well as the inconsistencies between current national security, CT and cyber strategies, and the laws, and policies that permit CT professionals to disrupt and degrade international terrorist organizations through the use of the internet. The results of this analysis reveal that current cyber-related counterterrorism policies constrain military CT professionals, and that before CT cyber strategies can be effectively implemented, they must be in holistic alignment with cyber policies and existing statutes. Furthermore, this work proffers several recommendations concerning adjustments to current CT cyber policies that are intended to better enable more efficient CT operations, and ultimately prevent future attacks on America and its interests.

The Nature of the Cyber-terror Threat

There is conclusive and irrefutable evidence that terrorist organizations such as al-Qa’ida in Iraq (AQI) not only recruit, propagandize, coordinate attacks, and finance their activities, but these terror organizations are actively seeking the means to initiate casualty-producing kinetic events using the worldwide web as well.5 Groups such as the Muslim Hackers Club have developed their own software and tutorials in order to sabotage not only U. S. computer networks, but to also seek to cause the physical destruction of key American infrastructure.6 ADM Michael Mullen, then Chairman of the Joint Chiefs of Staff described cyber terrorism as one of two existential threats to U. S. national security, the other being the Russian nuclear threat.7 Additionally, the intelligence community (IC) writ large considers cyber attacks as the most prominent, long-term threat to the country.8 Deputy Secretary of Defense William J. Lynn III similarly suggests that terrorists are seeking to effectively weaponize cyberspace in order to achieve kinetic effects against key U. S. infrastructure.9

Speed matters in stopping potentially calamitous events, and it is of seminal importance as al-Qa’ida and its ilk continue to develop more efficient and effective methods of attack.10 Current trends indicate that terrorist organizations such as Lashkar e-Tayyibah (LeT) and al-Qa’ida in Iraq (AQI) are investing heavily in the education of select members in the fields of computer and electrical engineering.11 Ayman al Zawahiri counseled deceased AQI leader Abu Musab al Zarqawi that half of the battle for Islam should be waged on the internet and he constantly stressed to Zarqawi the importance of digital information operations.12

In order to pay for their operations, terrorist groups have begun to resort to various forms of computer-assisted robbery and identity theft. Cybercrime has become so important to financing their operations, that it now surpasses drug trafficking as a source of income to fund their operations.13 During their investigation into the 2002 Bali bombing by Jemaah Islamiyah, the Indonesian police discovered that the attack was financed through computer credit card fraud.14

More disturbing than terror financing, is the implementation of a worldwide recruiting drive, launched by al-Qa’ida in order to co-opt computer and electrical engineers who already possess advanced degrees from elite universities. Before their demise, Al-Qa’ida in the Arabian Peninsula (AQAP) leaders Anwar al Awlaki and Inspire Magazine editor-in-chief Samir Kahn were posting high-tech want ads in their jihadi circular on the internet in order to elicit acts of terror by homegrown western Muslims. The two also posted numerous want-ads to recruit individuals who possessed high-tech degrees.15 As we shall learn, **the lack of an effective U. S. CT Cyber policy prevented the timely interdiction and/or manipulation of the data on this website--action that could have been used to not only thwart AQAP’s cyber efforts, but could have been used to create physical vulnerabilities within the organization as well.**

The plots that could be hatched by heavily recruited techno-savvy terrorists are especially horrifying. Imagine if you will, the mayhem that could be unleashed by a terrorist, who using the internet, pilots multiple unmanned aircraft armed with explosive, chemical, or biological payloads. A hint of this frightening scenario came to pass when FBI foiled a plot by Rezwan Ferdaus, a young Bangladeshi-American physicist, who was arrested while in the process of developing the means to fly remote-controlled aircraft packed with explosives into the U. S. Capitol and the Pentagon.(Valencia, Milton J. and Ballou, Brian R. 2011, A1) Another terrifying possibility consists of dozens, if not hundreds of improvised explosive devices igniting simultaneously through the instantaneity of the internet. The process of perfecting this method of terrorist attack was proven to be well on its way to fruition, as was evident after the capture of numerous Al-Qa’ida in Iraq (AQI) improvised explosive device (IED) cell members. These individuals were detained while in the possession of hundreds of digital tone multi-frequency (DTMF) boards that were purported to be used to simultaneously initiate multiple IEDs to destroy U. S. and Iraqi security forces.16

Today these potential threats may seem far-fetched to some, but so did the concept of crashing jet airliners into the World Trade Center and the Pentagon prior to September 11th, 2001. These and other cyber-enabled terror plots are unfortunately far from fiction, as their perpetrators were caught in the acts of planning or executing them. The cyber terror threats which emanate from the various international terrorist organizations around the globe are of a seminal concern to U. S. national decision-makers. Though significant, the task of countering these terrorists’ threats within cyberspace is anything but insurmountable, provided that those who are charged with exposing and attacking these networks are given the latitude to act effectively. The concerns of national leaders and their desires to exploit terrorist organizations in cyberspace are clearly evident in the content of numerous past, and current national security strategy documents.

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.

And nuke terror

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.

Plan bridges the gap in congressional oversight --- resolves confusion

Stevenson 13 (Charles, PhD in Government from Harvard, Professor of American foreign policy at the Nitze School of Advanced International Studies @ Johns Hopkins, former professor at the National War College --- director of the core course on the interagency process for national security policy, worked in the executive branch including service on the Secretary of State’s Policy Planning Staff, and served for 22 years as a Senate staffer on defense and foreign policy, and member of the Project on National Security Reform and headed its working group on Congress, “Overseeing the New Ways of War” March 6, 2013, Roll Call)

There’s a lot of confusion and disagreement over how the government should manage two increasingly important techniques of waging war: drones and cyber-activities.

President Barack Obama’s current counter-terrorism adviser and nominee to head the CIA, John Brennan, says the drone operations should be largely shifted from the CIA to the Pentagon. Some lawmakers want to create a special new court to review targeted killing operations. Meanwhile, Congress has repeatedly failed to agree on how to build cybersecurity domestically, and there is no consensus on what laws should control offensive cyber-operations.

Let me suggest one overarching principle that could help us bring these new ways of war under better control.

**Congress should write a new law putting** both drone operations and **offensive cyber-operations under the** same **rules that now govern covert operations by the CIA**. That law has two key features: a formal decision by the President, called a “finding,” and notification of a small group of members of Congress.

That law has worked pretty well since it was first enacted in 1974. Presidents have to be persuaded that the operation is well-designed and important to carry out, and Congress is informed so that it can exercise oversight on behalf of the American people. On occasion, covert actions have been modified or cancelled in response to congressional concerns. This kind of oversight is better than what a court could do, because courts judge only issues like due process, not the strategic and political factors that routinely confront the executive and legislative branches.

Right now, drone operations are conducted in a crazy bifurcated system. Those done by the CIA are regularly reviewed by the intelligence committees. Those done by the Pentagon are reportedly eventually briefed to the congressional defense committees, but there is no regular and required process as there is for the CIA operations.

The situation becomes especially murky when both the CIA and the Pentagon are conducting drone operations in the same area, as in Yemen, or when the CIA and the Joint Special Operations Command work together, as in the bin Laden raid. The Pentagon operates under laws called Title 10 of the U.S. Code, while the CIA is controlled by the **war powers provisions** of Title 50. What **we need** is a “Title 60” **to bridge the gaps**.

**Otherwise, a devious executive could assign tasks to the Pentagon** precisely **to escape notification and oversight**. Or the compartmentalization that necessarily surrounds sensitive operations could lead to conflicts in the field.

There are always risks of leaks when the circle of knowledgeable officials widens. But even in the case of the bin Laden raid, where the secrecy held, CIA Director Leon E. Panetta notified the intelligence committees in a general way months in advance.

The case for a “Title 60” process for drone operations is even stronger if the administration adopts Mr. Brennan’s suggestion to move most CIA drone operations to Pentagon control.

Offensive cyber-operations would also be best handled under a similar legal process. CIA-run operations are already covered, but the Pentagon has created a new Cyber Command that could carry out large-scale cyber operations. And the administration has reportedly concluded that the President has broad power even to launch a pre-emptive cyber-strike to thwart an impending digital attack from abroad.

If the circumstances are that dire, I suppose most Americans would support such an action. But the way to limit abuses, and be sure that there is careful consideration **beforehand and** accountability **afterward**, is for the President himself to make the final decision and for a designated group in Congress to be notified as soon as possible.

If Congress ever resolves its disagreements over domestic cybersecurity and passes some kind of law, I hope it also would include a provision requiring congressional notification and oversight if the President ever chooses to use special authorities to compel compliance with security directives.

Do drone and cyber-operations have to be reported to Congress every time? **Will a reporting requirement prevent timely action?**

**The** concerns are overblown because the experience with CIA covert operations has worked in practice, despite occasional complaints.

And the frequency issue can easily be solved by a simple rule: if the President has to decide under the executive branch’s own rules, then the matter is important enough that the Congress should be notified.

Only the plans committee resolves perceived and actual convergence issues

Wall 11 (Andru, Senior Associate with Alston & Bird LLP; former senior legal advisor for U.S. Special Operations Command Central from 2007 to 2009, “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action” 2011, Harvard National Security Journal, Vol. 3, p. 85 – 142)

8 . Congressional Oversight

Confusion over Title 10 and Title 50 authorities has more to do with congressional oversight and its attendant internecine power struggles than with operational or statutory authorities. Operators, be they special operations forces (SOF) operating under Title 10, CIA agents operating under Title 50, or NSA personnel operating under both Title 10 and Title 50, know from whence their authorities are derived. The operators recognize dual lines of authority and are primarily concerned with coordination and deconfliction. To outsiders looking in. such as a Senator in Washington. DC, the activities performed by SOF and CIA operatives, especially during periods preceding possible or anticipated conflict, may appear virtually indistinguishable. Yet similarity in no way vitiates their dual lines of authority, nor does it create great challenges for operators.

A former general counsel of the CIA. Jeffrey H. Smith, spoke of what he perceived as a "dichotomy between Title 10 and Title 50" that gives "executive branch lawyers and members of Congress . . . headaches."54 These headaches arise, Smith stated, during debates over military activities called "preparation of the battlefield." which are activities typically carried out by military personnel "in close collaboration with the U.S. intelligence community."55 We will examine these activities more closely in Parts III and IV. Smith, however, summarizes the issue as such: if the activity is defined as a military activity "Title 10") there is no requirement to notify Congress, while intelligence community activities ("Title 50"; require presidential findings and notice to Congress.56 The natural inclination for executive branch lawyers, according to Smith, is to prefer the Title 10 paradigm to obviate congressional notification requirements.57

This perception—that the Executive Branch is deliberately Irving to avoid congressional oversight—naturally riles the intelligence committees. In its report accompanying the Intelligence Authorization Act for Fiscal Year 2010, the House Permanent Select Committee on Intelligence noted "with concern the blurred distinction between the intelligence-gathering activities carried out by the Central Intelligence Agency (CIA) and the clandestine operations of the Department of Defense."58 The Committee accused DoD of labeling its clandestine activities as operational preparation of the environment OPE in order to justify them under Title 10 and avoid oversight by the intelligence committees "and the congressional defense committees cannot be expected to exercise oversight ovitside of their jurisdiction."59 The Intelligence Committee apparently perceives an oversight lacuna, yet no such lacuna exists. Rather, all activities condvicted under Title 10 authorities are subject to oversight by the armed services committees and. for example, commanders of special operations forces regularly brief the armed services committees on their clandestine activities.



As illustrated by Figure 1, the congressional intelligence committees exercise oversight of intelligence activities, while the armed services committees exercise oversight jurisdiction over military operations.60 The congressional oversight is not coterminous with statutory authorities, as Title 10 includes authority for the Secretary of Defense to engage in both intelligence activities and military operations. Congressional oversight overlaps when non-DoD elements of the intelligence community provide support to military operations and in the unlikely or at least rare instance where the President directs elements of DoD to conduct covert action.61

Oversight would also overlap with respect to intelligence activities carried out by an element of the intelligence community in support of a military operation authorized under Title 10.

Congressional oversight of the military is straightforward: both the Senate and House Armed Services Committees exercise jurisdiction over all aspects of DoD and matters relating to “the common defense.”62 Defense authorization bills originate in the armed services committees, where they must be approved before consideration by the full Senate or House. Problems arose in the wake of 9/11 as DoD expanded its intelligence capabilities in order to support ongoing military operations, and the intelligence committees correspondingly sought to expand their jurisdiction in an attempt to bring all military intelligence collection efforts within their purview, which created clashes with the armed services committees and the Executive Branch and generated debates over appropriate congressional oversight.

Congressional oversight of intelligence activities is considerably more complex. The National Security Act of 1947, which created the CIA, did not include statutory congressional oversight provisions. For nearly thirty years, Congress exercised little oversight of intelligence activities. This changed dramatically, however, following revelations in 1974 by then New York Times reporter Seymour Hersh that U.S. intelligence agencies engaged in domestic spying.63 The Church Committee’s subsequent investigation “did nothing less than revolutionize America’s attitudes toward intelligence supervision.”64

The Senate established its Select Committee on Intelligence (SSCI) in 1976 and the House followed suit a year later with its Permanent Select Committee on Intelligence (HPSCI). The era of benign neglect was over, replaced instead by dynamic if often dysfunctional congressional oversight. In 1980 Congress mandated for the first time that the Director of Central Intelligence and the heads of all other U.S. departments and agencies “involved in intelligence activities” keep the intelligence committees “fully and currently informed of all intelligence activities.”65 This provision was repealed in 1991 and responsibility for informing the congressional intelligence committees of all intelligence activities, including anticipated activities, was placed directly on the President.66

The intelligence committees exercise broad oversight of the intelligence community. They exercise exclusive authorizing powers for the CIA, the Director of National Intelligence, and the National Intelligence Program.67 They share jurisdiction of DoD intelligence components with the Senate and House armed services committees.

While the jurisdictions of the Senate and House intelligence committees are nearly identical, HPSCI exercises broader jurisdiction in two significant respects: HPSCI uses a much broader definition of intelligence activities and adds oversight of “sources and methods.”68 SSCI exercises jurisdiction over “intelligence activities,” while HPSCI exercises jurisdiction more broadly over “intelligence and intelligence-related activities . . . including the tactical intelligence and intelligence-related activities of the Department of Defense.”69 The House gives “intelligence and intelligence-related activities” this all-encompassing definition:

[The] collection, analysis, production, dissemination, or use of information that relates to a foreign country', or a government, political group, party, military force, movement, or other association in a foreign country, and that relates to the defense, foreign policy, national security, or related policies of the United States and other activity in support of the collection, analysis, production, dissemination, or use of svich information.70

Thus, the House of Representatives via a rule change gave HPSCI oversight of "intelligence-related activities" including "tactical intelligence" and other military information collection activities for which congressional notification is not statutorily mandated. This would be understandable if HPSCI controlled authorizations for those military activities, but it does not. All authorizations for these military activities originate in the House Armed Services Committee and House rules do not provide for their review by the intelligence committee. In fact, just the opposite occurs as all intelligence authorization bills passed by the intelligence committees must then clear the armed services committees before being considered by the full House.

Intelligence committee oversight is weakened by the bifurcated authorization and appropriations processes. Because most appropriations for intelligence activities are included as a classified section of the annual defense appropriations bill, "the real control over the intelligence purse lies with the defense subcommittees of the House and Senate Appropriations Committees."71 The 9/11 Commission recognized how "dysfunctional" this arrangement is in practice and recommended the establishment of a single joint intelligence committee with authorizing and appropriating authorities.72 Congress, to its detriment, has not adopted this recommendation.

Intelligence committee oversight is further weakened by the failure to enact an intelligence authorization bill for five of the past six years. Title 50 prohibits the expenditure or obligation of appropriated funds on intelligence or intelligence-related activities unless "these funds were specifically authorized by Congress for such activities."71 Congress meets this "specifically authorized" provision through the vise of a catch-all provision inserted into the defense appropriations acts.74 Over the past 30 years. Congress enacted an intelligence authorization bill prior to the start of the fiscal year on just two occasions—1983 and 1989.

Congress could end the Title 10-Title 50 debate by simply reforming its oversight of military and intelligence activities and align oversight with the statutory authorities. Rather than focus on what the activity in question looks like what is being done). Congress should simply ask who is funding the activity and who is exercising direction and control; oversight should be aligned in the House and Senate and should correspond to funding. direction and control. Congress should adopt the recommendations of the 9/11 Commission—align congressional oversight with statutory avithorities and reform its bifurcated intelligence authorization and appropriations functions—and thereby eliminate most real and perceived Title 10-Title 50 issues. With the crux **of the Title 10-Title 50 debate exposed as dysfunctional congressional oversight**, this article now turns to explaining why some military and intelligence activities look alike, yet remain distinguishable.

## plan

The United States federal government should restrict executive authority for offensive cyber operations to those authorized by a Joint Congressional Consultation Committee.

## solvency

AFF creates Joint Congressional Consultation Committee to authorize OCOs

Chen 12 (Julia – JD Candidate @ Boston College (2013) specializing in National Security, MEM in Engineering Management from Old Dominion, BA – Rice University, “NOTE: RESTORING CONSTITUTIONAL BALANCE: ACCOMMODATING THE EVOLUTION OF WAR” November, 2012, 53 B.C. L. Rev 1767)

The War Powers Resolution was an attempt to check unbounded executive war power, but it was clearly written for a 1973-era war. n327 Technological innovation and the changing face of warfare have evolved to put modern military actions outside the scope of the Resoltion. n328 [\*1800] The result of this evolution is nearly unbounded war powers for the executive branch. n329 Nonetheless, modern military actions should be subject to the system of checks and balances established in the Constitution. n330 Without this political dialogue, the executive could spend millions of dollars, endanger American lives, and embroil the nation in international disputes more easily. n331 As stated by George Mason, the constitutional check should "clog" rather than facilitate war, and guarantee that decisions are made in the best interests of the nation. n332 To ensure a broader congressional role and achieve the appropriate balance of war powers, a new statutory framework is needed. n333

B. Proposed Amendment to the War Powers Resolution

Congress should draft framework legislation to formalize its role in the decision to enter a war, thereby restoring the balance of powers contemplated by the Framers. n334 As noted above, when the President makes war powers decisions in the absence of congressional action, the decisions are in Justice Robert Jackson's "zone of twilight" and are of dubious constitutionality. n335 Passing new legislation mandating that the President consult with Congress--and obtain approval or disapproval--would solidify the constitutionality of war-making decisions. n336 The President's decision would thus fall within either Justice Jackson's first or third categories, which would clarify or strengthen the constitutionality of the executive action. n337

In 2008, the National War Powers Commission proposed new legislation, the War Powers Consultation Act of 2009. n338 This proposed legislation would clarify some of the issues that limit the effectiveness of the [\*1801] War Powers Resolution of 1973, and would require Congress to act affirmatively in response to presidential war powers decisions. n339 Although this proposal was a step in the right direction, the proposal requires further modification to encompass the full reality of modern warfare. n340 The modifications proposed below will ensure that the new law has sufficient breadth to encompass all conflicts regardless of the actors. n341 Furthermore, the modifications incorporate a bifurcated process to accommodate the realities of fighting modern wars, which rely on covert actions. n342 These proposed reforms bring the balance of power between the executive and legislative branches more closely in line with the Framers' intent and more thoroughly accommodate the realities of modern warfare. n343

1. Revise the Scope of War Powers Legislation

The scope of actors that fall within the War Powers Consultation proposal should be broadened. n344 The proposal currently is limited to "combat operation[s] by U.S. armed forces." n345 The legislation should be more expansive, and closer to the reality of modern war fighting, which is conducted by many actors in addition to the military. n346 This change could be accomplished by omitting the words "armed forces." n347 Therefore, the scope of the legislation should be modified to encompass "any combat operation by the United States." n348 This change to the proposed legislation would encompass military, government civilians, contractors, UAVs, and other technological innovations that act on behalf of the nation. n349

