## 1AC

### 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 agression 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.

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.

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.

### 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.

Goes nuclear

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.

**Causes US-Russia miscalc—extinction**

Barrett et al. 13—PhD in Engineering and Public Policy from Carnegie Mellon University, Fellow in the RAND Stanton Nuclear Security Fellows Program, and Director of Research at Global Catastrophic Risk Institute—AND Seth Baum, PhD in Geography from Pennsylvania State University, Research Scientist at the Blue Marble Space Institute of Science, and Executive Director of Global Catastrophic Risk Institute—AND Kelly Hostetler, BS in Political Science from Columbia and Research Assistant at Global Catastrophic Risk Institute (Anthony, 24 June 2013, “Analyzing and Reducing the Risks of Inadvertent Nuclear War Between the United States and Russia,” Science & Global Security: The Technical Basis for Arms Control, Disarmament, and Nonproliferation Initiatives, Volume 21, Issue 2, Taylor & Francis)

War involving significant fractions of the U.S. and Russian nuclear arsenals, which are by far the largest of any nations, could have globally catastrophic effects such as severely reducing food production for years, 1 potentially leading to collapse of modern civilization worldwide, and even the extinction of humanity. 2 Nuclear war between the United States and Russia could occur by various routes, including accidental or unauthorized launch; deliberate first attack by one nation; and inadvertent attack. In an accidental or unauthorized launch or detonation, system safeguards or procedures to maintain control over nuclear weapons fail in such a way that a nuclear weapon or missile launches or explodes without direction from leaders. In a deliberate first attack, the attacking nation decides to attack based on accurate information about the state of affairs. In an inadvertent attack, the attacking nation mistakenly concludes that it is under attack and launches nuclear weapons in what it believes is a counterattack. 3 (Brinkmanship strategies incorporate elements of all of the above, in that they involve intentional manipulation of risks from otherwise accidental or inadvertent launches. 4 ) Over the years, nuclear strategy was aimed primarily at minimizing risks of intentional attack through development of deterrence capabilities, and numerous measures also were taken to reduce probabilities of accidents, unauthorized attack, and inadvertent war. For purposes of deterrence, both U.S. and Soviet/Russian forces have maintained significant capabilities to have some forces survive a first attack by the other side and to launch a subsequent counter-attack. However, concerns about the extreme disruptions that a first attack would cause in the other side's forces and command-and-control capabilities led to both sides’ development of capabilities to detect a first attack and launch a counter-attack before suffering damage from the first attack. 5 Many people believe that with the end of the Cold War and with improved relations between the United States and Russia, the risk of East-West nuclear war was significantly reduced. 6 However, it also has been argued that inadvertent nuclear war between the United States and Russia has continued to present a substantial risk. 7 While the United States and Russia are not actively threatening each other with war, they have remained ready to launch nuclear missiles in response to indications of attack. 8 False indicators of nuclear attack could be caused in several ways. First, a wide range of events have already been mistakenly interpreted as indicators of attack, including weather phenomena, a faulty computer chip, wild animal activity, and control-room training tapes loaded at the wrong time. 9 Second, terrorist groups or other actors might cause attacks on either the United States or Russia that resemble some kind of nuclear attack by the other nation by actions such as exploding a stolen or improvised nuclear bomb, 10 especially if such an event occurs during a crisis between the United States and Russia. 11 A variety of nuclear terrorism scenarios are possible. 12 Al Qaeda has sought to obtain or construct nuclear weapons and to use them against the United States. 13 Other methods could involve attempts to circumvent nuclear weapon launch control safeguards or exploit holes in their security. 14 It has long been argued that the probability of inadvertent nuclear war is significantly higher during U.S.–Russian crisis conditions, 15 with the Cuban Missile Crisis being a prime historical example. It is possible that U.S.–Russian relations will significantly deteriorate in the future, increasing nuclear tensions. There are a variety of ways for a third party to raise tensions between the United States and Russia, making one or both nations more likely to misinterpret events as attacks. 16

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.