 [\*1802] The scope of conflicts that fall within the War Powers Consultation proposal should also be broadened. n350 The proposed legislation currently applies to "any conflict expressly authorized by Congress, or . . . combat operations lasting more than a week or expected by the President to last more than a week." n351 On the one hand, this proposal would encompass the 2011 action in Libya. n352 On the other hand, it would not encompass short-duration, high-impact strikes, such as the cyber-attack launched against Estonia in 2007. n353 Although an action may be of short duration, it may have long-term effects, and it may have sufficient force to profoundly affect the United States in the form of money, personnel, or foreign relations. n354 Thus, language should be added to the proposed legislation to make it applicable to all offensive strikes. n355 This expansion would add scenarios that are likely to instigate reprisal against America. n356 Therefore, this modification would force the President to explain to Congress why a fight is worth starting and why it is in the national interest. n357 Furthermore, this change would still allow the executive to act unilaterally to defend the country against attacks, and would ensure the balance between the political branches intended by the Framers. n358

2. Bifurcation of the Oversight Process

To check effectively the President's war power, Congress should divide the process of congressional oversight so it is tailored to address both open and covert warfare. n359 The War Powers Consultation proposal specifically exempts "covert operations" from its scope. n360 Nonetheless, "covert operations" are a significant element of modern warfare. n361 Covert actions should therefore not be exempt from legislation [\*1803] that governs war powers, because the Constitution envisions a role for both the Congress and the President in the decision to enter a war. n362

The Commission's proposed legislation calls for creation of a Joint Congressional Consultation Committee. n363 This Committee would be composed of the minority leaders of the House and Senate, the majority leader of the Senate, the Speaker of the House, and the chairs and ranking members of the Senate and House committees on foreign affairs, armed services, intelligence, and appropriations. n364 Thus, the Committee closely mirrors the requirements of the existing congressional oversight committees on intelligence. n365 The proposed legislation should be amended so that all intended acts of war by the executive, including open and covert actions, are initially referred to this Committee. n366

For non-covert operations, the War Powers Consultation proposal outlines a process for congressional oversight. n367 The President is required to have meaningful consultation with the Committee, rather than just notification. n368 This consultation must occur prior to the conflict, or in emergent circumstances, within three calendar days after operations begin. n369 The proposal also requires that Congress act to approve or disapprove of the action. n370 If Congress has not acted on its own accord, the Committee is required to "introduce an identical concurrent resolution in the Senate and House." n371 This process would result in meaningful consultation between the President and Congress, and would mandate that Congress act to check the President's power when appropriate. n372

This proposed legislation should be modified so that in situations that require covert operations, the process would be modeled on the [\*1804] Intelligence Oversight Act of 1991. n373 In these situations, the Joint Congressional Consultation Committee would assume an analogous role to the existing Senate and House intelligence committees. n374 Thus, the members of the Committee could engage in fully informed consultation with the President, rather than being limited to the discussion of only non-covert actions. n375 Following the model of the Intelligence Oversight Act of 1991, the process for covert operations should require the President to make a finding in writing within forty-eight hours of making the decision to conduct the action. n376 In addition, the action could commence prior to notification, but notification must follow soon afterward. n377 Furthermore, in a written finding the President should specify "each department, agency, or entity of the United States Government authorized to fund or otherwise participate in any significant way in such action." n378 The finding must also identify any third parties that are not employed by the government that are to be involved with the action. n379 This statement will give members of Congress the full picture of what forces are involved in the activity. n380

Upon receipt of this finding from the President, the Committee must have an affirmative requirement to balance the power of the executive. n381 It should first be required to make a finding as to whether the action truly requires secrecy or should be discussed with the full Congress. n382 If the Committee finds that the action is of a nature that requires secrecy, it should remain in the Committee for debate. n383 Conversely, if the Committee finds that there is no need for secrecy, it should consult accordingly with the executive and, if appropriate, treat the information as an open conflict. n384

Once the Committee makes a finding that the conflict is covert and should be kept secret, it must be further debated within the Committee. n385 [\*1805] Furthermore, the executive should be required to keep the Committee apprised of the conflict and provide periodic written updates. n386 This exchange would give Congress the opportunity to check the power of the President, and prevent the tyranny that the Framers so feared. n387 Additionally, it would enable Congress to balance the power of the executive and make informed decisions on defense appropriations. n388

These recommended modifications to the proposed War Powers Consultation Act of 2009 would make it match the realities of modern warfare. n389 Expanding its scope to include all of the actors that contribute to modern warfare, and all of the actions with the effects of warfare, would strike the appropriate balance of war powers between the executive and legislative branches. n390 This balance is necessary to ensure not only that the executive can adequately defend the nation, but also that both the executive and legislative branches are accountable to the people who pay the price of governmental decisions. n391

CONCLUSION

The Constitution's system of checks and balances gave both the President and Congress powers over war. The War Powers Resolution of 1973 was an attempt by Congress to reassert its constitutional prerogative and implement a formal structure for the division of power with the President. Forty years later, modern warfare has evolved sufficiently to render the War Powers Resolution ineffective. Thus, Congress should replace the War Powers Resolution with a new, more pragmatic [\*1806] statute aligned with the realities of modern warfare. The new statute should incorporate elements of the proposed War Powers Consultation Act of 2009 and the existing Intelligence Oversight Act of 1991. Moreover, its scope should be expansive, to encompass all actors and all actions of modern warfare. Such an approach will ensure real checks and balances and political accountability in the realm of war powers.

Plans statutory clarity develops cyber doctrine --- congressional signal is key

Waxman 10/1/13 (Matthew Waxman is a law professor at Columbia Law School, where he co-chairs the Roger Hertog Program on Law and National Security. He is also Adjunct Senior Fellow for Law and Foreign Policy at the Council on Foreign Relations and a member of the Hoover Institution Task Force on National Security and Law. He previously served in senior policy positions at the State Department, Defense Department, and National Security Council. After graduating from Yale Law School, he clerked for Judge Joel M. Flaum of the U.S. Court of Appeals and Supreme Court Justice David H. Souter, “The Constitutional Power to Threaten War” Forthcoming in YALE LAW JOURNAL, vol. 123, 2014, October 1st DRAFT) **\*\*Footnote 213 included**

A second argument, this one advanced by some congressionalists, is that stronger legislative checks on presidential uses of force would **improve deterrent and coercive strategies** by making them more selective and credible. The most credible U.S. threats, this argument holds, are those that carry **formal approval by Congress**, which reflects strong public support and willingness to bear the costs of war; requiring express legislative backing to make good on threats might therefore be thought to enhance the potency of threats by encouraging the President to seek congressional authorization before acting. 181 A frequently cited instance is President Eisenhower’s request (soon granted) for standing congressional authorization to use force in the Taiwan Straits crises of the mid- and late-1950s – an authorization he claimed at the time was important to bolstering the credibility of U.S. threats to protect Formosa from Chinese aggression. 182 (Eisenhower did not go so far as to suggest that congressional authorization ought to be legally required, however.) “It was [Eisenhower’s] seasoned judgment … that a commitment the United States would have much greater impact on allies and enemies alike because it would represent the collective judgment of the President and Congress,” concludes Louis Fisher. “Single-handed actions taken by a President, without the support of Congress and the people, can threaten national prestige and undermine the presidency. Eisenhower’s position was sound then. It is sound now.” 183 A critical assumption here is that legal requirements of congressional participation in decisions to use force **filters out unpopular uses of force**, the threats of which are unlikely to be credible and which, if unsuccessful, undermine the credibility of future U.S. threats.

A third view is that legal clarity is important to U.S. coercive and deterrent strategies; that ambiguity as to the President’s powers to use force undermines the credibility of threats. Michael Reisman observed, for example, in 1989: “Lack of clarity in the allocation of competence and the uncertain congressional role **will sow uncertainty among those who depend on U.S. effectiveness for security and the maintenance of world order**. Some reduction in U.S. credibility and diplomatic effectiveness may result.” 184 Such stress on legal clarity is common among lawyers, who usually regard it as important to planning, whereas strategists tend to see possible value in “constructive ambiguity”, or deliberate fudging of drawn lines as a negotiating tactic or for domestic political purposes. 185 A critical assumption here is that clarity of constitutional or statutory design **with respect to decisions about force exerts significant effects on** foreign perceptions of U.S. resolve **to make good on threats, if not by** affecting the substance of U.S. policy **commitments with regard to force then by pointing foreign actors to the appropriate institution or process for reading them.**

Political scientists almost never engage directly on these questions of constitutional design and reform (it is difficult, in fact, to find even passing references to questions of legal doctrine or reform in political science scholarship on threats of force). Partly this may reflect a general scholarly disposition favoring descriptive over normative or prescriptive analysis - the opposite of most American legal scholarship. Partly, though, it also reflects a difference in emphasis between legal scholars and political scientists with respect to democratic institutions. Whereas legal scholars tend to focus on formal legal powers and checks - such as binding legislative control and judicial review -political scientists focus on the political interactions that these institutions facilitate rather than the specific allocations of power among different institutions themselves.186 In other words, they tend to concentrate on the allocation of powers between branches of government only to the extent that such arrangements formalize or provide a forum for political contestation and competition among domestic political opponents. As a result, political scientists rarely examine how the sorts of constitutional and legislative reforms so often put forward by legal thinkers would affect the credibility of threats.

That said, political science contributions in this area suggest that all three views that have appeared in legal debates probably have some truth in some cases, but all three are also exaggerated. They are exaggerated to the extent that they fail to account for the political checks imposed by Congress that presidents already internalize and that foreign actors already perceive; they tend to consider formal legal checks in absolute terms rather than their marginal effects relative to baseline politics, which operate quite robustly as constraints.

Furthermore, anv reading of signals b> foreign audiences would have to take account of the possibility that a President might act outside the law. especially in a grave national security crisis. On balance and in general, though, the political science scholarship surveyed above suggests that a result of stronger formal congressional cheeks on force would probably be restricted reliance on threatened force, but the ensuing would in turn be more credible.

Even if Congress already wields informal political influence over threatened force, more potent and formal requirements of legislative force authorization or stricter enforcement of existing ones would still probably push U.S. policy a narrower set of commitments and more reserved use of threats - a more selective coercive and deterrent strategy - in several ways. For a President, knowing that he requires legally authorization from Congress to carry through on threats raises the expected political costs of making them (even very popular ones would require spending some political capital to obtain formal legislative backing). A more formal and substantial role for Congress in authorizing the carrying out of threats would also probably amplify some of the informational effects of executive-legislative dialogue and congressional debate described in the previous section: these processes - which could become more robust and attract greater attention - make it difficult to conceal or misrepresent preferences about war and peace, and therefore reduce opportunities for bluffing. If stronger legislative checks on war and force likely mean a more narrowly selective policy of threatened force, then the previous sections' analysis also suggests that the credibility of those select threats will probably be enhanced Returning to the Iran example with which this Article began, for example, a Presidents decision to draw a red-line threat would likely send an even more potent signal of resolve if legislation were required ultimately required to carry it out. because it would more clearly communicate likely inter-branch unity behind the threat. As the next Part will explain, whether more narrowly selective - but perhaps more credible - threats would result in an overall improvement from a policy standpoint depends on shifting geopolitical context and other balances in U.S. strategy.

The general point here is that the ultimate effects of any legal reform on war and peace will depend not just on the internal effects on U.S. government decision-making but the external perceptions of actors reading U.S. signals. An agenda for constitutional scholars and political scientists alike would more thoroughly link different internal legal arrangements within democracies to different strategies for using military power, some aspects of which arc outlined in the next Part. One question for future study of interest to both political scientists and legal scholars, for example, is whether Congress is as institutionally suited or inclined as the executive branch to consider the credibility effects of threatened or actual military actions in one case on other or future cases - that is. To take account of and give substantial weight to the signals it sends to other international actors with grants or denials of authorization to use force. A related question critical to considering possible legal reform is whether Congress's inclinations in that regard would shift were it to assume a more significant and sustained formal role in decision-making about war and force - that is. whether any such congressional policy biases are structurally inherent or a function of reigning legal doctrine

III. Constitutional War Powers and American Grand Strategy

One broad implication of this analysis is that the true allocation of constitutional war powers is - in anything but a formalistic sense - geopolitically and strategically contingent. It is often believed that the power to go to war is one of the most important constitutional powers because wars put American blood and treasure at risk.187 But even assuming as a normative matter that this means that our Constitution should be structured to be war-averse, as some constitutional scholars have argued,188 this principle does not provide as much guidance about legal doctrine as often supposed unless integrated with ideas about how the United States can and should pursue that agenda in relation to other actors pursuing theirs and amid a changing international context.

A. Threats of War and Presidential Powers in Historical and Strategic Context

Thinking generally about the "powers of war and peace/" the power to decide to go to war was a much more significant one relative to the power to threaten war - as well as other foreign relations powers - when the United States was a small, militarily-weak power and when our strategy was avowedly to stay out of foreign disputes, or when coercive diplomacy and deterrence that extended to protecting distant allies abroad was not a serious strategic option.189 If a major component of grand strategy is hiding behind geographical barriers and avoiding conflict by not taking sides in disputes among other powers - as it was during the infancy of the Republic and as it was again in the interwar years - then the power to threaten war is not often very consequential and an allocation of powers that makes it difficult to engage in military conflicts or even threaten to do so is consistent with that strategic vision.' Note. too. that the lack of a very potent standing military force during these periods limited options for coercive and deterrent strategies and made the President heavily dependent on Congress to furnish the means to initiate

Because the importance for the United States of threatened force - to coerce or deter adversaries, and to reassure allies - in affecting war and peace grew so substantially after World War II. the constitutional decision-making about using force has been relegated in large degree to a mechanism for implementing grand strategy rather than setting it.192 As a superpower that plays a major role in sustaining global security, threatening war is in some respects a much more policy-significant constitutional power than the power to actually make war.

Moreover, assessing the functional benefits or dangers attendant to unilateral presidential discretion to use force or to formulas for ensuring congressional involvement cannot be separated from the means by which the United States pursues its desired geopolitical ends. Of course those merits are inextricably linked to substantive policy ends associated with its military capacity, such as whether the United States is pursuing an aggressively expansionist agenda, a territorially-defensive one. or something else But it also depends on how it seeks to wield its military power - as much its potential for armed force as its engagement of the enemy with it - toward those ends.

B. Re framing "War Powers" Scholarship

One might object to the main point of this Article - that constitutional allocations of power to use force cannot meaningfully be assessed either descriptively or normatively in other than very formalistic ways without accounting for the way U.S. military power is used - that it falls victim to its own critique: if the American condition of war and peace is determined by more than just decisions to commence hostilities or resist actual force with force, why stop at threats of war and force'' Why not extend the analysis even further, to include the many other presidential powers - like diplomatic communication and recognition, intelligence activities, negotiation, and so on - that could lead also to or affect the course of events in crises?193

This Article has focused on the way presidents wield U.S. military might not because analysis of those powers can be neatly separated from other ones but to show how even widening the lens a little bit reveals a much more complex interaction of law and strategy then often assumed and opens up new avenues for analysis and possible reform Military force is also an important place to start because it has always carried special political and diplomatic salience.194 Moreover, many types of non-military moves a President might take to communicate threats, such as imposing economic sanctions or freezing financial assets.195 rest on express statutory delegations from Congress.196 Military threats, by contrast, often rest primarily on the President's independent constitutional powers, perhaps buttressed by implicit congressional assent, and therefore pose the most fundamental questions of constitutional structure and power allocation in relation to strategy

A next step, though, would incorporate into this analysis other instruments of statecraft, such as covert intervention or economic and financial actions, recognizing that their legal regulation could similarly affect perceptions about U.S. power abroad as well as the political and institutional incentives a President has to rely on one tool versus another. Moreover, sometimes coercive strategies involve both carrots and sticks -threats as well as positive inducements197 - and Congress's powers may be dominant with regard to the latter elements of that formula, perhaps in the form of spending on offered benefits or lifting of economic sanctions.198 Further study might focus on such strategies and the way they necessarily require inter-branch coordination, not only in carrying out those elements but in signaling credibly an intention to do so.

At this point, many legal scholars reading this (yet another) Article on constitutional war powers are bound to be disappointed that it proposes neither a specific doctrinal reformulation nor offers an account of optimal legal-power allocation to achieve desired results One reason for that is that evidence surveyed in Part II is inconclusive with respect to some key questions. Another, however, is that the very quest for optimal allocation of these powers is generally mis-framed, because "optimal" only makes sense in reference to some assumptions about strategy, which are not themselves fixed By tying notions of optimal legal allocations to strategy I do not simply mean the basic point that we need prior agreement on desired ends (in the same sense that economists talk about optimality by assuming goals of maximizing social welfare), but the linking of means to ends. As the Article tries to show throughout, even if one agrees that the desired ends are peace and security. there are many strategies to achieve it - isolation, preventive war. deterrence, and others - and variations among them, depending on prevailing geopolitical conditions.

A more productive mode of study, then, recognizes the interdependence of the allocation of war-related powers and the setting of grand strategy. Legal powers and institutions enable or constrain strategies, and they also provide the various actors in our constitutional system w ith levers for shaping those strategies. At the same time, some strategies either reinforce or destabilize legal designs.

C. Threats, Grand Strategy, and Future Executive-Congressional Balances

Having homed in here on threatened war or force, one might take from this analysis yet another observation about the expanding or constitutionally "imperial" power of the U.S. President. That is, beyond the President's wide latitude to use military force abroad, he can take threatening steps that could provoke or prevent war and even alter unilateral the national interests at stake in a crisis by placing U.S. credibility on the line -the President's powers of war and peace are therefore even more expansive than generally supposed

It is also important to see this analysis, however, as showing more complex dependency of presidential powers on Congress with respect to setting and sustaining American grand strategy. In that respect, Philip Bobbitt was quite correct when he decried lawyers' undue emphasis on the Declare War clause and the commencement of armed hostilities as the critical legal events in thinking about constitutional allocations and U.S. security policy:

Wars rarely start as unexpected ambushes; they are usually the culmination of a long period of policy decisions. & If we think of the declaration of war as a commencing act - which it almost never is and which the Framers did not expect it to be - we will not scrutinize those steps that bring us to war, steps that are in the main statutory in nature. Moreover, we will be inclined to pretend & that Congress really has played no role in formulating and funding very specific foreign and security policies.199

Those foreign and security policies to which Bobbitt refers include coercive and deterrent strategies.

Indeed- it is important to remember that the heavy reliance on threatened force especially after World War II has itself been a strategic choice by the United States - not a predestined one - and one that could only be made and continued with sustained congressional support. Since the beginning of the Cold War period, the reliance on deterrence and coercive diplomacy became so deeply engrained in U.S. foreign policy that it is easy to forget that the United States had other strategic options open to it. One option was war: some senior policy-makers during the early phases of the Cold War believed that conflict with the Soviet Union was inevitable, so better to seize the initiative and strike while the United States held some advantages in the balance of strength. Another option was isolation: the United States could have retracted it security commitments to its own borders or hemisphere, as it did after World War I, ceding influence to the Soviet bloc or other political forces/01 These may have been very bad alternatives, but they were real ones and they were rejected in favor of a combination of standing threats of force and discrete threats of force - sometimes followed up with demonstrative uses of force - that was only possible with congressional buy-in. That buy-in came in the form of military funding for the standing forces and foreign deployments needed to maintain the credibility of U.S. threats, as well as in Senate support for defense pacts with allies. While a strategy of deterrent and coercive force has involved significant unilateral discretion as to how and when specifically to threaten military action in specific crises and incidents, the overall strategy rested on a foundation of executive-congressional collaboration and dialogue that played out over decades.

Looking to the future, the importance of threatened force relative to other foreign policy instruments will shift - and so, therefore, will the balance of powers between the President and Congress. United States grand strategy for the coming decades will be shaped by conditions of fiscal austerity, for example, which may mean cutting back on some security commitments or reorienting doctrine for defending them toward greater reliance on less-expensive means (perhaps such as a shift from large-scale military forces to smaller ones, or **greater reliance on high-technology**, or even revised doctrines of nuclear deterrence).

One possible geostrategic outlook is that the United States will retain its singular military dominance, and that it will continue to play a global policing role. Another outlook, though, is that U.S. military dominance will be eclipsed by other rising powers and diminished U.S. resources and influence." The latter scenario might mean that international relations will be less influenced by credible threats of U.S. intervention, and perhaps more so by the actions of regional powers and political bodies, or by institutions of global governance like the UN Security Council." These possibilities could entail a practical rebalancing of powers wielded by each branch, including the pow er to threaten force and other foreign policy tools.

Were the United States to retreat from underw riting its allies' security and some elements of global order with strong coercive and deterrent threats, one should expect different patterns of executive-congressional behavior with respect to threatening and using force, because wars and threats of wars will come about in different ways: less often as a breakdown of U.S. hegemonic commitments, for example. Reduced requirements of maintaining credible U.S. threats, and therefore reduced linkage between U.S. actions in one crisis and others, would also likely reduce pressure on the President to protect prerogatives to threaten force and to make good on those threats. A foreign policy strategy of more selective and reserved military engagement would likely be one more accommodating to case-by-case, joint executive-legislative deliberation as to the threat or use of U.S. military might, insofar as U.S. strategy would self-consciously avoid cultivating foreign reliance on U.S. power.

Besides shifting geostrategic visions, ranging from a global policing role to receding commitments, the set of tools available to Presidents for projecting power will evolve, too, as will the nature of security threats, and this will produce readjustments among the relative importance of constitutional powers and inter-branch relations.

Transnational terrorist threats, for example, are sometimes thought to be impervious to deterrent threats, whether because they may hold nihilistic agendas or lack tangible assets that can be held at risk. 06 Technologies like unmanned drones may make possible the application of military violence with fewer risks and less public visibility than in the past/ While discussion of these developments as revolutionary is in vogue, they are more evolutionary and incremental; their purported effects are matters of degree. Such developments will, however, retune strategies for brandishing and exercising military capabilities and the politics of using them.

Whatever the future of U.S. power and strategies for wielding it, the analysis above points toward **a revised war powers reform agenda**. If legal discourse of war powers is too narrowly focused on actual wars and forceful military engagements to the exclusion of threats of them, then so too is discussion of reforms too narrowly focused on congressional involvement at the end stages of coercive diplomacy - often long after threats have been issued and responded to, positively or negatively - rather than at earlier ones.

A more productive agenda (and by no means a mutually exclusive one) would focus on strengthening Congress's role in the shaping of U.S. grand strategy more broadly - that rather than devoting its institutional energy to reasserting it control over decisions to engage the enemy with military force in particular circumstances, it would work to engage the executive branch more seriously and continually on the general policy circumstances under which force might be contemplated. This would mean Congress doing something it is not disposed toward, which is using its other powers - such as hearings, control of funds,statutory delegations of bounded policy discretion - to engage the executive branch on strategic questions inadvance of or at the earliest stages of crises about the way force may be wielded**. Proposals to restructure congressional national security committees - such as creating more** consolidated, joint House-Senate national security committee, to give them more leverage, expertise, and oversight responsibility that ties together the elements of U.S. power **213 213 See KOH, supra note , at 167-68; NATIONAL WAR POWERS COMMISSION REPORT 36-37 (2008). -** should be viewed not simply as a means for consulting with the Executive once large-scale military intervention is imminent, but for consulting on the matching of foreign policy means and ends well in advance of crises.

Congress signals strong legal foundation – key to international acceptance

Moss 2 (Kenneth B. Moss is Associate Dean for Academic Programs in the Industrial College of the Armed Forces, National Defense University, and a professor in its department of grand strategy. Previously Professor Moss was a member ofthe staff of the House Subcommittee on Europe and the Middle East, “Information Warfare and War Powers: Keeping the Constitutional Balance” Summer/Fall 2002, The Fletcher Forum of World Affairs, Vol.26:2)

Imagine the following scenario. The United States learns that a particular foreign government has regularly allowed several terrorist groups that target U.S. citizens and interests to deposit money in banks within its borders. Furthermore, this government sometimes provides money to these accounts through third parties. After weighing the options, the President agrees to an attack using information technologies, such as launching a new virus, on the networks serving this country's financial institutions. A significant disruption of banking and other transactions occurs, and the country's government, convinced that the U.S. is behind this "cyber-attack," supports a terrorist attack on a U.S. installation a few weeks later. Through intelligence channels, the U.S. learns of this direct involvement and sends air strikes against select targets in the country. The "White House informs the congressional leadership of the decision only a few hours before the planned air strikes.

The last part of this scenario, involving a Presidential order to use limited military force and an ensuing disagreement with Congress over prior consultation and authorization to use force, is fairly predictable. Congress has been trying to protect its war powers—the power of declaration of war or an authorization to use force—since the 1970s through the War Powers Resolution of 1973 and other measures. But the first half of the scenario, involving "information war-fare," as it is now being called, places law and U.S. lawmakers on terra incognita. Perhaps consultation with Congress would occur with the senior Senate and House leadership, the Senate Foreign Relations Committee or the International Relations Committee in the House, as well as the intelligence committees, but it is just as likely that no consultation would take place. The role of Congress in information warfare operations is unclear because the status of such operations remains undefined in national law, international law, or the laws of warfare. Yet, if Congress is to protect its constitutional powers in war-making and the use of military force, the time has come when it must study the subject of information warfare and amend or create legislation to address this issue.

As Congress does so, it will have to bear in mind that even the experts do not agree on a definition of information warfare. Consider as a start the definition offered by the Joint Chiefs of Staff. Information warfare is composed of "[information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or conflict." A key term in that definition is "information operations," which are "[a]ctions taken to affect adversary information and information systems while defending ones own information and information systems."1 On first reading, this definition seems fairly limited to measures that are taken via computers, other information technologies, and information systems and networks. This definition of information warfare could generate congressional concerns about the efficiency and protection of U.S. information networks and systems, but it would not seemingly provoke any efforts to protect congressional war powers.

However, another definition greatly expands the scope of information warfare and raises significant questions about the relationship among information warfare, the conduct of war, and the role of congressional war powers. In What Is Information Warfare, Martin Libicki defines it as "conflicts that involve the protection, manipulation, degradation, and denial of information."2 Libicki then adds that it can occur in seven different forms: strikes at command and control capabilities, intelligence-based warfare related to acquiring or protecting information that can help one dominate a battlefield, electronic warfare, psychological warfare, "hacker" warfare, economic information warfare, and various scenarios in cyber warfare.3 This definition presents an open-ended meaning that can embrace elements of traditional means of warfare as well as recent or future ones. The inclusions of such traditional measures, which are the foundations of Congress's understanding of war, make this definition something that Congress should study closely.

An opposite approach argues that war should be removed from the term "information warfare." The focus of such operations should be on nonviolent means or stimuli. Taking the argument possibly to an extreme conclusion, advocates of this view argue that war will not occur if the information part is done cor-recdy. In short, these are acts that will prevent or pre-empt the resort to violence. It is also a concept of Information warfare that implies that a number of such measures can be performed by the civilian sector rather than the military, the traditional home of war-fighting capabilities.4 Here, it would seem Congress has little reason or basis to be concerned about the use of information or information technology as an instrument of war, since the goal is to avoid a use of traditional military force.

Regardless of the difficulty in defining it, information warfare is increasingly being examined by policy-makers because it offers a number of advantages not provided by traditional warfare. Information operations are arguably lower risk because they may accomplish their objective without resort to armed force. Furthermore, they may cost less: consider the cost of an information operation versus the deployment of almost any military unit. Finally, in a climate where both the nation's political and military leadership wish to avoid casualties, the prospect of being able to act forcefully while avoiding any socially and politically unacceptable loss of life holds a powerful attraction. In Operation Allied Force in 1999, the use of information technologies in precision-guided munitions as well as in other combat and command-and-control systems contributed significandy to the lack of fatalities for the U.S. and its NATO allies. The low casualty rate in Afghanistan seems to reinforce the appeal of this capability. On the other hand, some informa-tion warfare operations are not linked at all with the use of weaponry, and, in fact, may be a desirable alternative to it. As information warfare capabilities improve, the nations political and military leaders will want to rely more on a choice that may offer worthwhile results at lower budgetary and human costs.

The technologies and means of information warfare offer the President major advantages in the conduct of war chat come at the expense of Congress. There are a number of reasons for this. Because troops and weaponry may not be involved, it is unclear whether operations in information warfare would be regarded as a use of force or a hostile act. If not judged as a use of force, what would be the constitutional basis for congressional action? Historically, Congress has been reluctant to assert its war powers against the actions of a President, even when traditional military means are used. Will the use of information technologies in weaponry and the accompanying promise (and hope) of fewer casualties invite Congress to give the President more leeway over the authorization of military force? Taking this idea one step further, could the use of information technology rather than traditional weaponry and troops be regarded as an acceptable course that requires no congressional oversight and action? A decision to use military force and to risk lives is a difficult one—a choice leaders righdy prefer not to make not to make if they can avoid it. Legislators do not want to stare into the abyss of military action where outcomes and political consequences can be uncertain. If a new type of warfare at a lower threshold is available to the President and Congress, the need for congressional review and action may not seem as compelling. Yet, if that is the conclusion that emerges, any imbalance that already favors the President in using military force will become greater.

NEW FORMS OF LIMITED FORCE AND THE CONSTITUTION

To define its responsibilities in an information warfare environment, Congress must wrestle with a number of questions. Foremost is the question of whether information warfare and cyber attacks fall within the definition of military force used by Congress. Consider the foundation of congressional powers in this area: the power to declare war. Aside from the fact that a declaration of war is a rare event in U.S. history, another fundamental question is the definition of war itself. Throughout history there has been a common understanding that war involves the use of armed force.

Thus, one can see why a debate continues among specialists in law and information warfare over the question of whether or not such operations are an act of war. Sensing the confusion within the U.S. defense community, the Office of General Counsel in the Department of Defense presented an analysis of this question in June 1999.5 The counsel argues that an act of war is a concept rarely heard in modern diplomatic discourse. It goes on to state:

"An act of war is a violation of another nations rights under international law that is so egregious that the victim would be justified in declaring war. Declarations of war have fallen into disuse, and the act of war concept plays no role in the modern international legal system."6

There are those who would strongly disagree with this position, but the argument reflects the calculated efforts of the U.S. for over half a century to avoid a declaration of war.7

Much of the current discussion about what constitutes war rests on the UN Charter and other UN declarations. For example, in 1974 the UN General Assembly passed the Definition of Aggression Resolution, which, although not regarded by the U.S. as the absolute and final word, posited that the resolution provided "useful guidance." The important thread throughout the definition was the use of actual, or "kinetic," force, as one group of writers described it.8 Thus, the emphasis in the resolution falls on land, air, or sea actions, such as invasions, forceful annexation, bombardment, the use of weapons by one state against another, blockade, or sending armed bands, mercenaries, irregulars or other groups against another state. There is little here to suggest that information warfare could ever fall under the definition of war as understood by the writers of the Constitution or by subsequent generations of U.S. presidents and legislators.

To cloud the issue further, an ongoing debate continues over whether or not the technologies used in information warfare, such as computers, are really weapons. An Air Force instruction document in 1994 suggested that "computer systems would probably not be considered weapons." "Weapons are devices designed to kill, injure, or disable people, or to damage or destroy' property. Weapons do not include...electronic warfare devices." This definition places full emphasis on the consequences. A weapon has to destroy something; if it does not, it is not a weapon.

A different approach to defining a weapon places emphasis on its intended use. This definition suggests that the computer relaying the information to the actual destructive device could be regarded as a weapon on its own. This very question is one of the major disagreements about the Outer Space Treaty. Some argue satellites are not weapons, since they merely relay information. Obviously, a personal computer on its own is hardly a traditional or kinetic weapon (unless perhaps heaved by a frustrated employee at a supervisor), but when linked to an actual weapon on the ground, sea, or in the air is it not essentially the same?9 It does provide the information, such as guidance, that enables the device to destroy the target.

The above question pertains to information technology linked through a system or network to a real weapon. A harder question to answer is posed, however, when a computer, not linked to any weapon, is used to provide commands or to install a virus that causes disorder or even destruction elsewhere. Stand-alone com-puters would have played an important part in the introductory scenario—the attacks on the foreign country's banking network. It may seem a stretch of the imagination to equate a collection of digital signals to bombs and bullets, but cyber-attacks can produce very destructive consequences such as downed power grids that shut off power in hospitals or the disruption of flood control systems at dams. Such impacts are not significandy different from the results of a bomb dropped on a power station or on a dam. Consequendy, as the Department of Defenses own legal counsel points out, one may have to answer the question about a computer as weaponry not in terms of the technology but in terms of the consequences. If the results are comparable to what might be produced by traditional weapons in an act of aggression, a government may well be justified in responding not with another cyber operation but with direct military force.10

In such circumstances, Congress is poorly equipped to act and to review, much less challenge, the actions of a President who has ordered an information operation against another state. Current laws simply provide no effective means for doing so.

Consider the War Powers Resolution of 1973, in which Congress tried to strengthen its powers to control Presidential actions in instances where military force was being used without a declaration of war. The key words are at the beginning of Section 4(a): "In the absence of a declaration of war, in any case in which United States Armed Forces are introduced..." and with the pivotal words being "United States Armed Forces." Section 4(a) (1) concerns introducing forces "into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances."11 This is the most vague of the three provisions in the law requiring a presidential report to Congress. One may argue that the use of U.S. military resources (such as employing troops at computers) to commence an information warfare operation against a foreign actor might be a form of introducing armed forces into hostilities or situations where they are imminent. However, that is a very sweeping interpretation that seemingly exceeds the intent of the law. The provision clearly implies movement of personnel.

If Congress was preparing to use the War Powers Resolution in this context, it should revisit the entire statute and determine after close scrutiny what types of information operations may amount to mea-. sures that could bring the United States into hostilities. Presidents have consistendy challenged the constitutionality of the War Powers Resolution, and it is certain any President would do so if Congress tried to expand its definition to information warfare scenarios. A President would likely argue that these are pre-hostile measures and that Congress's authority in war powers does not commence until the decision to move U.S. forces occurs. However, it is the prospect of consequences comparable to an actual use of force offered by some information warfare scenarios that justifies congressional study of this question.

It is also possible that some information operations could fall under the jurisdiction of the intelligence committees. The Intelligence Oversight Act of 1991 requires the President to keep the two committees "fully and currendy informed of the intelligence activities of the United States, including any significant anticipated intelligence activity [covert action] as required by this tide." This act defines covert acdon as "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly/' Certainly, the need to conceal the origins of the action requires any information warfare measures to be covert. However, the provision specifically excludes from the definition "traditional diplomatic or military activities or routine support to such activities."12 Information warfare activities are not traditional, but they are becoming another option in the military's arsenal alongside the personnel and weapons that a President can use. To the extent that the intelligence committees can provide oversight of information warfare, they are not in the best position to protect Congress's role in war powers. That fells primarily in the jurisdiction of the Senate Foreign Relations Committee, the House International Relations. Committee, and the two armed services committees.

A CHALLENGE FOR CONGRESS

It is unfair to suggest that Congress has ignored information warfare or cyber warfare. Like the executive branch, it has paid much attention to measures to protect the United States against such attacks. However, the prospect of an attack on America using information technologies invites another prospect—that of retaliation by the United States.13 This question, and the question of whether the measures selected amount to or are equivalent to a use of force by the United States, should also concern Congress. Four years ago, Congress received just such a warning from the President's Commission on Critical Infrastructure Protection, when it urged Congress to examine this very issue in light of the War Powers Resolution.14 Nothing has happened, however. Meanwhile, U.S. strategic thinking is evolving in a way that increasingly foresees information operations as a dimension of war fighting.

As with any major policy development, Congress needs first to educate itself about information operations and cyber warfare before it considers any legislation. Doing so through hearings and study will provide a major service not only to itself, but also to the nation at large. One of the most difficult aspects of information warfare is clearly defining it. Hearings will help the strategic community clarify its own thinking as it tries to explain concepts and applications to Congress. Information warfare is a subject discussed mainly in a small, specialized community. In spite of some coverage in the press, it still carries too many science fiction connotations to be quickly understood and comfortably discussed in the larger policy community.

More importantly, as in any debate and vote on the use of traditional military force, Congress's placement of information warfare within the context of the Constitution guarantees that the Presidents policy towards it will have a stronger legal foundation and public support. This is critical not only for sustained acceptance of the policy at home but also for international recognition of the justification of the Presidents decisions abroad. Ultimately, information warfare, cyber-attacks, or cyber warfare must come under the same requirements for accountability in the Constitution as traditional military force. The President cannot be given an instrument of warfare over which Congress has no power.

## at failed states

#### No impact to failed states – star this card!

Patrick, senior fellow, director – program on international institutions and global governance @ CFR, 4/15/’11

(Stewart M, “Why Failed States Shouldn’t Be Our Biggest National Security Fear,” <http://www.cfr.org/international-peace-and-security/why-failed-states-shouldnt-our-biggest-national-security-fear/p24689>)

In truth, while failed states may be worthy of America's attention on humanitarian and development grounds, most of them are irrelevant to U.S. national security. The risks they pose are mainly to their own inhabitants. Sweeping claims to the contrary are not only inaccurate but distracting and unhelpful, providing little guidance to policymakers seeking to prioritize scarce attention and resources.

In 2008, I collaborated with Brookings Institution senior fellow Susan E. Rice, now President Obama's permanent representative to the United Nations, on an index of state weakness in developing countries. The study ranked all 141 developing nations on 20 indicators of state strength, such as the government's ability to provide basic services. More recently, I've examined whether these rankings reveal anything about each nation's role in major global threats: transnational terrorism, proliferation of weapons of mass destruction, international crime and infectious disease.

The findings are startlingly clear. Only a handful of the world's failed states pose security concerns to the United States. Far greater dangers emerge from stronger developing countries that may suffer from corruption and lack of government accountability but come nowhere near qualifying as failed states.

The link between failed states and transnational terrorism, for instance, is tenuous. Al-Qaeda franchises are concentrated in South Asia, North Africa, the Middle East and Southeast Asia but are markedly absent in most failed states, including in sub-Saharan Africa. Why? From a terrorist's perspective, the notion of finding haven in a failed state is an oxymoron. Al-Qaeda discovered this in the 1990s when seeking a foothold in anarchic Somalia. In intercepted cables, operatives bemoaned the insuperable difficulties of working under chaos, given their need for security and for access to the global financial and communications infrastructure. Al-Qaeda has generally found it easier to maneuver in corrupt but functional states, such as Kenya, where sovereignty provides some protection from outside interdiction.

Pakistan and Yemen became sanctuaries for terrorism not only because they are weak but because their governments lack the will to launch sustained counterterrorism operations against militants whom they value for other purposes. Terrorists also need support from local power brokers and populations. Along the Afghanistan-Pakistan border, al-Qaeda finds succor in the Pashtun code of pashtunwali, which requires hospitality to strangers, and in the severe brand of Sunni Islam practiced locally. Likewise in Yemen, al-Qaeda in the Arabian Peninsula has found sympathetic tribal hosts who have long welcomed mujaheddin back from jihadist struggles.

Al-Qaeda has met less success in northern Africa's Sahel region, where a moderate, Sufi version of Islam dominates. But as the organization evolves from a centrally directed network to a diffuse movement with autonomous cells in dozens of countries, it is as likely to find haven in the banlieues of Paris or high-rises of Minneapolis as in remote Pakistani valleys.

What about failed states and weapons of mass destruction? Many U.S. analysts worry that poorly governed countries will pursue nuclear, biological, chemical or radiological weapons; be unable to control existing weapons; or decide to share WMD materials.

These fears are misplaced. With two notable exceptions — North Korea and Pakistan — the world's weakest states pose minimal proliferation risks, since they have limited stocks of fissile or other WMD material and are unlikely to pursue them. Far more threatening are capable countries (say, Iran and Syria) intent on pursuing WMD, corrupt nations (such as Russia) that possess loosely secured nuclear arsenals and poorly policed nations (try Georgia) through which proliferators can smuggle illicit materials or weapons.