High risk of escalating cyberattacks – newest, most qualified evidence

CrowdStrike Global Threat Report 1-22, cyber-security think tank / consulting group, “2013 Year in Review”, <http://www.lawfareblog.com/wp-content/uploads/2014/01/CrowdStrike_Global_Threat_Report_2013.pdf>

Looking to 2014, there is no indication that malicious actors’ operational tempo, particularly with respect to targeted intrusion operations, will decrease. Without total visibility into the actors conducting this activity, it is not possible to predict exactly where, when, and what they will target; however, based on patterns observed over the past year, it is possible to make educated guesses on what the threat landscape will look like in 2014.

EXPECTED TRENDS FOR 2014

CrowdStrike expects to see a rise in vulnerability research, as well as exploit development and usage in several key areas through 2014.

• Windows XP End of Life - Microsoft Windows XP will reach end-of-life on 8 April 2014, meaning that Microsoft will no longer release security patches for Windows XP after that date. Vulnerability researchers are likely sitting on backlogs of unreported Windows XP vulnerabilities with plans to publicly release or privately sell the vulnerabilities’ details after this date. As such, CrowdStrike expects to see a rise in XP-targeted exploits and a resulting rise in XP infections in Q2 and Q3 of 2014.

• Third-Party Targeting - Expect to see adversaries targeting third-party vendors in an attempt to compromise the ultimate target. Vendors often have less-robust security than their larger customers, and their networks offer an avenue through which those customers can be compromised. DEADEYE JACKAL used this tactic several times throughout 2013 when it compromised several third-party vendors offering DNS, social media, and content management services to major U.S. media organizations.

• gTLDs - We predict that 2014 will see a great deal of activity around ICANN’s new generic top-level domains (gTLDs). These gTLDs will be used by adversaries to support more effective phishing attacks. CrowdStrike also expects new vulnerabilities to be discovered and exploited in network-facing software with regard to handling gTLD hostnames.

• Increased Use of Encryption - Malware in general will be developed with a greater focus on encrypted network traffic. In 2014, we will see a rise in malware that uses SSL and custom encryption methods in order to communicate with remote servers for beaconing, receiving C2 commands, performing data exfiltration, etc.

• Sandbox-Aware Malware - As more security technologies increase their reliance on sandboxes for malware analysis, CrowdStrike foresees an increase in sandbox-aware malware. This functionality will cause the malware to appear benign to a sandbox, while performing its malicious functionality on a legitimate target system.

• Use of High-Level Languages - The past several years have seen a downward trend in the popularity of low-level languages such as C++, and an upward trend for high-level languages such as C# and Python. These trends are reflected in malware development, and as such we will see higher rates of high-level languages used to develop malware in 2014.

• More Black Market Exploit Activity - The past couple of years saw a surge in bug bounty programs from companies such as Microsoft, Yahoo!, and PayPal, and a corresponding decline in public disclosures of vulnerabilities. This trend will continue in 2014 with an increase in black market activity of newly discovered vulnerabilities and newly developed exploits. As the black market activity increases, so will the demand for custom-made malware.

• Activity in the Physical World - Security organizations and other targets of interest should look out for more adversary interactions in the physical world. The physical world activity will not be the kind resulting in physical harm, but rather it will influence and complement cyber operations.

TARGETING AROUND MAJOR EVENTS IN 2014

Targeted intrusion operators like to leverage major events in their operations. This is most often done through spear phishing emails that use a particular event as a theme in order to grab the interest of a target. There are a number of significant global events in 2014 that malicious actors could leverage in their operations:

• Winter Olympics/World Cup - The Winter Olympics and World Cup are both being held in 2014 in Russia and Brazil, respectively. In the past, spear phishing campaigns have been themed after significant sporting events such as these. They can be useful in general because they attract the interest of individuals in countries all over the world and across all levels of potential target organizations. Olympic- or World Cup-themed spear phishing campaigns could also be used specifically against sponsors of the events or organizations in the same sector as those sponsors. Sponsors for these events come from a wide variety of sectors, including: technology, finance, aerospace, energy, manufacturing, and food/ beverage.