When it comes to crime, the story is more complex. Failed states do dominate production of some narcotics: Afghanistan cultivates the lion's share of global opium, and war-torn Colombia rules coca production. The tiny African failed state of Guinea-Bissau has become a transshipment point for cocaine bound for Europe. (At one point, the contraband transiting through the country each month was equal to the nation's gross domestic product.) And Somalia, of course, has seen an explosion of maritime piracy. Yet failed states have little or no connection with other categories of transnational crime, from human trafficking to money laundering, intellectual property theft, cyber-crime or counterfeiting of manufactured goods.

Criminal networks typically prefer operating in functional countries that provide baseline political order as well as opportunities to corrupt authorities. They also accept higher risks to work in nations straddling major commercial routes. Thus narco-trafficking has exploded in Mexico, which has far stronger institutions than many developing nations but borders the United States. South Africa presents its own advantages. It is a country where “the first and the developing worlds exist side by side,” author Misha Glenny writes. “The first world provides good roads, 728 airports . . . the largest cargo port in Africa, and an efficient banking system. . . . The developing world accounts for the low tax revenue, overstretched social services, high levels of corruption throughout the administration, and 7,600 kilometers of land and sea borders that have more holes than a second-hand dartboard.” Weak and failing African states, such as Niger, simply cannot compete.

Nor do failed states pose the greatest threats of pandemic disease. Over the past decade, outbreaks of SARS, avian influenza and swine flu have raised the specter that fast-moving pandemics could kill tens of millions worldwide. Failed states, in this regard, might seem easy incubators of deadly viruses. In fact, recent fast-onset pandemics have bypassed most failed states, which are relatively isolated from the global trade and transportation links needed to spread disease rapidly.

Certainly, the world's weakest states — particularly in sub-Saharan Africa — suffer disproportionately from disease, with infection rates higher than in the rest of the world. But their principal health challenges are endemic diseases with local effects, such as malaria, measles and tuberculosis. While U.S. national security officials and Hollywood screenwriters obsess over the gruesome Ebola and Marburg viruses, outbreaks of these hemorrhagic fevers are rare and self-contained.

I do not counsel complacency. The world's richest nations have a moral obligation to bolster health systems in Africa, as the Obama administration is doing through its Global Health Initiative. And they have a duty to ameliorate the challenges posed by HIV/AIDS, which continues to ravage many of the world's weakest states. But poor performance by developing countries in preventing, detecting and responding to infectious disease is often shaped less by budgetary and infrastructure constraints than by conscious decisions by unaccountable or unresponsive regimes. Such deliberate inaction has occurred not only in the world's weakest states but also in stronger developing countries, even in promising democracies. The list is long. It includes Nigeria's feckless response to a 2003-05 polio epidemic, China's lack of candor about the 2003 SARS outbreak, Indonesia's obstructionist attitude to addressing bird flu in 2008 and South Africa's denial for many years about the causes of HIV/AIDS.

Unfortunately, misperceptions about the dangers of failed states have transformed budgets and bureaucracies. U.S. intelligence agencies are mapping the world's “ungoverned spaces.” The Pentagon has turned its regional Combatant Commands into platforms to head off state failure and address its spillover effects. The new Quadrennial Diplomacy and Development Review completed by the State Department and the U.S. Agency for International Development depicts fragile and conflict-riddled states as epicenters of terrorism, proliferation, crime and disease.

Yet such preoccupations reflect more hype than analysis. U.S. national security officials would be better served — and would serve all of us better — if they turned their strategic lens toward stronger developing countries, from which transnational threats are more likely to emanate.

## terror adv

Risk of nuclear terrorism is real and high now

Bunn 13 (Matthew, Valentin Kuznetsov, Martin B. Malin, Yuri Morozov, Simon Saradzhyan, William H. Tobey, Viktor I. Yesin, and Pavel S. Zolotarev. "Steps to Prevent Nuclear Terrorism." Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, October 2, 2013, Matthew Bunn. Professor of the Practice of Public Policy at Harvard Kennedy School andCo-Principal Investigator of Project on Managing the Atom at Harvard University’s Belfer Center for Science and International Affairs. • Vice Admiral Valentin Kuznetsov (retired Russian Navy). Senior research fellow at the Institute for U.S. and Canadian Studies of the Russian Academy of Sciences, Senior Military Representative of the Russian Ministry of Defense to NATO from 2002 to 2008. • Martin Malin. Executive Director of the Project on Managing the Atom at the Belfer Center for Science and International Affairs. • Colonel Yuri Morozov (retired Russian Armed Forces). Professor of the Russian Academy of Military Sciences and senior research fellow at the Institute for U.S. and Canadian Studies of the Russian Academy of Sciences, chief of department at the Center for Military-Strategic Studies at the General Staff of the Russian Armed Forces from 1995 to 2000. • Simon Saradzhyan. Fellow at Harvard University’s Belfer Center for Science and International Affairs, Moscow-based defense and security expert and writer from 1993 to 2008. • William Tobey. Senior fellow at Harvard University’s Belfer Center for Science and International Affairs and director of the U.S.-Russia Initiative to Prevent Nuclear Terrorism, deputy administrator for Defense Nuclear Nonproliferation at the U.S. National Nuclear Security Administration from 2006 to 2009. • Colonel General Viktor Yesin (retired Russian Armed Forces). Leading research fellow at the Institute for U.S. and Canadian Studies of the Russian Academy of Sciences and advisor to commander of the Strategic Missile Forces of Russia, chief of staff of the Strategic Missile Forces from 1994 to 1996. • Major General Pavel Zolotarev (retired Russian Armed Forces). Deputy director of the Institute for U.S. and Canadian Studies of the Russian Academy of Sciences, head of the Information and Analysis Center of the Russian Ministry of Defense from1993 to 1997, section head - deputy chief of staff of the Defense Council of Russia from 1997 to 1998., 10/2/2013, “Steps to Prevent Nuclear Terrorism: Recommendations Based on the U.S.-Russia Joint Threat Assessment”, <http://belfercenter.ksg.harvard.edu/publication/23430/steps_to_prevent_nuclear_terrorism.html>)

I. Introduction In 2011, Harvard’s Belfer Center for Science and International Affairs and the Russian Academy of Sciences’ Institute for U.S. and Canadian Studies published “The U.S. – Russia Joint Threat Assessment on Nuclear Terrorism.” The assessment analyzed the means, motives, and access of would-be nuclear terrorists, and concluded that the threat of nuclear terrorism is urgent and real. The Washington and Seoul Nuclear Security Summits in 2010 and 2012 established and demonstrated a consensus among political leaders from around the world that nuclear terrorism poses a serious threat to the peace, security, and prosperity of our planet. For any country, a terrorist attack with a nuclear device would be an immediate and catastrophic disaster, and the negative effects would reverberate around the world far beyond the location and moment of the detonation. Preventing a nuclear terrorist attack requires international cooperation to secure nuclear materials, especially among those states producing nuclear materials and weapons. As the world’s two greatest nuclear powers, the United States and Russia have the greatest experience and capabilities in securing nuclear materials and plants and, therefore, share a special responsibility to lead international efforts to prevent terrorists from seizing such materials and plants. The depth of convergence between U.S. and Russian vital national interests on the issue of nuclear security is best illustrated by the fact that bilateral cooperation on this issue has continued uninterrupted for more than two decades, even when relations between the two countries occasionally became frosty, as in the aftermath of the August 2008 war in Georgia. Russia and the United States have strong incentives to forge a close and trusting partnership to prevent nuclear terrorism and have made enormous progress in securing fissile material both at home and in partnership with other countries. However, to meet the evolving threat posed by those individuals intent upon using nuclear weapons for terrorist purposes, the United States and Russia need to deepen and broaden their cooperation. The 2011 “U.S. - Russia Joint Threat Assessment” offered both specific conclusions about the nature of the threat and general observations about how it might be addressed. This report builds on that foundation and analyzes the existing framework for action, cites gaps and deficiencies, and makes specific recommendations for improvement. “The U.S. – Russia Joint Threat Assessment on Nuclear Terrorism” (The 2011 report executive summary): • Nuclear terrorism is a real and urgent threat. Urgent actions are required to reduce the risk. The risk is driven by the rise of terrorists who seek to inflict unlimited damage, many of whom have sought justification for their plans in radical interpretations of Islam**;** by the spread of information about the decades-old technology of nuclear weapons; by the increased availability of weapons-usable nuclear materials; and by globalization, which makes it easier to move people, technologies, and materials across the world. • Making a crude nuclear bomb would not be easy, but is potentially within the capabilities of a technically sophisticated terrorist group, as numerous government studies have confirmed. Detonating a stolen nuclear weapon would likely be difficult for terrorists to accomplish, if the weapon was equipped with modern technical safeguards (such as the electronic locks known as Permissive Action Links, or PALs). Terrorists could, however, cut open a stolen nuclear weapon and make use of its nuclear material for a bomb of their own. • The nuclear material for a bomb is small and difficult to detect, making it a major challenge to stop nuclear smuggling or to recover nuclear material after it has been stolen. Hence, a primary focus in reducing the risk must be to keep nuclear material and nuclear weapons from being stolen by continually improving their security, as agreed at the Nuclear Security Summit in Washington in April 2010. • Al-Qaeda has sought nuclear weapons for almost two decades. The group has repeatedly attempted to purchase stolen nuclear material or nuclear weapons, and has repeatedly attempted to recruit nuclear expertise. Al-Qaeda reportedly conducted tests of conventional explosives for its nuclear program in the desert in Afghanistan. The group’s nuclear ambitions continued after its dispersal following the fall of the Taliban regime in Afghanistan. Recent writings from top al-Qaeda leadership are focused on justifying the mass slaughter of civilians, including the use of weapons of mass destruction, and are in all likelihood intended to provide a formal religious justification for nuclear use. While there are significant gaps in coverage of the group’s activities, al-Qaeda appears to have been frustrated thus far in acquiring a nuclear capability; it is unclear whether the the group has acquired weapons-usable nuclear material or the expertise needed to make such material into a bomb. Furthermore, pressure from a broad range of counter-terrorist actions probably has reduced the group’s ability to manage large, complex projects, but has not eliminated the danger. However, there is no sign the group has abandoned its nuclear ambitions. On the contrary, leadership statements as recently as 2008 indicate that the intention to acquire and use nuclear weapons is as strong as ever.

## 2ac must prohibit

We meet --- we prohibit the authority to use cyber operations without congressional approval

Chen 12 (Julia – JD Candidate @ Boston College (2013) specializing in National Security, MEM in Engineering Management from Old Dominion, BA – Rice University, “NOTE: RESTORING CONSTITUTIONAL BALANCE: ACCOMMODATING THE EVOLUTION OF WAR” November, 2012, 53 B.C. L. Rev 1767)

To check effectively the President's war power, Congress should divide the process of congressional oversight so it is tailored to address both open and covert warfare. n359 The War Powers Consultation proposal specifically exempts "covert operations" from its scope. n360 Nonetheless, "covert operations" are a significant element of modern warfare. n361 Covert actions should therefore not be exempt from legislation [\*1803] that governs war powers, because the Constitution envisions a role for both the Congress and the President in the decision to enter a war. n362

The Commission's proposed legislation calls for creation of a Joint Congressional Consultation Committee. n363 This Committee would be composed of the minority leaders of the House and Senate, the majority leader of the Senate, the Speaker of the House, and the chairs and ranking members of the Senate and House committees on foreign affairs, armed services, intelligence, and appropriations. n364 Thus, the Committee closely mirrors the requirements of the existing congressional oversight committees on intelligence. n365 The proposed legislation should be amended so that all intended acts of war by the executive, including open and covert actions, are initially referred to this Committee. n366

For non-covert operations, the War Powers Consultation proposal outlines a process for congressional oversight. n367 The President is required to have meaningful consultation with the Committee, rather than just notification. n368 This consultation must occur prior to the conflict, or in emergent circumstances, within three calendar days after operations begin. n369 The proposal also requires **that Congress act to** approve or disapprove **of the action.** n370 If Congress has not acted on its own accord, the Committee is required to "introduce an identical concurrent resolution in the Senate and House." n371 This process would result in meaningful consultation between the President and Congress, and would **mandate** that Congress act to check the President's power when appropriate. n372

This proposed legislation should be modified so that in situations that require covert operations, the process would be modeled on the [\*1804] Intelligence Oversight Act of 1991. n373 In these situations, the Joint Congressional Consultation Committee would assume an analogous role to the existing Senate and House intelligence committees. n374 Thus, the members of the Committee could engage in fully informed consultation with the President, rather than being limited to the discussion of only non-covert actions. n375 Following the model of the Intelligence Oversight Act of 1991, the process for covert operations should require the President to make a finding in writing within forty-eight hours of making the decision to conduct the action. n376 In addition, the action could commence prior to notification, but notification must follow soon afterward. n377 Furthermore, in a written finding the President should specify "each department, agency, or entity of the United States Government authorized to fund or otherwise participate in any significant way in such action." n378 The finding must also identify any third parties that are not employed by the government that are to be involved with the action. n379 This statement will give members of Congress the full picture of what forces are involved in the activity. n380

Upon receipt of this finding from the President, the Committee must have an affirmative requirement to balance the power of the executive. n381 It should first be required to make a finding as to whether the action truly requires secrecy or should be discussed with the full Congress. n382 If the Committee finds that the action is of a nature that requires secrecy, it should remain in the Committee for debate. n383 Conversely, if the Committee finds that there is no need for secrecy, it should consult accordingly with the executive and, if appropriate, treat the information as an open conflict. n384

Once the Committee makes a finding that the conflict is covert and should be kept secret, it must be further debated within the Committee. n385 [\*1805] Furthermore, the executive should be required to keep the Committee apprised of the conflict and provide periodic written updates. n386 This exchange would give Congress the opportunity to check the power of the President, and prevent the tyranny that the Framers so feared. n387 Additionally, it would enable Congress to balance the power of the executive and make informed decisions on defense appropriations. n388

These recommended modifications to the proposed War Powers Consultation Act of 2009 would make it match the realities of modern warfare. n389 Expanding its scope to include all of the actors that contribute to modern warfare, and all of the actions with the effects of warfare, would strike the appropriate balance of war powers between the executive and legislative branches. n390 This balance is necessary to ensure not only that the executive can adequately defend the nation, but also that both the executive and legislative branches are accountable to the people who pay the price of governmental decisions. n391

CONCLUSION

The Constitution's system of checks and balances gave both the President and Congress powers over war. The War Powers Resolution of 1973 was an attempt by Congress to reassert its constitutional prerogative and implement a formal structure for the division of power with the President. Forty years later, modern warfare has evolved sufficiently to render the War Powers Resolution ineffective. Thus, Congress should replace the War Powers Resolution with a new, more pragmatic [\*1806] statute aligned with the realities of modern warfare. The new statute should incorporate elements of the proposed War Powers Consultation Act of 2009 and the existing Intelligence Oversight Act of 1991. Moreover, its scope should be expansive, to encompass all actors and all actions of modern warfare. Such an approach **will ensure real checks and balances and political accountability in the realm of war powers**.

The legislative veto is an explicit statutory restriction on the President

Quint, professor of law at Maryland, January 1989

(Peter E., “Reflections on the Separation of Powers and Judicial Review at the End of the Reagan Era,” 57 Geo. Wash. L. Rev. 427, Lexis)

Another type of separation of powers dispute, however, is not generally susceptible of a form of intermediate determination through statutory interpretation, or through the "convenient apologetics" of the political-question doctrine. In the 1970s -- in reaction to the extraordinary executive claims of the Nixon administration and the tragedies of executive policy during the period of the Vietnam War -- Congress attempted to reassert its policymaking authority in a number of areas, **and** sought **to impose explicit statutory limits on the power of the presidency**. Among other actions, Congress sought to limit the asserted war powers of the President, regulate executive budgetary authority, impose limitations on the exercise of emergency power, rationalize the use of information from presidential papers, and provide for independent investigation of high executive officers suspected of committing criminal offenses. Moreover, in several disparate areas, Congress sought to limit executive policymaking powers through the widespread use of one or another of the devices known as **the legislative veto**.

In several instances, the Reagan administration took the position that certain **statutory restrictions** could not be validly applied against the President or executive officers in general. In some of these cases -- **for example**, in the dispute over **the legislative veto** -- the administration pursued arguments that had also been invoked by its predecessor. n29 In other important instances -- in the dispute over the independent counsel legislation, for example -- it claimed more extensive (and more exclusive) executive power than had been [\*435] asserted under President Carter. n30

In many of these cases, some sort of intermediate argument based on statutory construction was ordinarily not available to the administration. Perhaps it was occasionally possible to argue that a statutory scheme should be interpreted so that it does not apply to the executive in specific cases, or even that it might actually grant power to the President under certain circumstances. n31 In many important instances, however, **the language and purpose of these statutory schemes** of the mid-1970s **were so clearly directed toward specific limitation of the executive**, **that such arguments were not plausible**. Rather, in these cases the administration was required to argue that the statutes themselves were unconstitutional.

“On” means there’s no limits disad

Dictionary.com, http://dictionary.reference.com/browse/on

On

preposition

1.so as to be or remain supported by or suspended from: Put your package down on the table; Hang your coat on the hook.

2.so as to be attached to or unified with: Hang the picture on the wall. Paste the label on the package.

## 2AC OLC cp

Perm: Do both --- counterplan implements the plans statute or it lacks legal signal

Gitterman 13

Daniel Gitterman is associate professor of Public Policy at UNC-Chapel Hill, Presidential Studies Quarterly, June 2013, "The American Presidency and the Power of the Purchaser", Vol. 43, No. 2, Ebsco

Presidents and their staffs consider executive orders an indispensable policy and political tool (Mayer 2001). Executive orders and presidential policy directives to the bureaucracy are instruments of political control and inﬂuence. Formally, an executive order is a directive that draws on the president’s unique legal authority to require or authorize some action within the administrative state (Mayer 1999). The ability to issue and to enforce an executive order is based on statutory authority, an act of Congress, or the Constitution.1 Executive orders are not deﬁned in the Constitution, and there are no speciﬁc provisions in the Constitution authorizing the president to issue them.2 These orders are used to direct agencies and ofﬁcials in their execution of congressionally established policies. In many instances, they have been used to guide federal administrative agencies in directions contrary to congressional intent.

Political scientists recognize executive orders as an important policy tool, however constrained by legal and political considerations its use may be (Deering and Maltzman 1999; Krause and D. Cohen 1997; Mayer 1999, 2001; Moe and Howell 1999a). Presidents have used executive orders to reorganize executive branch agencies, to alter administrative and regulatory processes, to shape legislative interpretation and implementation, and to make public policy.3 In a study of the history of executive branch practice, Calabresi and Yoo (2008) conclude that since the days of George Washington, presidents have consistently asserted their power to execute law.4

To have the full force of law, executive orders must be “derived from the statutory or constitutional authority cited by the president in issuing the decree” (Cooper 2002, 21). However, courts have allowed the president to claim implied statutory authority when Congress has not opposed the president on the public record. In staying out of separationof-powers issues, the courts have left it up to Congress to protect its own interests against the expansion of executive power. More broadly, executive orders have continued to grow in importance, and overly deferential court decisions have laid the foundation for further expansion. Congress has had a difﬁcult time enacting laws that amend or overturn orders issued by presidents, though efforts to either codify in law or fund an executive order enjoy higher success rates. While judges and justices have appeared willing to strike down executive orders, the majority of such orders are never challenged, and for those that are, presidents win more than 80% of the cases that go to trial (Howell 2005).

But the counterplan doesn’t and wont be enforced

Rudalevige 12

Andrew Rudalevige is Walter E. Beach ’56 Chair in Political Science at Dickinson College, Presidential Studies Quarterly, March 2012, "The Contemporary Presidency: Executive Orders and Presidential Unilateralism", Vol. 42, No. 1, Ebsco, EOP = Executive Office of the President

After all, is it really safe to assume that the executive branch is a single actor? Most of the history of public administration is predicated on the notion it is not (see, e.g., Seidman and Gilmour 1986). Can we safely assume that the president incurs no transaction costs of collective action when dealing with the bureaucracy, even when dealing with the presidential branch’s own “counter-bureaucracy” (Nathan 1983) within the Executive Ofﬁce of the President (EOP)? Even Mayer (2001), in his magisterial book on the importance of executive orders, provides important cautions against that claim. The empirical literature suggests that some orders are not issued at all, in the face of interior objections (see Gibson 2009); that they often move policy closer to congressional preferences (Law 2011); and that many rely for their content on internal and external coalitionbuilding (Morgan 1970; Rodrigues 2007; Wigton 1996). Dickinson (2009, 757) argues that “the difference in administrative and legislative policymaking is not that it signiﬁes a shift between a ‘unilateral’ and a ‘multilateral’ process. Instead, it is a change in where, and with whom, bargaining takes place.”

Indeed, an established body of literature suggests that even within the EOP, coordination has clear managerial limits. This is true even when everyone concerned is well meaning. And the relationship grows more fraught as we move outwards from the White House complex (e.g., Dickinson 1997; Heclo 1977). In a branch that collects nearly three million persons within its purview, we can expect collective action problems. Richard Nixon’s aide William Saﬁre (1975, 246-47) called the executive branch a “lethargic behemoth” that presidents struggle to control: “the so-called Chief Executive,” he added, “can tug and haul all day and never rip up the bureaucracy.” More analytically, Krause (2009, 75) notes that “analyses grounded exclusively in formal executive powers understate organizational complexity, and thus overstate presidential capacity for controlling the bureaucracy.” Recent cases in this vein might include Bill Clinton’s 1993 effort to end the ban on gays’ open service in the military, George W. Bush’s program of domestic surveillance (including a dramatic showdown between Department of Justice and White House staff in Attorney General John Ashcroft’s hospital room), or Barack Obama’s so-far unheeded order to close the detention facility at Guantanamo Bay. To take a different sort of example, consider one of Gerald Ford’s ﬁrst executive orders. It dealt with the early promotion of outstanding army ofﬁcers—but Ford (or even his staff) had nearly nothing to do with it. It had been proposed in July 1974, and sent to the White House later that month, well before President Nixon’s resignation.2

These examples hardly prove that presidents have no power of command (even Neustadt [1990] did not argue that). They do, however, speak “to the illusion that administrative agencies comprise a single structure, ‘the’ executive branch, where presidential word is law, or ought to be” (Neustadt 1990, 33-34). They suggest the value in breaking up the “unitary executive” into the fragments and routines with which presidents must daily contend. Those lie across the executive branch, and even within the Executive Ofﬁce.Assuch,thecasemovesinratherparallelfashiontotheshifttracedbyGrahamAllison when he wrote about the 1962 Cuban Missile Crisis. Beginning with a model that assumed a uniﬁed rational actor, Allison discovered this left odd but important details unexplained. To understand the nuance of what happened over those “thirteen days” it was necessary to bring in two other models more closely associated with bureaucratic policy making, dealing with the standard operating procedures relied upon by agencies and the intragovernmental politicking they engaged in (Allison and Zelikow 1999).

Counterplan maintains an unchecked executive – links to both advantages

Dycus 10 (Stephen – Professor @ Vermont Law School, “Cybersecurity Symposium: National Leadership, Individual Responsibility: Congress's Role in Cyber Warfare” 2010, 4 J. Nat'l Security L. & Pol'y 155)

I. Congress's Role in Deciding When and How To Go to War

There is broad agreement that congressional authorization is needed to start a war. n9 On the other hand, the President may act without Congress's approval to repel an attack on the United States. n10 Between these two extremes, the scope of the President's unilateral authority to use military [\*157] force is less well understood. n11 Once hostilities are under way, there is a consensus that the President has the tactical powers of a Commander in Chief, although it may not always be clear which of the President's actions are tactical and which are strategic. n12

Before an attack can be launched, of course, Congress must have supplied the President with personnel and weapons. n13 Moreover, Congress may regulate the President's actions as Commander in Chief, except when the nation comes under sudden attack or the President exercises her tactical powers (and perhaps even then). In the Supreme Court's 1800 decision in Bas v. Tingy, Justice Paterson, one of the Framers, echoed the other Justices in declaring that "as far as congress authorized and tolerated the war on our part, so far may we proceed in hostile operations." n14 Four years later, in Little v. Barreme, the Court reiterated that the President must not exceed limits set forth in Congress's authorization of hostilities. n15 Since then, no court has ruled otherwise. n16

In the intervening two centuries, Congress has adopted a number of measures to control the initiation or conduct of warfare. At the end of the Vietnam War, for example, Congress passed the War Powers Resolution (WPR), n17 which requires the President to report to Congress within 48 hours [\*158] the introduction of U.S. armed forces into hostilities or imminent hostilities, and to withdraw those forces within 60 days if Congress does not expressly approve of their continued deployment. n18 Lambasted by some as an unconstitutional encroachment on presidential powers, the WPR has been followed (or at least lip service has been paid to it) by each President since the Nixon administration, n19 and Congress has repeatedly referred to the WPR approvingly in subsequent legislation. n20

If Congress now fails to enact guidelines for cyber warfare, it might be perceived as inviting "measures on independent presidential responsibility." n21 Chief Justice Marshall suggested in Little v. Barreme that if Congress had remained silent, the President might have been free to conduct the Quasi-War with France as he saw fit. n22 But the national interest in electronic warfare, just as in that early maritime conflict, is so great that the planning and conduct of such a war should not be left entirely to the Executive. And because a cyber war might be fought under circumstances that make it impossible for Congress to play a meaningful contemporaneous role, Congress ought to get out in front of events now in order to be able to participate in the formulation of national policy.

OLC can’t solve and links to politics

Posner 11 Eric Posner is the Kirkland & Ellis Professor, University of Chicago Law School. “DEFERENCE TO THE EXECUTIVE IN THE UNITED STATES AFTER 9/11 CONGRESS, THE COURTS AND THE OFFICE OF LEGAL COUNSEL” available at http://www.law.uchicago.edu/academics/publiclaw/index.html.

These two events neatly encapsulate the dilemma for OLC, and indeed all the president’s legal advisers. If OLC tries to block the president from acting in the way he sees fit, it takes the risk that he will disregard its advice and marginalize the institution. If OLC gives the president the advice that he wants to hear, it takes the risk that it will mislead him and fail to prepare him for adverse reactions from the courts, Congress, and the public. Can OLC constrain the executive? That is the position taken by many scholars, most notably Jack Goldsmith. 18 The underlying idea here is that even if Congress and the courts cannot constrain the executive, perhaps offices within the executive can. The opposite view, advanced by Bruce Ackerman, is that OLC is a rubber stamp. 19 I advocate a third view: OLC does not constrain the executive but enables him to accomplish goals that he would not otherwise be able to accomplish. It is more accurate to say that OLC enables than constrains. B. OLC as a Constraint on the Executive A number of scholars have argued that OLC can serve as an important constraint on executive power. I will argue that OLC cannot act as a constraint on executive power. Indeed, its only function is the opposite—as an “enabler” (as I will put it) or extender of executive power. A president must choose a course of action. He goes to OLC for advice. Ideally, OLC will provide him good advice as to the legality of the course of action. It will not provide him political advice and other relevant types of advice. The president wants to maximize his political advantage, 21 and so he will follow OLC’s advice only if the legal costs that OLC identifies are greater than the political benefits. On this theory, OLC will properly always give the president neutral advice, and the president will gratefully accept it although not necessarily follow it. If the story ended here, then it would be hard to see what the controversy over OLC could be about. As an adviser, it possesses no ability to constrain the executive. It merely provides doctrinal analysis, in this way, if it does its job properly, merely supplying predictions as to how other legal actors will react to the president’s proposed action. The executive can choose to ignore OLC’s advice, and so OLC cannot serve as a “constraint” on executive power in any meaningful sense. Instead, it merely conveys to the president information about the constraints on executive power that are imposed from outside the executive branch. However, there is an important twist that complicates the analysis. The president may choose to publicize OLC’s opinions. Naturally, the president will be tempted to publicize only favorable opinions. When Congress 22 claims that a policy is illegal, the president can respond that his lawyers advised him that the policy is legal. This response at least partially deflects blame from the president. There are two reasons for this. First, the Senate consented to the appointment of these lawyers; thus, if the lawyers gave bad advice, the Senate is partly to blame, and so the blame must be shared. Second, OLC lawyers likely care about their future prospects in the legal profession, which will turn in part on their ability to avoid scandals and to render plausible legal advice; they may also seek to maintain the office’s reputation. When OLC’s opinions are not merely private advice, but are used to justify actions, then OLC takes on a quasi-judicial function. Presidents are not obliged to publicize OLC’s opinions, but clearly they see an advantage to doing so, and they have in this way given OLC quasi-judicial status. But if the president publicizes OLC opinions, he takes a risk. The risk is that OLC will publicly advise him that an action is illegal. If OLC approval helps deflect blame from the president, then OLC disapproval will tend to concentrate blame on the president who ignores its advice. Congress and the public will note that after all the president is ignoring the advice of lawyers that he appointed and thus presumably he trusts, and this can only make the president look bad. To avoid such blame, the president may refrain from engaging in a politically advantageous action. In this way, OLC may be able to prevent the president from taking an action that he would otherwise prefer. At a minimum, OLC raises the political cost of the action. I have simplified greatly, but I believe that this basic logic has led some scholars to believe that OLC serves as a constraint on the president. But this is a mistake. OLC strengthens the president’s hand in some cases and weakens them in others; but overall it extends his power—it serves as enabler, not constraint. To see why, consider an example in which a president must choose an action that lies on a continuum. One might consider electronic surveillance. At one extreme, the president can engage in actions that are clearly lawful—for example, spying on criminal suspects after obtaining warrants from judges. At the other extreme, the president can engage in actions that are clearly unlawful—for example, spying on political opponents. OLC opinions will not affect Congress’s or the public’s reaction to either the obviously lawful or the obviously unlawful actions. But then there are middle cases. Consider a policy L, which is just barely legal, and a policy I, which is just barely illegal. The president would like to pursue policy L but fears that Congress and others will mistakenly believe that L is illegal. As a result, political opposition to L will be greater than it would be otherwise. In such a case, a favorable advisory opinion from a neutral legal body that has credibility with Congress will help the president. OLC’s approval of L would cause political opposition (to the extent that it is based on the mistaken belief that L is unlawful) to melt away. Thus, OLC enables the president to engage in policy L, when without OLC’s participation that might be impossible. True, OLC will not enable the president to engage in I, assuming OLC is neutral. And, indeed, OLC’s negative reaction to I may stiffen Congress’ resistance. However, the president will use OLC only because he believes that OLC will strengthen his hand on net. It might be useful to make this point using a little jargon. In order for OLC to serve its ex ante function of enabling the president to avoid confrontations with Congress in difficult cases, it must be able to say “no” to him ex post for barely illegal actions as well as “yes” to him for barely legal actions. It is wrong to consider an ex post no as a form of constraint because, ex ante, it enables the president to act in half of the difficult cases. OLC does not impose any independent constraint on the president, that is, any constraint that is separate from the constraint imposed by Congress. An analogy to contract law might be useful. People enter contracts because they enable them to do things ex ante by imposing constraints on them ex post. For example, a debtor can borrow money from a creditor only because a court will force the debtor to repay the money ex post. It would be strange to say that contract law imposes “constraints” on people because of ex post enforcement. In fact, contract law enables people to do things that they could not otherwise do—it extends their power. If it did not,people would not enter contracts. A question naturally arises about OLC’s incentives. I have assumed that OLC provides neutral advice—in the sense of trying to make accurate predictions as to how other agents like Congress and the courts would reaction to proposed actions. It is possible that OLC could be biased—either in favor of the president or against him. However, if OLC were biased against the president, he would stop asking it for advice (or would ask for its advice in private and then ignore it). This danger surely accounts for the fact that OLC jurisprudence is pro-executive. 23 But it would be just as dangerous for OLC to be excessively biased in favor of the president. If it were, it would mislead the president and lose its credibility with Congress, with the result that it could not help the president engage in L policies. So OLC must be neither excessively pro-president nor anti-president. If it can avoid these extremes, it will be an “enabler”; if it cannot, it will be ignored. In no circumstance could it be a “constraint.” If the OLC cannot constrain the president on net, why have people claimed that OLC can constrain the president? What is the source of this mistake? One possibility, which I have already noted, is that commentators might look only at one side of the problem. Scholars note that OLC may “prevent” the president from engaging in barely illegal actions without also acknowledging that it can do so only if at the same time it enables the president to engage in barely legal actions. This is simply a failure to look at the full picture. For example, in The Terror Presidency, Goldsmith argues that President Bush abandoned a scheme of warrantless wiretapping without authorization from the FISA court because OLC declared the scheme illegal, and top Justice Department officials threatened to resign unless Bush heeded OLC’s advice. 25 This seems like a clear example of constraint. But it is important to look at the whole picture. If OLC had approved the scheme, and subsequently executive branch agents in the NSA had been prosecuted and punished by the courts, then OLC’s credibility as a supplier of legal advice would have been destroyed. For the president, this would have been a bad outcome. As I have argued, a credible OLC helps the president accomplish his agenda in “barely legal” cases. Without taking into account those cases where OLC advice helps the president’s agenda ex post as well as the cases where OLC advice hurts the president’s agenda ex post, one cannot make an overall judgment about OLC’s ex ante effect on executive power. Another possible source of error is that scholars imagine that “neutral” advice will almost always prevent the president from engaging in preferred actions, while rarely enabling the president to engage in preferred actions. The implicit picture here is that a president will normally want to break the law, that under the proper interpretation of the Constitution and relevant standards the president can accomplish very little. So if OLC is infact neutral and the president does obey its advice, then it must constrain the president. But this theory cannot be right, either. If OLC constantly told the president that he cannot do what he wants to do, when infact Congress and other agents would not object to the preferred actions, then the president would stop asking OLC for advice. As noted above, for OLC to maintain its relevance, it cannot offer an abstract interpretation of the Constitution that is divorced from political realities; it has to be able to make realistic predictions as to how other legal agents will react to the president’s actions. This has led OLC to develop a pro-executive jurisprudence in line with the long-term evolution of executive power. If OLC tried to impose constraints other than those imposed by Congress and other institutions with political power, then the president would ignore it.

Zero chance of Congressional follow-on AND CP links to politics

Kevin Drum, Mother Jones, 4/22/13, Maureen Dowd and Presidential Leverage, www.motherjones.com/kevin-drum/2013/04/maureen-dowd-and-presidential-leverage

Finally, there's the most obvious change of all: the decision by Republicans to stonewall every single Obama initiative from day one. By now, I assume that even conservative apologists have given up pretending that this isn't true. The evidence is overwhelming, and it's applied to practically every single thing Obama has done in the domestic sphere. The only question, ever, is whether Obama will get two or three Republican votes vs. three or four. If the latter, he has a chance to win. But those two or three extra votes don't depend on leverage. In fact, Obama's leverage is negative. The last thing any Republican can afford these days is to be viewed as caving in to Obama. That's a kiss of death with the party's base.

Executive transparency fails—not legally binding, no cred, raises expectations

Sarah Knuckey, NYU Law School Project on Extrajudicial Executions Director, Special Advisor to the UN Special Rapporteur on extrajudicial executions, 10/1/13, Transparency on Targeted Killings: Promises Made, but Little Progress, justsecurity.org/2013/10/01/transparency-targeted-killings-promises-made-progress/

Some interpreted these efforts and the President’s speech to mark the beginning of improved transparency. But despite transparency promises and expectations, many of the same, core concerns regarding undue secrecy remain. The President’s speech, the Policy Guidance, and Holder’s letter – because of textual ambiguities within each, and combined with events since – have largely failed to address these longstanding concerns, and in some important respects aggravated them.

Continuing Secrecy on Core Issues

Key areas in which transparency has not yet been forthcoming include:

 Who can be killed, where, and on what basis. Demands for legal and policy information on who and when the US believes it can kill have long been at the center of calls for more transparency. Senior US officials, before 2013, delivered important speeches outlining the government’s views on the applicable legal frameworks for targeting. But the speeches lacked detail, and left crucial legal questions unanswered. Legal concepts key to understanding the scope of US targeting – like “imminence,” “associated forces,” and “directly participating in hostilities” – remain unclear (see this and this). The relevant legal memos have still not been published, even in redacted form. In addition, although President Obama’s speech and the published Policy Guidance set out strict rules for the use of force – stricter, in numerous respects, than the laws of war – they are not legally binding, and we do not know when they began to apply, or when the strict policy limits on killing may be relaxed (and if we will ever be told when they are). And, crucially, we don’t know where the new guidelines actually apply (original assumptions by many outside government that they applied in Pakistan were later called into question). Since Obama’s May 2013 speech, confusion about who can be targeted has at times increased (e.g. a “senior American official” stated in August that a security threat had “expanded the scope” of who could be targeted in Yemen).

That increases mistrust—boosts opposition

Jack Goldsmith, Harvard Law School Professor, focus on national security law, presidential power, cybersecurity, and conflict of laws, Former Assistant Attorney General, Office of Legal Counsel, and Special Counsel to the Department of Defense, Hoover Institution Task Force on National Security and Law, 3/1/13, How Obama Undermined the War on Terror, [www.newrepublic.com/node/112964/print](http://www.newrepublic.com/node/112964/print)

Many in Congress want to increase the transparency of the processes and legal standards for placing a suspect (especially an American) on a targeting list, to tighten those legal standards (perhaps by recourse to a "drone court"), and to establish a more open accounting of the consequences (including civilian casualties) from the strikes. "This is now out in the public arena, and now it has to be addressed," Senator Dianne Feinstein, a Democrat, recently said.

Others in Congress worry about the obsolescence of the legal foundation for the way of the knife: the congressional authorization, in 2001, of force against Al Qaeda. "I don't believe many, if any, of us believed when we voted for [the authorization] that we were voting for the longest war in the history of the United States and putting a stamp of approval on a war policy against terrorism that, 10 years plus later, we're still using," said Senator Richard Durbin, also a Democrat, in a Wall Street Journal interview. "What are the checks and balances of the system?" he asked. Senator John McCain, who led bipartisan efforts against what he saw as Bush-era legal excesses, is now focusing similar attention on Obama. "I believe that we need to revisit this whole issue of the use of drones, who uses them, whether the CIA should become their own air force, what the oversight is, [and] what the legal and political foundations [are] for this kind of conflict," he said last month.

These are unhappy developments for the president who in his first inaugural address pledged with supercilious confidence that, unlike his predecessor, he would not expend the "rule of law" for "expedience's sake." Obama reportedly bristles at the legal and political questions about his secret war, and the lack of presidential trust that they imply. "This is not Dick Cheney we're talking about here," he recently pleaded to Democratic senators who complained about his administration's excessive secrecy on drones, according to Politico. And yet the president has ended up in this position because he committed the same sins that led Cheney and the administration in which he served to a similar place.

The first sin is an extraordinary institutional secrecy that Obama has long promised to reduce but has failed to. In part this results from any White House's inevitable tendency to seek maximum protection for its institutional privileges and prerogatives. The administration's disappointing resistance to sharing secret legal opinions about the secret war with even a small subset of Congress falls into this category.

But the point goes deeper, for secrecy is the essence of the type of war that Obama has chosen to fight. The intelligence-gathering in foreign countries needed for successful drone strikes there cannot be conducted openly. Nor can lethal operations in foreign countries easily be acknowledged. Foreign leaders usually insist on non-acknowledgment as a condition of allowing American operations in their territories. And in any event, an official American confirmation of the operations might spark controversies in those countries that would render the operations infeasible. The impossible-to-deny bin Laden raid was a necessary exception to these principles, and the United States is still living with the fallout in Pakistan.