• G20 Summit - The 2014 G20 Summit will be held in November in Brisbane, Australia, and will likely be leveraged in targeted attacks. The 2013 summit was leveraged in a targeted campaign discussed above, and the 2014 event will draw attention from the same targeted sectors. G20-themed spear phishing campaigns can be expected, and it is possible that SWC operations could be staged on the websites of G20-related organizations. Entities in the financial, government, and NGO/international relations sectors should remain alert for possible targeted activity in the weeks leading up to this event.

• Elections - There are elections occurring in numerous countries around the world in 2014, any of which could be used in malicious activity. Elections in any country could be used as an effective theme for targeting NGO or governmental entities focused on democratic or government processes. There are also specific regions that have numerous elections occurring that could be of particular interest to targeted intrusion operators in those regions. For example, Middle East-based actors may target entities interested in upcoming elections in Egypt, Iraq, Tunisia, and Turkey. Elections in Bangladesh, Thailand, and Indonesia may see related activity from Chinese operators, and those in India could be targeted by Pakistani and/or Indian actors.

• Dissident Targeting - Targeted intrusion operations against dissident communities is a constant in all regions. China-based operators are particularly interested in activities against Tibet and Uyghur issues, while Middle East operations often target political dissidents. Malicious actors will often use news of protests or violence related to these groups as themes in their attacks. Dissident-related activity affects those groups, but can also affect governmental or NGO entities interested in dissident issues.

These are just a few examples of events that have been leveraged in targeted intrusion operations in the past and are likely to be leveraged in the coming year. Organizations should also be aware of targeting around major holidays, as they also present opportunities to target individuals throughout target organizations. Furthermore, major events that occur throughout the year are often closely followed by malicious activity. Significant natural disasters, violence, or economic events could be used in targeted campaigns, as could major business events like mergers or IPOs.

CYBER SPILLOVER FROM REGIONAL CONFLICT

Real-world physical conflicts will increasingly spawn cyber threats as tensions from those conflicts spill over into cyber operations. The Syrian conflict is a perfect example; the conflict began in March 2011, inflicting great deal of kinetic damage. In May of that same year, the Syrian Electronic Army formed and began conducting cyber operations in support of the Assad regime. As the topic of chemical weapon usage took center stage during the summer of 2013, a sustained campaign of related malicious cyber operations carried out by DEADEYE JACKAL sought to identify anti-regime activists, as well as control the messaging of the conflict.5 Consequently, these operations targeted both high-profile media organizations and U.S. government entities, as well as third-party communications platforms. The common technique across the various operations was credential collection activity accomplished using spear phishing attacks, and attacks on third-party service providers. These targeted organizations had no obvious connection to the physical conflict in Syria, but they were affected by it nonetheless. Similarly, escalated cyber espionage activity was observed related to the uprisings in Tunisia and in the tensions between China and Japan over the Diaoyu/Senkaku Islands. As we look at what 2014 has in store**, there are a number of areas where ongoing conflict is likely to continue, and some where it may intensify**