For official secrecy abroad to work, the secrets must be kept at home as well. In speeches, interviews, and leaks, Obama's team has tried to explain why its operations abroad are lawful and prudent. But to comply with rules of classified information and covert action, the explanations are conveyed in limited, abstract, and often awkward terms. They usually raise more questions than they answer—and secrecy rules often preclude the administration from responding to follow-up questions, criticisms, and charges.

As a result, much of what the administration says about its secret war—about civilian casualties, or the validity of its legal analysis, or the quality of its internal deliberations—seems incomplete, self-serving, and ultimately non-credible. These trust-destroying tendencies are exacerbated by its persistent resistance to transparency demands from Congress, from the press, and from organizations such as the aclu that have sought to know more about the way of the knife through Freedom of Information Act requests.

A related sin is the Obama administration's surprising failure to secure formal congressional support. Nearly every element of Obama's secret war rests on laws—especially the congressional authorization of force (2001) and the covert action statute (1991)—designed for different tasks. The administration could have worked with Congress to update these laws, thereby forcing members of Congress to accept responsibility and take a stand, and putting the secret war on a firmer political and legal foundation. But doing so would have required extended political efforts, public argument, and the possibility that Congress might not give the president precisely what he wants.

The administration that embraced the way of the knife in order to lower the political costs of counterterrorism abroad found it easier to avoid political costs at home as well. But this choice deprived it of the many benefits of public argumentation and congressional support. What Donald Rumsfeld said self-critically of Bush-era unilateralism applies to Obama's unilateralism as well: it fails to "take fully into account the broader picture—the complete set of strategic considerations of a president fighting a protracted, unprecedented and unfamiliar war for which he would need sustained domestic and international support."

Instead of seeking contemporary congressional support, the administration has relied mostly on government lawyers' secret interpretive extensions of the old laws to authorize new operations against new enemies in more and more countries. The administration has great self-confidence in the quality of its stealth legal judgments. But as the Bush administration learned, secret legal interpretations are invariably more persuasive within the dark circle of executive branch secrecy than when exposed to public sunlight. On issues ranging from proper targeting standards, to the legality of killing American citizens, to what counts as an "imminent" attack warranting self-defensive measures, these secret legal interpretations—so reminiscent of the Bushian sin of unilateral legalism—have been less convincing in public, further contributing to presidential mistrust.

Feeling the heat from these developments, President Obama promised in his recent State of the Union address "to engage with Congress to ensure not only that our targeting, detention, and prosecution of terrorists remains consistent with our laws and system of checks and balances, but that our efforts are even more transparent to the American people and to the world." So far, this promise, like similar previous ones, remains unfulfilled.

The administration has floated the idea of "[shifting] the CIA's lethal targeting program to the Defense Department," as The Daily Beast reported last month. Among other potential virtues, this move might allow greater public transparency about the way of the knife to the extent that it would eliminate the covert action bar to public discussion. But JSOC's non-covert targeted killing program is no less secretive than the CIA's, and its congressional oversight is, if anything, less robust.

A bigger problem with this proposed fix is that it contemplates executive branch reorganization followed, in a best-case scenario, by more executive branch speeches and testimony about what it is doing in its stealth war. The proposal fails to grapple altogether with the growing mistrust of the administration's oblique representations about secret war. The president cannot establish trust in the way of the knife through internal moves and more words. Rather, he must take advantage of the separation of powers. Military detention, military commissions, and warrantless surveillance became more legitimate and less controversial during the Bush era because adversarial branches of government assessed the president's policies before altering and then approving them. President Obama should ask Congress to do the same with the way of the knife, even if it means that secret war abroad is harder to conduct.

Doesn’t solve legal clarity OR president ignores

Posner 11 Eric Posner is the Kirkland & Ellis Professor, University of Chicago Law School. “DEFERENCE TO THE EXECUTIVE IN THE UNITED STATES AFTER 9/11 CONGRESS, THE COURTS AND THE OFFICE OF LEGAL COUNSEL” available at http://www.law.uchicago.edu/academics/publiclaw/index.html.

C. Evidence

1. Testing the Three Hypotheses

We have three hypotheses about OLC on the table. The first is that OLC is an ex ante constraint on presidential power, serving a role similar to thatof Congress and the courts. The second is that OLC is an ex ante enabler of presidential power. The third hypothesis is Ackerman’s rubber-stamp theory that OLC serves neither as a constraint nor as an enabler because it cannot say no ex post. In this section, I will briefly discuss the evidence. It is easy enough to distinguish Ackerman’s hypothesis from the other two: if OLC never or rarely says no, then Ackerman is right. In addition, Ackerman is right even if OLC sometimes says no but the president ignores OLC in those cases. Distinguishing the constraint and enabler hypotheses is more difficult. Both hypotheses predict some ex post no’s. To distinguish the hypotheses, one would need to look at the other side of the ledger: the cases where OLC has enabled the president to act where otherwise Congress would have opposed him. Unfortunately, it would be hard to identify such cases. 2. Statistical Evidence In a study of the written opinions of OLC, Trevor Morrison found that 79 percent approved the president’s position, 8 percent provided a mixed answer, and 13 percent disapproved the president’s position. 26 In several cases, OLC rejected the White House position on issues of significance. In addition, Morrison notes that since OLC usually provides negative advice orally, the written record reflects a selection bias in favor of approvals. 27 But there is less here than meets the eye. First, one must keep in mind that the executive is a “they,” not an “it.” When the president cannot resolve policy differences among his major advisers, he may well be indifferent about OLC’s reaction and indeed welcome a legal resolution (“sorry, my hands are tied”). Second, the relevant focus, for the purpose of my argument, is OLC advice on national security issues. On this topic, the consensus appears to be that OLC has said no to the executive in only four cases in its entire history aside from matters that remain classified: the rejection of the Bush administration’s argument that the Geneva Conventions do not apply to terrorists in Iraq in 2002; 28 the rejection of certain forms of coercive interrogation in 2003; rejection of electronic surveillance that circumvented the FISA court in 2003; and rejection of the Libya intervention in 2011. 2 Even these cases turn out to be ambiguous. It must be recalled that OLC first said “yes” on coercive interrogation and electronic surveillance, and then changed its mind a few years later. In addition, OLC’s “no” on coercive interrogation turned out to be less than absolute: it continued to authorize waterboarding even after the earlier memorandum was withdrawn. Unfortunately, evaluating the empirical evidence is even harder than Morrison indicates. The problem is not just that negative advice is confidential; the problem is that we do not know how the executive responded to this negative advice. Did it desist from its conduct? Modify it along the margins? Or ignore OLC? Maybe, maybe not. A further methodological problem concerns whether a “no” blocks an important policy or simply requires certain i’s to bedotted or t’s to be crossed. OLC officials often emphasize that their job is to help the White House find a legally acceptable method of accomplishing their aims. Even the early Bush administration OLC drew the line on certain forms of torture (such as mock executions, the use of insects to exploit fears, etc.) and established guidelines to ensure the safety of detainees. The problem with treating this advice as a “no” is that it is not clear that the executive cared about these details, as opposedto the broad agenda of using coercive interrogation practices. It no doubt wanted legal advice so as to minimize the risk of legal liability. Finally, as we have seen, President Obama ignored OLC’s position on the Libya intervention. So in that case, OLC took a brave stand and then discovered that it had been pushed to the sidelines. This major event offered unusuallyrapid confirmation of Ackerman’s claim that the executive can avoid negative advice from OLC by soliciting advice from the White House Counsel’s Office. (Obama also received favorable advice from the State Department legal counsel.) Morrison argued prior to this event that the president faces strong disincentives to end-running OLC. 30 Afterwards, he could only criticize the president, claim he suffered from negative political fallout, and hope that this sort of thing does not happen too often. 31 However, while the president was criticized, there is simply no evidence that his evasion of OLC has hurt him politically. As is so often case, the (apparent) success of the operation provides its own justification. The upshot is that there is some evidence that OLC serves as an ex post constraint, but it is fairly weak. Ackerman’s hypothesis seems too extreme, but it is hard to distinguish between the constraint and enabler hypothesis. It is possible that OLC serves as a weak constraint or a weak enabler. Why has it been so weak? First,it may turn out that the constellation of factors that drive decisionmaking in the executive branch prevents the president from solving a time-inconsistency problem by using OLC. The president benefits fromneutral advice, and frombeing able to cite OLC’s approval, but when OLC blocks the president, short-term political considerations trump the medium-term advantages of maintaining a neutral OLC. Meanwhile, OLC’s lawyers yield to political pressure either for careerist reasons or in order to prevent the president from cutting OLC out of the process. Private lawyers face similar pressures, but the market in legal services might provide some additional discipline. Second, the problem might lie in the nature offoreign relations and national security, an area of action that has been notoriously difficult to bring under legal control. Courts have frequently been asked to adjudicate disputes between Congress and the president inthe area of national security. Generally speaking, they have resisted these requests, treating these issues as political questions or nonjusticiable for other reasons. The usual explanation for this resistance is that courts are not experts on these issues; that the highly fluid, frequently changing nature of foreign relations and national security makes themunsuitable for judicial resolution, which is rule-bound, public, decentralized, and slow; and that, accordingly, courts fear that if they intervene, their rulings will be ignored by the executive branch, provoking a constitutional crisis. The supposed solution to this problem is to ask an advisory office in the executive branch to take over a function that the courts have repudiated. It is true that a small office in the executive branch can overcome certain problems that courts face relating to secrecy and speed. But the fundamental problem is that foreign relations are not susceptible to regulation by rules. 32

Congress circumvents signal

Waxman 8/25/13 (Matthew Waxman is a law professor at Columbia Law School, where he co-chairs the Roger Hertog Program on Law and National Security. He is also Adjunct Senior Fellow for Law and Foreign Policy at the Council on Foreign Relations and a member of the Hoover Institution Task Force on National Security and Law. He previously served in senior policy positions at the State Department, Defense Department, and National Security Council. After graduating from Yale Law School, he clerked for Judge Joel M. Flaum of the U.S. Court of Appeals and Supreme Court Justice David H. Souter, “The Constitutional Power to Threaten War” Forthcoming in YALE LAW JOURNAL, vol. 123, 2014, August 25th DRAFT)

The formal participation of political opponents in legislative bodies provides them with a forum for registering dissent to presidential policies of force through such mechanisms floor statements, committee oversight hearings, resolution votes, and funding decisions. 147 **These official actions prevent the President “from monopolizing the nation’s political discourse”** on decisions regarding military actions can thereby make it difficult for the President to depart too far from congressional preferences. 148 Members of the political opposition in Congress also have access to resources for gathering policyrelevant information from the government that informs their policy preferences. Their active participation in specialized legislative committees similarly gives opponent party members access to fact-finding resources and forums for registering informed dissent from decisions within the committee’s purview. 149 As a result, legislative institutions within democracies can enable political opponents to have a more immediate and informed impact on executive’s decisions regarding force than can opponents among the general public. Moreover, studies suggest that Congress can actively shape media coverage and public support for a president’s foreign policy engagements. 150 In short, these findings among political scientists suggest that, even without having to pass legislation or formally approve of actions, Congress often operates as an important check on threatened force by providing the president’s political opponents with a forum for registering dissent from the executive’s decisions regarding force in ways that attach domestic political costs to contemplated military actions or even the threats to use force.

Under this logic, **Presidents, anticipating dissent, will be more selective in issuing threats** in the first place, making only those commitments that would not incite widespread political opposition should the threat be carried through. 151 Political opponents within a legislature also have few electoral incentives to collude in an executive’s bluff, and they are capable of expressing opposition to a threatened use of force in ways that could expose the bluff to a threatened adversary. 152 This again narrows the President’s range of viable policy options for brandishing military force.

Counter-intuitively, given the President’s seemingly unlimited and unchallenged constitutional power to threaten war, **it may** in some cases **be easier for** members of **Congress to influence presidential decisions to threaten military action than** presidential war decisions **once U.S. forces are already engaged** in hostilities. It is widely believed that once U.S. armed forces are fighting, congressmembers’ hands are often tied: policy opposition at that stage risks being portrayed as undermining our troops in the field. 153 Perhaps, it could be argued, the President takes this phenomenon into account and therefore discounts political opposition to threatened force; he can assume that such opposition will dissipate if he carries it through. Even if that is true, **before that point occurs**, however, members of **Congress may have communicated messages domestically and communicated signals abroad that the President will find difficult to counter**. 154

## WAR POWERS NB

Congressional authority of cyber activities strengthens Presidential power – squo unchecked Prez authority hamstrings legitimacy

Chen 12 (Julia – JD Candidate @ Boston College (2013) specializing in National Security, MEM in Engineering Management from Old Dominion, BA – Rice University, “NOTE: RESTORING CONSTITUTIONAL BALANCE: ACCOMMODATING THE EVOLUTION OF WAR” November, 2012, 53 B.C. L. Rev 1767)

Although courts have not made decisive rulings on the division of war powers between the political branches, they have provided guidance on the scope of executive power generally. n156 In 1952, in Youngstown Sheet and Tube Co. v. Sawyer, the Supreme Court held that an executive order to seize steel mills to prevent a wartime strike was unconstitutional. n157 Justice Robert Jackson's concurring opinion outlined three zones of presidential power. n158 Courts often reference this opinion to analyze the constitutionality of executive actions. n159 Justice Jackson's first zone exists when "the President acts pursuant to an express or implied authorization of Congress." n160 In this zone, presidential authority is at its [\*1784] zenith, because it encompasses the executive power as well as congressional power. n161 Actions taken in the first zone are presumed to be lawful. n162 Justice Jackson's second zone includes actions the President takes with neither approval nor disapproval by Congress. n163 In this zone, the President relies solely on the executive power, and there is a "zone of twilight" in which the allocation of constitutional powers is uncertain. n164 According to Justice Jackson, the general constitutionality of actions in this second zone is unclear. n165 The third zone includes actions taken by the President that are "incompatible with the . . . will of Congress." n166 In this zone, presidential "power is at its lowest ebb," and the constitutionality of presidential actions is most suspect. n167 In Youngstown, Justice Jackson concluded that the President was acting in the third zone, where constitutionality is most doubtful, because Congress had explicitly taken actions contrary to the presidential action. n168

In summary, the Court has addressed the broader subject of executive power, but it has been unwilling to rule on the specific war powers question. n169 Instead, it defers that question to the political branches. n170 War powers were allocated to the legislative and executive branches by the Framers, who implemented structural checks and balances to avoid tyranny. n171 The War Powers Resolution was an attempt by Congress to deal with the war powers question, reasserting its power over war, by forcing the President to seek congressional approval. n172 Applying Justice Jackson's reasoning in Youngstown, congressional approval of presidential decisions to go to war would strengthen the constitutionality of the executive decision. n173 Modern warfare, however, is growing outside the strictures of the War Powers Resolution. n174 Specifically, modern warfare [\*1785] technologies and methods allow the President to act without the approval of Congress, thereby asserting more war-making power. n175

II. MODERN WARFARE CARVES OUT INCREASING EXECUTIVE POWER

The ambiguity in congressional and presidential war powers augments the tension between the President's desire to enter foreign wars and Congress's inherent reticence as direct representatives of the people. n176 This ambiguity creates a risk that presidential power will increase if unchecked. n177 Furthermore, modern technological and warfare developments increase the potential for aggrandizing the executive power. n178

Section A of this Part explains that modern wars are fought by government civilians and contractors as much as, and sometimes more than, they are fought by military personnel. n179 Section B then describes how improvements in military technology are changing the modes by which countries wage war. n180 Section C presents the 2011 action in Libya as an example, provides an analysis of the executive's claims that the action in Libya was outside the scope of the War Powers Resolution, and demonstrates that the Resolution is an insufficient check on executive power in the context of modern conflicts. n181 This Part suggests that against the backdrop of the outmoded statute and judicial refusal to settle the war powers dispute, the legislative branch is ceding war-making power to the President. n182

A. The Cast of Characters Is Changing: The "Who" of Modern Warfare

Civilians have always been involved in military operations, but the level of involvement today is unprecedented. n183 By some accounts, civilians hold half of all defense-related jobs. n184 Many of these civilians serve in logistics- and support-related roles, such as cleaning offices, doing [\*1786] the laundry, and maintaining roads for the military. n185 Still others have much more direct involvement, such as in combat missions, protecting dignitaries, and possibly targeting terrorists in impenetrable areas of the world. n186

Civilian operatives of the CIA's clandestine service deployed to hostile environments now perform roles once reserved for military personnel. n187 This change in CIA operations stemmed from the events of September 11, 2001 and the resulting Global War on Terror. n188 The CIA's intelligence directorate deploys more personnel overseas than ever before, and forms strong relationships with foreign military personnel and intelligence agencies to deepen their knowledge of terrorist activities. n189 Moreover, the CIA operates unmanned aerial vehicles (UAVs) out of remote bases in Pakistan and Afghanistan, conducting missile and bomb strikes on targets. n190 The CIA's overseas intelligence network contributes significantly to military operations, such as the raid into Pakistan that killed Osama Bin Laden in May 2011. n191 Furthermore, many CIA personnel die in overseas deployments such as the seven that died in an ambush on their remote post in Afghanistan in December 2009. n192

Nonetheless, the CIA does not act alone; they, like the military, increasingly bring contractors to the fight. n193 In June 2009, the CIA director revealed to Congress that in 2004, the CIA had hired outside contractors to locate and assassinate terrorist leaders. n194 Outside contractors had previously been hired to interrogate terrorists, but not for lethal means. n195 Contractors are trained to load Hellfire missiles and [\*1787] laser-guided bombs on UAVs, and serve alongside the CIA and military personnel at UAV bases. n196 Still, this revelation that contractors helped with planning, training, surveillance, and possibly even targeting terrorists for capture or assassination was the first evidence that the CIA's covert programs were directly using contractors for lethal means. n197 The CIA director ended the program after determining that it was unsuccessful. n198 Yet the classified program had operated for seven years and spent millions of dollars, without notification to the congressional committees charged with oversight of the intelligence community. n199

There are several reasons for the increase in civilians at war, including cost concerns, institutional memory, and expertise. n200 The maintenance of military and civilian government personnel is very expensive, providing incentive to outsource jobs to contractors that will cost the government less money. n201 Furthermore, the complexity of modern weaponry frequently necessitates bringing civilian contractors along for maintenance and sometimes even operation of equipment. n202 Additionally, many weapons, such as UAVs, can be operated remotely, and there is seemingly no need to have a military pilot in that job when a contractor could do it just as well. n203 Sometimes contractors have even better capabilities to accomplish a mission than the government personnel that hire them. n204 Civilian contractors do not have the frequent personnel transfers that military personnel encounter; thus the contractors can spend more time training with complex equipment, becoming the unit's institutional memory. n205 Finally, it may be easier politically to send the CIA and other civilians into a conflict than to deploy the military, because the executive is not required to justify publicly [\*1788] the requirement to Congress. n206 Thus, civilians have emerged as a significant component of modern warfare. n207

B. Modern Warfare Methods Change the Character of War

Senator Thomas Eagleton's prediction that activities outside the scope of the War Powers Resolution would increase has become a reality. n208 In addition to a change in participants, development of technology is changing the methods of warfare in the modern era. n209 New technology decreases the risk of injury or death for humans that have the assistance of improved intelligence, firepower support, and long-range automated capabilities. n210 Furthermore, technology has the potential to reduce severely the need for humans to operate a foreign war. n211 Thus, war waged remotely, as made possible by these technological advances, is beyond the scope of "war" as contemplated by the War Powers Resolution. n212

1. Use of Unmanned Aerial Vehicles

The use of UAVs is outside the bounds of what the 1973 drafters of the War Powers Resolution envisioned. n213 Between the years 2000 and 2010, the number of UAVs used to support military operations grew from under fifty to over six thousand, ushering in a new era of warfare. n214 The American government, including the Pentagon and the CIA, has created an extensive support network including several operational bases in the United States and around the world. n215 As of 2012, more military pilots are being trained for and more hours are being flown by American UAVs than conventional aircraft. n216

UAVs are not just unmanned planes; rather they have enhanced capabilities that make military operations more effective. n217 The Reaper MQ-9 aircraft, for example, can loiter above a target for up to twenty-four [\*1789] hours, microscopically observe activities on the ground from an altitude of up to five miles, transmit real-time video to its controllers on the other side of the world, and fire a missile at the target with meticulous precision. n218 Thus, UAVs bring unprecedented surveillance, intelligence, and strike capabilities to the warfighter. n219 Moreover, the use of UAVs allows the United States to attack military targets and avoid the high civilian death rates that occurred during bygone wars. n220 Thus, one of the biggest advantages UAVs bring is that they take the pilot out of hostile situations. n221 UAVs can fly missions that would be too dangerous for a manned aircraft, such as surveillance or air sampling after a chemical attack. n222 Ultimately UAVs make new combat missions possible and may make war-fighting efforts more effective. n223

The use of UAVs changes the risks of combat scenarios, because it eliminates the human cost of putting troops on the ground. n224 Whereas historically, politicians have weighed the political cost of putting American forces in hostile situations, UAVs remove this barrier. n225 By minimizing American casualties, UAVs remove the emotional tie between public approval of war and the military. n226 This removes the need for the President to demonstrate to the American public that the human costs of war are worth the overall benefit to the nation. n227 Thus, although UAVs may increase targeting accuracy in combat, enabling the United States to prosecute more effective wars, they may also lower political hurdles to entering combat situations. n228

 [\*1790] 2. Use of Cyber-Warfare

Another type of warfare not anticipated by the drafters of the War Powers Resolution is cyber-warfare. n229 It can be used as a tool to support the nation's interests in many different ways: to collect information on the enemy, to optimize the use of the nation's weaponry, to disrupt the computer network that controls the enemy's weaponry, to directly attack the enemy's national infrastructure, or to impact morale. n230 Cyber-warfare does not leave the footprints of conventional warfare, and thus it can inflict damage on another country anonymously. n231 This anonymity allows an attacker to make an impact without affecting international relations, and potentially without political impact at home. n232 Furthermore, there are no restraints on the personnel that can conduct cyber-attacks. n233 These activities are easily outsourced to private industry, and tasking is easily dispersed to multiple entities, making an attack even more difficult to trace. n234 Moreover, because cyber-warfare is conducted remotely, it does not require troops on the ground, and thus it would not be subject to the War Powers Resolution. n235

In October 2012, U.S. Secretary of Defense Leon Panetta warned that America, like other nations, is at risk of a "'cyber Pearl Harbor:' an attack that would cause physical destruction and the loss of life." n236 In May 2007, Estonian authorities experienced such an attack when they [\*1791] removed a World War II-era Soviet statue from a park. n237 They did not anticipate that such a cyber-attack would threaten their national security. n238 The distributed denial-of-service attack rapidly increased traffic to websites, depleted available bandwidth, caused websites to crash, and threatened the nation's electronic infrastructure, forcing the Estonian government to defend its population and commerce. n239 As the Estonian technicians attempted to block their connections to international servers, the actions were analogous to a conventional "blockade" of the nation's access points to the rest of the world. n240 This was the first case of a cyber-attack crippling an entire nation, but it may be just the beginning of a new frontier in warfare. n241

There are indications that the United States is using cyber-warfare in its secret war against the Iranian nuclear weapons program. n242 Sometime in 2009, a software program was introduced into the Iranian computer network. n243 The program, which is now known as Stuxnet, made its way through the computer system and sabotaged its designated target: nuclear centrifuges that are vital to the Iranian weapons program. n244 Then in May 2012, Iran announced that computers used by [\*1792] many of their high-ranking officials were attacked by a data collecting and reporting virus called Flame. n245 It is widely believed that both Stuxnet and Flame were joint operations by the American and Israeli governments, although neither country has claimed responsibility. n246

C. The Conflict in Libya: Illustrating the Limits of the War Powers Resolution

The 2011 conflict in Libya demonstrates that the use of these modern warfare methods is outside the bounds of the War Powers Resolution of 1973, and thus evades a legislative check on executive power. n247 On March 19, 2011, President Barack Obama ordered American forces to join a NATO operation in Libya, without congressional authorization. n248 On June 14, Speaker of the House John Boehner sent a letter to the President, warning him that he would soon be in violation of the time limits established by the War Powers Resolution, because the President had not received authorization from Congress for the action in Libya. n249 The next day, the White House sent a report to Congress, asserting that the level of American involvement in Libya was less than "hostilities," and thus fell outside the scope of the Resolution. n250 The report asserted that because the operations did "not involve sustained fighting or active exchanges of fire with hostile forces, nor [did] they involve the presence of U.S. ground troops, U.S. casualties, or a serious threat thereof," the actions were different from those contemplated by the Resolution. n251 The next day, Speaker Boehner responded that with UAV attacks underway and the military spending ten million dollars a day on the effort, he did not understand how the United States was not engaged in "hostilities." n252

 [\*1793] On June 28, 2011, Senator John Kerry held a hearing before the Senate Committee on Foreign Relations regarding the War Powers Resolution and America's use of force in Libya. n253 In his opening statement, Senator Kerry asserted that he supported the administration's position that action in Libya was outside the scope of the Resolution. n254 He explained that the Resolution was drafted in response to the Vietnam War and was written to provide guidance for "a particular kind of war, to a particular set of events." n255 Senator Kerry reasoned that after many years of fighting and the loss of almost 60,000 American lives in Vietnam, Congress drafted the law to ensure that the legislative branch would be able to weigh in before American soldiers are sent abroad. n256 At this point, Senator Kerry drew a contrast with the conflict in Libya, which was "a very limited operation" and did not involve American armed forces in "hostilities." n257

Senator Richard Lugar, the ranking member of the Committee, expressed dismay that the President acted unilaterally without seeking congressional authorization to initiate military action in Libya. n258 He expressed that even if the President did have the legal authority to initiate a war without congressional approval, that did not mean the action was "wise or helpful to the operation." n259 He suggested that most people educated on the matter would agree that the President should "seek congressional authorization for war when circumstances allow." n260

Harold Koh, a legal advisor to the U.S. Department of State, explained the administration's legal position on war powers. n261 The American military activity in Libya was limited largely to providing intelligence and refueling for NATO allies. n262 The administration's view was that in cases like this when the military engages in a "limited military [\*1794] mission that involves limited exposure for U.S. troops and limited risk of serious escalation and employs limited military means," the "hostilities" are not covered by the Resolution. n263

Mr. Koh, like Senator Kerry, differentiated the action from those envisioned by the drafters of the War Powers Resolution. n264 Unlike previous administrations, the Obama administration did not challenge the constitutionality of the Resolution. n265 Rather, it argued that the Resolution was drafted to "play a particular role," and that to "play that role effectively in this century" the Resolution would require modification. n266 The Resolution regulates "the introduction of U.S. Armed Forces into hostilities." n267 As Mr. Koh explained, the Resolution does not address the situation of "unmanned uses of weapons that can deliver huge volumes of violence," such as UAVs. n268 Thus the administration claimed that there was a large hole in the Resolution for combat activities employing unmanned weaponry. n269

Clearly, the use of technologies such as UAVs and cyber-attacks in modern warfare are outside the bounds of the War Powers Resolution as it currently stands. n270 This removes a legislative check on executive power, and when considered in light of historical views on the balance of power, augments executive power. n271 Although some consider modern warfare methods to be a legitimate augmentation of executive power, others believe that the Resolution should be amended to provide a legislative check to this power. n272

III. RESTORING THE NECESSARY BALANCE OF POWER

This Part argues for the restoration of balance between the executive and legislative branches in light of the nature of modern warfare [\*1795] and limitations of the War Powers Resolution. n273 It asserts that the Resolution can no longer accomplish its intended purpose and should be replaced by new war powers framework legislation. n274 As Senator Thomas Eagleton stated in his attempt to broaden the Resolution, "[e]ither we are involved in hostilities or we are not." n275 Thus, the law should be written to "match the realities of war." n276

Section A asserts that the War Powers Resolution is outdated. n277 Modern warfare is happening outside the bounds of the Resolution, and the U.S. Constitution's system of checks and balances calls for recalibrating the balance. n278 Section B proposes new framework legislation on war powers. n279 It endorses broader legislation to accommodate inevitable changes in future technology. n280 It also recognizes that much of modern warfare is reliant on covert operations. n281 Thus, the legislation should be bifurcated to accommodate open as well as covert warfare. n282

A. The Balance of War Powers Is Out of Kilter

Since the framing of the Constitution, the American commitment to separation and balance of powers has been seen as necessary for preventing tyranny. n283 In response to unilateral action by the executive, Congress attempted to reassert its prerogative over war powers in 1973. n284 Although broad issues prompted the statute, the result was a [\*1796] limited doctrine. n285 Its limitations on presidential power are now constrained by its own parameters as the Resolution applies only to military personnel. n286 Thus, over time, warfare outgrew the strictures established by the Resolution, and executive control over war is once again overly powerful. n287

1. The Need for Balance of Powers

The American constitutional democracy's system of checks and balances supports a "joint decision" system. n288 This model of decision making gives the President the unilateral power to make war, without authorization from Congress, only in emergency situations. n289 These scenarios include the need to fend off an attack on the United States, to prevent an imminent attack, and to protect American citizens whose lives are threatened, as opposed to scenarios involving a "sustained use of force." n290 Conversely, any use of armed forces for sustained operations and non-emergencies should require consultation with Congress. n291 This division of powers between the branches of government ensures that the decision to bring the nation into war--a significant decision that the American people pay for with their lives and money--is scrutinized by both political branches. n292

The negotiations over the powers allocated to the executive and legislative branches during the Constitution's drafting lend support to this view. n293 It was asserted that the legislative branch would proceed too slowly to respond to and appropriately repel attacks on the nation. n294 [\*1797] Still, the Framers thought it was necessary to change the wording to give the President the power to act in emergency situations. n295 Thus the meaning of "declare war" was likely understood by the Framers as power over war-making decisions, excluding defensive and emergency situations. n296 Their debate implies that outside of the necessity for the President to repel attacks, the power to "make war" remains with Congress. n297

Furthermore, when the Framers discussed war powers, they did not envision actions by only the military. n298 Rather, they envisioned control over both public and private actors in war. n299 The congressional power to grant letters of marque and reprisal lends support to this view. n300 This power brought privately owned ships into the service of the nation to capture and kill enemy forces. n301 Letters of marque and reprisal were vital to the nation in the late eighteenth century, because at the time, the United States did not have a sufficient Navy to stand up against the power of the large British Navy. n302 Rather, the United States had to get assistance from civilian vessels. n303 Similarly, modern warfare is better fought with the use of civilian augmenters. n304 The military relies on government civilians and contractors to increase capabilities at war. n305 Thus, just as Congress was given power to grant letters of marque and reprisal, it should have authority over the reality of modern day civilians at war. n306

 [\*1798] An appropriate balance of powers is evidenced in modern statutes, such as the Intelligence Oversight Act of 1991. n307 Although the statute acknowledges the importance of covert activities to national security, it works within the framework of the Constitution. n308 The Act requires the executive to keep the congressional oversight committees "fully and currently informed of the intelligence activities." n309 Thus, it is understood that the President must sanction covert activities for national security, but that the activities are subject to scrutiny by members of Congress. n310 This allows for further review and political debate by representatives of the nation on issues that affect the nation. n311 Lack of adherence to this system could result in the tyranny so feared by the Framers. n312

History disproves their impact

Bradley et al ‘12

Curtis A. Bradley, Sarah H. Cleveland, The Honorable Brett M. Kavanaugh, Martin S. Lederman, Judith Resnik and Stephen I. Vladeck, “WAR, TERROR, AND THE FEDERAL COURTS, TEN YEARS AFTER 9/11: CONFERENCE\*: ASSOCIATION OF AMERICAN LAW SCHOOLS' SECTION ON FEDERAL COURTS PROGRAM AT THE 2012 AALS ANNUAL MEETING IN WASHINGTON, D.C.,” 61 Am. U.L. Rev. 1253

So where are we? Marty mentioned a word that had not been mentioned before, which was "Congress." What's the big picture of where we are right now in terms of federal courts, separation of powers, war powers? I would start with, in the wake of September 11th, Congress authorizing two wars: it authorized the war against Al-Qaeda and the Taliban, and authorized the war in Iraq. That itself is a significant precedent. When you ask, twenty years from now, thirty years from now, what's the most significant precedent arising out of the post-9/11 years? I think one of them, if not the most important, will be that those were congressionally authorized wars. **A President, who in the future tries to engage in an unauthorized ground war of any significance,** will be faced with those precedents used against them. President Bush obtained authorization for those two wars. Second. As Marty's article with David Barron points out so well, Congress has regulated the Executive's conduct of war in many respects, both before and after September 11th. We tend to forget that and sometimes think, well this is all just the Executive Branch operating in kind of a free zone, free from congressional restraint. And in fact, whether it's interrogation or detention, surveillance, a number of particulars of how the **Executive goes about the war effort**, Congress has been deeply involved, including in the wake of September 11th. I think it's very important to remember Congress's role there. And then third - and this was not self-evident on September 12th - the courts have played a significant role, as Sarah mentioned, in enforcing restrictions on the Executive's conduct of war. Where was the political question doctrine in Hamdi or Hamdan? Nowhere to be found. Nowhere to be found. What about the President's exclusive, preclusive Article II power, to ignore congressional restrictions or disregard congressional restrictions, depending on - what's the scope of that? Not a single Justice in Hamdi or Hamdan suggested that detention or activities related to detainees were within the exclusive, preclusive power of the President. Hamdan, footnote twenty-three, I think, pointedly ends with, "The government does not argue otherwise." Which was a recognition that not even the Executive Branch was asserting in that case, an exclusive, preclusive power. So the political question doctrine has not played a major role. The exclusive, preclusive power of the President was the big issue raised by some of the OLC opinions [\*1268] in 2002/2003, but the Bush Administration later backed away from it, culminating in the January 15, 2009 OLC memo for the file essentially but publicly retracting or distancing itself from a number of prior OLC memos. So the courts are playing a role in enforcing congressional restrictions.

Opposition is inevitable and outweighs the link

Howell ‘7

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

It is of some consequence, then, that we find so much evidence that the partisan composition of Congress factors into presidential decision making about the nation's response to assorted foreign crises. Estimating a wide range of statistical models, we find that those presidents who face large and cohesive congressional majorities from the opposite party exercise military force less regularly than do those whose party has secured a larger number of seats within Congress. Additionally, other statistical models reveal that partisan opposition to the president **reliably depresses** the likelihood of a military response to specific crises occurring abroad and significantly extends the amount of time that transpires between the precipitating event and the eventual deployment. Modern presidents consistently heed the distinctly political threat posed by large, cohesive, and opposing congressional majorities—a threat that is all too often latent, but that when mobilized, materially affects the president's efforts to rally public support for an ongoing deployment and to communicate the nation's foreign policy commitments to both allies and adversaries abroad.

Spillover bolsters credibility of threats

Waxman 8/25/13 (Matthew Waxman is a law professor at Columbia Law School, where he co-chairs the Roger Hertog Program on Law and National Security. He is also Adjunct Senior Fellow for Law and Foreign Policy at the Council on Foreign Relations and a member of the Hoover Institution Task Force on National Security and Law. He previously served in senior policy positions at the State Department, Defense Department, and National Security Council. After graduating from Yale Law School, he clerked for Judge Joel M. Flaum of the U.S. Court of Appeals and Supreme Court Justice David H. Souter, “The Constitutional Power to Threaten War” Forthcoming in YALE LAW JOURNAL, vol. 123, 2014, August 25th DRAFT)

Part II draws on several strands of political science literature to illuminate the relationship between war powers law and threats of force. As a descriptive matter, the swelling scope of the president’s practice in wielding threatened force largely tracks the standard historical narrative of war powers shifting from Congress to the President. Indeed, adding threats of force to that story might suggest that this shift in powers of war and peace has been even more dramatic than usually supposed, at least in terms of how formal congressional checks are exercised.

Part II also shows, however, that congressional checks and influence – even if not formal legislative powers – operate more robustly and in different ways to shape strategic decision-making than usually supposed in legal debates about war powers, and that **these checks and influence can enhance the potency of threatened force**. This Article thus fits into a broader scholarly debate now raging about the extent to which the modern President is meaningfully constrained by law, and in what ways. 20 Recent political science scholarship suggests that Congress already exerts constraining influences on presidential decisions to threaten force, even without resorting to binding legislative actions. 21 Moreover, when U.S. security strategy relies heavily on threats of force, credibility of signals is paramount. Whereas it often used to be assumed that institutional checks on executive discretion undermined democracies’ ability to threaten war credibly, some **recent political science scholarship** also offers reasons to expect that congressional political constraints can actually bolster the credibility of U.S. threats. 22

Syria pounds

Nather and Palmer, 9-1-13

[David and Anna, Politico, Bushies fear Obama weakening presidency, <http://www.politico.com/story/2013/09/bushies-fear-obama-weakening-presidency-96143.html>]

President Barack **Obama** just turned decades of debate over presidential war powers on its head. Until Saturday, when Obama went to Congress to ask for permission to strike Syria, the power to launch military action had been strongly in the hands of the commander in chief. Even the 1973 War Powers Resolution allows bombs to start falling before the president has to ask Congress for long-term approval. For three decades after Watergate, conservatives like Dick Cheney and those of his ilk sought to increase executive branch power that they felt had been eroded by liberal congressional reformers. George W. Bush’s legal team crafted controversial opinions that emboldened the White House on a wide range of national security areas, from interrogation to surveillance. That makes the move by Obama to hand a piece of the messy situation in Syria to Congress a clear step in the other direction — an abdication of power to Congress at a moment when he has no good solutions. And even if Obama ultimately balks at Congress if they vote down his ask, prominent conservatives who fueled the expansion of presidential power — especially Bush administration alums — are beside themselves, arguing that Obama has weakened the presidency.

## k

Legal restraints work – the theory of the exception is self-serving and wrong

William E. Scheuerman 6, Professor of Political Science at Indiana University, Carl Schmitt and the Road to Abu Ghraib, Constellations, Volume 13, Issue 1

Yet this argument relies on Schmitt’s controversial model of politics, as outlined eloquently but unconvincingly in his famous Concept of the Political. To be sure, there are intense conflicts in which it is naïve to expect an easy resolution by legal or juridical means. But the argument suffers from a troubling circularity: Schmitt occasionally wants to define “political” conflicts as those irresolvable by legal or juridical devices in order then to argue against legal or juridical solutions to them. The claim also suffers from a certain vagueness and lack of conceptual precision. At times, it seems to be directed against trying to resolve conflicts in the courts or juridical system narrowly understood; at other times it is directed against any legal regulation of intense conflict. The former argument is surely stronger than the latter. After all, legal devices have undoubtedly played a positive role in taming or at least minimizing the potential dangers of harsh political antagonisms. In the Cold War, for example, international law contributed to the peaceful resolution of conflicts which otherwise might have exploded into horrific violence, even if attempts to bring such conflicts before an international court or tribunal probably would have failed.22

Second, Schmitt dwells on the legal inconsistencies that result from modifying the traditional state-centered system of international law by expanding protections to non-state fighters. His view is that irregular combatants logically enjoyed no protections in the state-centered Westphalian model. By broadening protections to include them, international law helps undermine the traditional state system and its accompanying legal framework. Why is this troubling? The most obvious answer is that Schmitt believes that the traditional state system is normatively superior to recent attempts to modify it by, for example, extending international human rights protections to individuals against states. 23 But what if we refuse to endorse his nostalgic preference for the traditional state system? Then a sympathetic reading of the argument would take the form of suggesting that the project of regulating irregular combatants by ordinary law must fail for another reason: it rests on a misguided quest to integrate incongruent models of interstate relations and international law. We cannot, in short, maintain core features of the (state-centered) Westphalian system while extending ambitious new protections to non-state actors.