**.** The Arab Spring continues to impact governmental stability in parts of the Middle East/North Africa region; this is an area to watch for proliferation of cyber operations. Within that geographical area, Syria remains an area of concern, but more alarming is the influx of Syrian refugees into surrounding countries, particularly Jordan, which could potentially drag those countries into the conflict. North African countries (such as Egypt, Libya, and Tunisia) that have gone through political turmoil over the past year will likely continue to have unrest and political turmoil that could escalate in 2014. In response to a rapidly growing refugee situation and continued political dissent, these countries may increase cyber operations to monitor dissidents and even each other. CrowdStrike Intelligence has been observing a continued escalation in malicious software and exploitation targeting emanating from the Middle East. As these actors continue to explore the cyber domain, it is likely that their sophistication and capabilities will continue to evolve. South Asia is also an area of concern. The U.S. plans to withdraw most of its forces from Afghanistan in 2014, and while there is little to no observed activity from adversaries in that country, the drawdown could result in heightened tensions in neighboring Pakistan and India. Additionally, the unstable situation left in Afghanistan following U.S. withdrawal threatens to diminish or destroy the Karzai government. In the wake of a perceived defeat of the Karzai government or a reduction in capabilities, there is increased possibility that Al Qaeda or other groups may seek to leverage cyber capabilities to control messaging; track dissidents or uncooperative tribal factions; or monitor movement of democratic factions. Increased tensions in the region overall are likely to create the need for cyber espionage activity from cyber adversaries operating out of both India and Pakistan, particularly VICEROY TIGER, which carried out numerous operations throughout 2013. Finally, there are a number of contentious issues to watch in the Far East. The disagreement over the Diaoyu/Senkaku Islands was already mentioned, but other issues such as territorial rights in the South China Sea whereby China’s aggression towards the Philippines and Japan over fish-rich waters, as well as oil and gas-rich land resulted in the deployment of military assets in the region. Moreover, events such as China’s declaration of an air defense identification zone is creating further tension and are likely to provide even more motivation for activity from China-based actors. As a result, while Chinese intrusion operations against regional government entities have been previously observed and remain an issue of concern to diplomatic and military-associated organizations, further expansion of targeting may be observed. Expanded targeting may include potential new victims in elements of government not traditionally considered military forces, such as coast guard fleets, as well as commercial targets, such as firms in the aerospace and shipping sectors. Other countries may also seek to leverage cyber operations to collect intelligence from these areas; Taiwan, Korea, Japan, Singapore, and others will likely see cyber operations as low-cost options to collect intelligence at network speed from the infrastructure of perceived threat actors. The growing unpredictability of the Democratic People’s Republic of Korea (DPRK) remains of concern to neighboring countries like China, South Korea, and Japan, as well as the U.S. It is likely that the regime may instigate future aggression against regional neighbors to consolidate power, or in pursuit of international aid concessions. Such behaviors have been seen in prior crisis periods involving nuclear and missile systems as well as computer network attack. CrowdStrike Intelligence tracks one adversary with a nexus to North Korea, SILENT CHOLIMMA, and escalated tensions in 2014 could see more malicious cyber activity from that country. In previous years, tensions between the Republic of Korea (ROK) and the DPRK have been accented with computer network attacks ranging from Distributed Denial of Service (DDoS) to wiping of financial and media systems by automated weaponized code targeting critical infrastructure in the ROK. DPRK government-sponsored operators have been implicated in other prior cyber attacks. Kim Jong Un’s personal involvement in these cyber actions was purportedly key to ensuring his elevation during his father’s decisions regarding future leadership succession. As a result, the projection of cyber power may be of particular interest to the new North Korean leader as a means to exhibit strength on the international stage, as it is less provocative than projections of kinetic power, which could result in significant negative reaction from other countries. The North Korean military is also entering its winter training cycle, which could also result in increased activity from units focused on cyber operations. Any organization is a potential target in these cases depending on whether the adversary perceives it to be connected to the regional conflict, or even just presenting itself as a target of opportunity. Observations in 2013 suggest that media organizations may be particularly attractive targets because of reporting that those on either side of the conflict may find objectionable, or due to the high visibility that media organizations have in presenting and shaping public opinion. It is important to keep in mind: **organizations in all geographic regions and across all sectors could be affected by cyber spillover**.