This is a powerful argument, but it remains flawed. Every modern legal order rests on diverse and even conflicting normative elements and ideals, in part because human existence itself is always “in transition.” When one examines the so-called classical liberal legal systems of nineteenth-century England or the United States, for example, one quickly identifies liberal elements coexisting uneasily alongside paternalistic and authoritarian (e.g., the law of slavery in the United States), monarchist, as well as republican and communitarian moments. The same may be said of the legal moorings of the modern welfare state, which arguably rest on a hodgepodge of socialist, liberal, and Christian and even Catholic (for example, in some European maternity policies) programmatic sources. In short, it is by no means self-evident that trying to give coherent legal form to a transitional political and social moment is always doomed to fail. Moreover, there may be sound reasons for claiming that the contemporary transitional juncture in the rules of war is by no means as incongruent as Schmitt asserts. In some recent accounts, the general trend towards extending basic protections to non-state actors is plausibly interpreted in a more positive – and by no means incoherent – light.24

Third, Schmitt identifies a deep tension between the classical quest for codified and stable law and the empirical reality of a social world subject to permanent change: “The tendency to modify or even dissolve classical [legal] concepts…is general, and in view of the rapid change of the world it is entirely understandable” (12). Schmitt’s postwar writings include many provocative comments about what contemporary legal scholars describe as the dilemma of legal obsolescence. 25 In The Partisan, he suggests that the “great transformations and modifications” in the technological apparatus of modern warfare place strains on the aspiration for cogent legal norms capable of regulating human affairs (17; see also 48–50). Given the ever-changing character of warfare and the fast pace of change in military technology, it inevitably proves difficult to codify a set of cogent and stable rules of war. The Geneva Convention proviso that legal combatants must bear their weapons openly, for example, seems poorly attuned to a world where military might ultimately depends on nuclear silos buried deep beneath the surface of the earth, and not the success of traditional standing armies massed in battle on the open field. “Or what does the requirement mean of an insignia visible from afar in night battle, or in battle with the long-range weapons of modern technology of war?” (17).

As I have tried to show elsewhere, these are powerful considerations deserving of close scrutiny; Schmitt is probably right to argue that the enigma of legal obsolescence takes on special significance in the context of rapid-fire social change.26 Unfortunately, he seems uninterested in the slightest possibility that we might successfully adapt the process of lawmaking to our dynamic social universe. To be sure, he discusses the “motorization of lawmaking” in a fascinating 1950 publication, but only in order to underscore its pathological core.27 Yet one possible resolution of the dilemma he describes would be to figure how to reform the process whereby rules of war are adapted to novel changes in military affairs in order to minimize the danger of anachronistic or out-of-date law. Instead, Schmitt simply employs the dilemma of legal obsolescence as a battering ram against the rule of law and the quest to develop a legal apparatus suited to the special problem of irregular combatants.

Legal norms don’t cause wars and the alt can’t effect liberalism

David Luban 10, law prof at Georgetown, Beyond Traditional Concepts of Lawfare: Carl Schmitt and the Critique of Lawfare, 43 Case W. Res. J. Int'l L. 457

Among these associations is the positive, constructive side of politics, the very foundation of Aristotle's conception of politics, which Schmitt completely ignores. Politics, we often say, is the art of the possible. It is the medium for organizing all human cooperation. Peaceable civilization, civil institutions, and elemental tasks such as collecting the garbage and delivering food to hungry mouths all depend on politics. Of course, peering into the sausage factory of even such mundane municipal institutions as the town mayor's office will reveal plenty of nasty politicking, jockeying for position and patronage, and downright corruption. Schmitt sneers at these as "banal forms of politics, . . . all sorts of tactics and practices, competitions and intrigues" and dismisses them contemptuously as "parasite- and caricature-like formations." n55 The fact is that Schmitt has nothing whatever to say about the constructive side of politics, and his entire theory focuses on enemies, not friends. In my small community, political meetings debate issues as trivial as whether to close a street and divert the traffic to another street. It is hard to see mortal combat as even a remote possibility in such disputes, and so, in Schmitt's view, they would not count as politics, but merely administration. Yet issues like these are the stuff of peaceable human politics.

Schmitt, I have said, uses the word "political" polemically--in his sense, politically. I have suggested that his very choice of the word "political" to describe mortal enmity is tendentious, attaching to mortal enmity Aristotelian and republican associations quite foreign to it. But the more basic point is that Schmitt's critique of humanitarianism as political and polemical is itself political and polemical. In a word, the critique of lawfare is itself lawfare. It is self-undermining because to the extent that it succeeds in showing that lawfare is illegitimate, it de-legitimizes itself.

What about the merits of Schmitt's critique of humanitarianism? His argument is straightforward: either humanitarianism is toothless and [\*471] apolitical, in which case ruthless political actors will destroy the humanitarians; or else humanitarianism is a fighting faith, in which case it has succumbed to the political but made matters worse, because wars on behalf of humanity are the most inhuman wars of all. Liberal humanitarianism is either too weak or too savage.

The argument has obvious merit. When Schmitt wrote in 1932 that wars against "outlaws of humanity" would be the most horrible of all, it is hard not to salute him as a prophet of Hiroshima. The same is true when Schmitt writes about the League of Nations' resolution to use "economic sanctions and severance of the food supply," n56 which he calls "imperialism based on pure economic power." n57 Schmitt is no warmonger--he calls the killing of human beings for any reason other than warding off an existential threat "sinister and crazy" n58 --nor is he indifferent to human suffering.

But international humanitarian law and criminal law are not the same thing as wars to end all war or humanitarian military interventions, so Schmitt's important moral warning against ultimate military self-righteousness does not really apply. n59 Nor does "bracketing" war by humanitarian constraints on war-fighting presuppose a vanished order of European public law. The fact is that in nine years of conventional war, the United States has significantly bracketed war-fighting, even against enemies who do not recognize duties of reciprocity. n60 This may frustrate current lawfare critics who complain that American soldiers in Afghanistan are being forced to put down their guns. Bracketing warfare is a decision--Schmitt might call it an existential decision--that rests in part on values that transcend the friend-enemy distinction. Liberal values are not alien extrusions into politics or evasions of politics; they are part of politics, and, as Stephen Holmes argued against Schmitt, liberalism has proven remarkably strong, not weak. n61 We could choose to abandon liberal humanitarianism, and that would be a political decision. It would simply be a bad one.

## politics

PC fails, and the plan isn’t necessary for GOP obstruction

The Economist, 1/30/14, Clowns to the left, jokers to the right, www.economist.com/blogs/democracyinamerica/2014/01/barack-obama

I find this argument unpersuasive. Ed Luce made the key point a year and a half ago: LBJ had liberal Republicans and conservative Democrats to work with, whose decision about whether to vote with or against the president on different bills could be influenced by a variety of political considerations. Those legislative cross-loyalties don't exist anymore. Neither do earmarks, the budget goodies targeted to individual districts that were once a widespread currency of congressional dealmaking (something we lamented here). The parties today are ideologically sorted, and there is almost nothing Mr Obama can do to convince or compel Republicans to vote with him. Republicans are able to halt the president's agenda in its tracks, and they have every reason to do so. There simply isn't any reason to believe that more aggressive legislative arm-twisting would have generated more success for Mr Obama; it seems entirely possible that if he had aggressively tried to dictate the terms of health-care reform legislation rather than allowing various senators to rewrite (and weaken) the bill, he might have lost even that signature achievement. Last year, Mr Obama decided to throw his entire weight behind gun-control legislation, taking on just the sort of ambitious and improbable crusade Mr Ignatius had advised him to attempt. The result was that he lost, squandered political capital, and mired his party in the mud.

Unemployment benefits won’t pass

Ramsey Cox, 2/6/14, Senate rejects jobless benefits, thehill.com/blogs/floor-action/senate/197676-senate-rejects-unemployment-benefits

Senate Republicans on Thursday blocked Democrats’ third attempt to pass an extension of federal unemployment benefits. The Senate voted 58-40 Thursday on a proposal that would have continued unemployment insurance for three months, just short of the 60 votes needed to end debate. “I’m beginning to believe there is nothing that will get Republicans to yes,” Senate Majority Leader Harry Reid (D-Nev.) said. “It’s a ‘no’ vote because they don’t want to extend unemployment insurance.” “We’re one Republican vote away from restoring benefits to 1.7 million Americans,” Reid said. “There is one Republican vote standing in the way of a lifeline to these 1.7 million people.” Republican Sens. Dean Heller (Nev.), Susan Collins (Maine), Lisa Murkowski (Alaska) and Kelly Ayotte (N.H.) voted with Democrats to end debate. Sen. Rob Portman (R-Ohio), who was involved in the bipartisan negotiations, said he couldn't support the deal because he believed the pay-for "put taxpayers at risk." Democrats say they plan to use Republican refusal to pass a short-term extension of the benefits as a weapon in the midterm elections. Nearly 1.3 million people lost their long-term unemployment benefits at the end of December. The benefits, first put in place during the financial crisis, took effect for people when state-level assistance ran out. The White House slammed Senate Republcians and accused them of denying a "vital lifeline" to the unemployed. "We cannot allow one vote to stand in the way of supporting these Americans as they struggle to find work. Both sides of the aisle have worked together to prevent this kind of hardship in the past, and neglecting to do so now is unacceptable — especially given the high long-term unemployment rate," White House press secretary Jay Carney said in a statement. Democrats tried and failed to pass a three-month extension in January after Republicans demanded that the $6.5 billion cost be offset elsewhere in the budget. They then tried to pass an 11-month extension that was fully paid for by extending sequestration for an additional year, which would have generated roughly $25 billion for the government. Republicans balked at that plan and demanded an open amendment process. The latest proposal from Sens. Jack Reed (D-R.I.) and Dean Heller (R-Nev.) would have paid for the extension through “pension smoothing” — a budget maneuver used in the 2012 highway bill. “This is not a controversial pay-for,” Reed said ahead of the vote. “This is something we’ve embraced before. … It’s been used by colleagues on both sides of the aisle.” Pension smoothing reduces pension expenditures for companies in the short term by creating more taxable income. The measure would use this accounting procedure for four years to produce the $6.5 billion needed to cover the three-month benefit extension, and Reed said it would generate $1.2 billion that would go toward deficit reduction. But some Republicans decried the practice as a budget “gimmick” that risks greater liability in the long run. The Reed proposal also includes an amendment from Sen. Tom Coburn (R-Okla.) that would prevent millionaires from collecting unemployment benefits. But Senate Minority Leader Mitch McConnell (R-Ky.) said Republicans want the chance to make more changes to the bill. “We have a number ideas on this side of the aisle to promote economic growth,” McConnell said Tuesday. “So I ask the majority leader to modify his request to have an orderly, open amendment process.” Republicans have criticized Reid for rarely allowing amendments on legislation before filing cloture. They say not having an open amendment process gives them no voice in the chamber, forcing them to “sit down and shut up.” Reid counters that an open amendment process would simply be a way for Republicans to obstruct legislation.

NSA fights now

Feaver 1/17/14

Peter, Foreign Policy, “Obama Finally Joins the Debate He Called For,” http://shadow.foreignpolicy.com/posts/2014/01/17/obama\_finally\_joins\_the\_debate\_he\_called\_for

Today President Barack Obama finally **joins the national debate he called for** a long time ago but then abandoned: the debate about how best to balance national security and civil liberty. As I outlined in NPR's scene-setter this morning, this debate is a **tricky** one for a president who wants to lead from behind. The public's view shifts markedly in response to perceptions of the threat, so a political leader who is only following the public mood will **crisscross himself repeatedly**. Changing one's mind and shifting the policy is not inherently a bad thing to do. There is no absolute and timeless right answer, because this is about trading off different risks. The risk profile itself shifts in response to our actions. When security is improving and the terrorist threat is receding, one set of trade-offs is appropriate. When security is worsening and the terrorist threat is worsening, another might be. It is likely, however, that the optimal answer is not the one advocated by the most fringe position. A National Security Agency (NSA) hobbled to the point that some on the far left (and, it must be conceded, the libertarian right) are demanding would be a mistake that the country would regret every bit as much as we would regret an NSA without any checks or balances or constraints. Getting this right will require **inspired and active political leadership.** **To date**, Obama has preferred to stay far removed from the debate swirling around the Snowden leaks. This president relishes opportunities to spend **political capital** on behalf of policies that disturb Republicans, but, as former Defense Secretary Robert Gates's memoir details, Obama **has** been very reluctant to expend **political capital** on behalf of national security policies that disturb his base. Today Obama is finally engaging. It will be interesting to see how he threads the political needle and, just as importantly, how much political capital he is willing to spend in the months ahead to defend his policies.

Ongoing controversial push for executive trade authority now, triggers Dem fights

Amie Parnes, The Hill, 1/21/14, Obama: Give me fast track trade, thehill.com/homenews/administration/195858-white-house-works-to-convince-dems-to-give-obama-fast-track-on-trade

The White House is making a major push to convince Congress to give the president trade promotion authority (TPA), which would make it easier for President Obama to negotiate pacts with other countries.

A flurry of meetings has taken place in recent days since legislation was introduced to give the president the authority, with U.S. Trade Representative Mike Froman meeting with approximately 70 lawmakers on both sides of the aisle in the House and Senate.

White House chief of staff Denis McDonough has also been placing calls and meeting with top Democratic lawmakers in recent days to discuss trade and other issues.

Republicans have noticed a change in the administration’s interest in the issue, which is expected to be a part of Obama’s State of the Union address in one week.

While there was “a lack of engagement,” as one senior Republican aide put it, there is now a new energy from the White House since the bill dropped.

The effort to get Congress to grant Obama trade promotion authority comes as the White House seeks to complete trade deals with the European Union, and a group of Asian and Latin American countries as part of the Trans-Pacific Partnership, or TPP.

The authority would put time limits on congressional consideration of those deals and prevent the deals from being amended by Congress. That would give the administration more leverage with trading partners in its negotiations.

The trade push dovetails with the administration’s efforts to raise the issue of income inequality ahead of the 2014 midterm elections. The White House is pressing Republicans to raise the minimum wage and extend federal unemployment benefits.

The difference is, on the minimum wage hike and unemployment issue, Obama has willing partners in congressional Democrats and unions, who are more skeptical of free trade. Republicans are more the willing partner on backing trade promotion authority.

Legislation introduced last week to give Obama trade promotion authority was sponsored by House Ways and Means Committee Chairman Dave Camp (R-Mich.) and Senate Finance Committee Chairman Max Baucus (D-Mont.), as well as Sen. Orrin Hatch (R-Utah), the ranking member on Finance.

No House Democrats are co-sponsoring the bill, however, and Rep. Sandy Levin (D-Mich.), the Ways and Means Committee ranking member, and Rep. Charles Rangel (D-N.Y.), the panel’s former chairman, have both criticized it. They said the legislation doesn’t give enough leverage and power to Congress during trade negotiations.

Getting TPA passed would be a major victory for the administration, and one that would please business groups, but the White House will first have to convince Democrats to go along with it.

One senior administration official said the White House has been in dialogue with lawmakers on both sides of the aisle “with a real focus on Democrats” to explain TPA and take into account their concerns.

“Any trade matter presents challenges,” the senior administration official said, adding that White House officials are “devoted” to working with members on the issue.

The Democratic opposition makes it highly unlikely the trade promotion authority bill, in its current form at least, will go anywhere.

One big problem is that it was negotiated by Baucus, who is about to leave the Senate to become ambassador to China.

Baucus will be replaced by Sen. Ron Wyden (Ore.), who is said to disagree with the approach taken by his predecessor. Democratic aides predict the legislation, which Majority Leader Harry Reid (D-Nev.) called “controversial” last week, would have to be completely redone to gain traction among lawmakers in their party.

Some Democrats might see a disconnect between the White House’s push for trade and it’s separate push on income inequality, which has been embraced by the party.

But **that doesn’t mean the White House won’t** ramp up their focus **on trade in the coming weeks** and months.

Senior congressional aides expect trade to be a part of Obama’s upcoming State of the Union address, since the White House has made clear that the trade bill is a priority and the TPP trade pact is a core part of the administration’s overall jobs agenda, in terms of increasing exports and opening markets.

“**This is a priority of the president's**,” White House press secretary Jay Carney told reporters last week. “It's part of a broad approach to expanding exports and, you know, creating more opportunities for our businesses to grow. And we're going to continue to push for it.”

Obama losing on executive authority now

Ginger Gibson, Politico, 1/29/14, Republicans bash Obama for overstepping bounds, dyn.politico.com/printstory.cfm?uuid=B6D21B66-98C7-4059-B77D-8CFB4009563F

In his State of the Union address Tuesday night, President Barack Obama said if Congress won’t help him get things done, he’ll do it on his own — and congressional Republicans aren’t pleased. Many in the GOP said they don’t intend to sit quietly if Obama starts signing executive orders. Sen. Marco Rubio (R-Fla.) had sharp criticism for the president’s expanded authority. “I think it’s unfortunate, I think it’s divisive and quite frankly, borderline unconstitutional on many of those issues,” Rubio said. “I understand the [legislative] process takes long and can be frustrating, but I think it truly undermines the republic.” Rep. Tim Huelskamp (R-Kan.) said the president requested more controversial pieces of legislation — like immigration reform — than he did when Democrats controlled both chambers of Congress. “Suddenly he wants things that Republicans won’t give him that he didn’t ask Democrats to do — it seems like a lot of theatrics,” Huelskamp said. Huelskamp said he joked with fellow members that he’s going to file legislation that doesn’t require a presidential signature. The Kansas conservative said there are ways Republicans could push back at Obama’s executive orders but that he doesn’t think the GOP leadership is willing to wage the fight. “There are things we can do — I’m just afraid leadership is not willing to challenge them,” he said. Sen. Lindsey Graham (R-S.C.) argued that Obama employing executive powers could harm the Democrats as a whole. “I think he’s going to create a narrative for himself that’s going to hurt Democrats by acting unilaterally,” Graham said. “I think he’s going to create an impression among the American people that he’s abusing the power of his office and that will hurt Democrats.” Rep. Tom Cole (R-Okla.) took a soft approach to criticizing the president for overstepping his bounds on executive orders. “We’ll wait and see what he does,” Cole said. “The president has certain executive powers, but if he wants to achieve anything, an executive order is not a very good way to do it. Usually legislative achievement is what is enduring achievement. Executive orders are like writing on the beach, it may last a while but when the tide comes in or goes out, it disappears. So I think it’s a poor way to govern.” Sen. Tim Scott (R-S.C.) said acting without congressional authority is problematic. “We continue to erode the whole notion of the rule of law,” Scott said. “To the extent that he continues to move unilaterally without the consent of Congress, I think it doesn’t sit well with a message of unity.”

No econ impact

Jervis 11, Robert Professor in the Department of Political Science and School of International and Public Affairs at Columbia University, December 2011, “Force in Our Times,” Survival, Vol. 25, No. 4, p. 403-425

Even if war is still seen as evil, the security community could be dissolved if severe conflicts of interest were to arise. Could the more peaceful world generate new interests that would bring the members of the community into sharp disputes? 45 A zero-sum sense of status would be one example, perhaps linked to a steep rise in nationalism. More likely would be a worsening of the current economic difficulties, which could itself produce greater nationalism, undermine democracy and bring back old-fashioned beggar-my-neighbor economic policies. While these dangers are real, it is hard to believe that the conflicts could be great enough to lead the members of the community to contemplate fighting each other. It is not so much that economic interdependence has proceeded to the point where it could not be reversed – states that were more internally interdependent than anything seen internationally have fought bloody civil wars. Rather it is that even if the more extreme versions of free trade and economic liberalism become discredited, it is hard to see how without building on a preexisting high level of political conflict leaders and mass opinion would come to believe that their countries could prosper

 by impoverishing or even attacking others. Is it possible that problems will not only become severe, but that people will entertain the thought that they have to be solved by war? While a pessimist could note that this argument does not appear as outlandish as it did before the financial crisis, an optimist could reply (correctly, in my view) that the very fact that we have seen such a sharp economic down-turn without anyone suggesting that force of arms is the solution shows that even if bad times bring about greater economic conflict, it will not make war thinkable.