INCREASED MIDDLE EAST/NORTH AFRICA-BASED ACTIVITY

An increasing level of activity from actors based in the Middle East and North Africa can be expected. Adversaries from this region have been known to use openly available malicious tools such as Poison Ivy and Xtreme RAT, but the past year saw adoption of a number of other openly available malware variants such as njRAT, Njw0rm, and Fallaga RAT. The proliferation of these newer proprietary tools during 2013 suggests that a growing number of individuals and organizations in the region are attempting to obtain the targeted intrusion capabilities that these tools afford. Such tools would allow this growing number of adversaries to compromise sensitive data from targets of interest across numerous spectrums and disciplines. As mentioned above, this region is home to several areas where there is ongoing physical conflict or political unrest. This conflict will fuel motivation of adversaries in the region to conduct malicious cyber attacks on entities they feel are deserving. Motivation for such attacks may range from retribution for police or military action, counter-intelligence programs, message control, or even anti-regime hacktavism; previous events in this theatre demonstrate that both sides of the conflict understand the importance and power of cyber capabilities. Activity from actors in the Middle East/North Africa will also not likely be confined to those serving a political or ideological end. Apart from malicious activity stemming from political or ideological motivations, actors from this region are showing a general desire to conduct targeted intrusion activities aimed at compromising information of strategic value. Much of the observed activity from 2013 targeted organizations in the energy, government, media, and technology sectors, but organizations in all sectors are at risk from targeted activity carried out by Middle East/North Africa-based adversaries.

PRIVATE ENTITIES ACTING ON BEHALF OF NATION-STATES

CrowdStrike Intelligence is seeing more indications of nation-states using actors for hire, which is a trend to follow in 2014. VICEROY TIGER is an adversary that appears to fall into this category, and that was very active over the past year. Public reporting suggests that this actor is actually an India-based security firm known as Appin Security Group that may have been contracted by the Indian government. Investigation into VICEROY TIGER’s operations shows that it targeted numerous entities across the globe that would be of strategic interest to India’s government, including heavy targeting of Pakistani military and political entities. Changes in TTPs during 2013 suggest that DEADEYE JACKAL could be another actor that is acting in concert with the Syrian regime. The group moved from an opportunistic attack model to one more targeted-objective based, in which their main intrusion method became targeted credential harvesting via spear phishing attacks. The targeting of Western media and government entities concerned with the Syrian conflict suggests more than casual affiliation to the Syrian regime. Additionally, the scale and sustained nature of the targeted operations indicates this adversary may have been granted access to resources later in the conflict that were not previously available. A recent investigation into the activity of a Russian-speaking adversary identified an actor whose services may have been acquired for specific operations on behalf of a nation-state customer. This adversary has been involved in targeted activity for nearly a decade, but malware analysis showed significant similarities to known cybercrime activity utilizing Sheldor and Zeus malware. The combination of criminal and targeted activity suggests an adversary that conducts malicious activity on its own accord, possibly as part of a continuing criminal enterprise, and also at the direction of a government entity. The motivations of private entities that conduct operations in support of a nation-state may vary. In certain circumstances, it may be that a government will turn a blind eye to criminal activity if an actor will use its skills to further the state’s interests. In others, it may be that the private entity is a company that sells its expertise and resources to its government, or to the governments of other countries. Another motivation could be more nationalistic, possibly like the case of DEADEYE JACKAL, where a private group lends its services to the state out of a feeling of patriotism. Whatever the motivation may be, having private groups carry out malicious activity has advantages for nation-states. One advantage is that private entities often have expertise and/or resources that the state does not have. Skilled personnel are often drawn to the private sector for financial or other reasons, and contracting out work is a way for the state to leverage that expertise. Another advantage for the state is deniability. Even if malicious activity were able to be linked back to the private entity, the state can easily deny involvement and say that the private party was acting on its own. Conversely, there are some challenges to outsourcing this activity to third parties. Control over the infrastructure preventing reuse for other efforts is difficult to assert, and as can be seen in the diverse targets of VICEROY TIGER, it is possible that the same infrastructure supporting nationalistic objectives may be used for other purposes. Working through a third party introduces additional risk: there is less control over the individuals connected with the activity. It has long been suggested that some of these operators “moonlight” conducting hacking for hire – this is amplified when those individuals are not beholden to a specific state apparatus and are motivated not by patriotism alone. CRIMINAL ACTIVITY BECOMES MORE TARGETED

In the latter part of 2013, several major retailers were compromised in high-profile attacks. These attacks appear to have taken a page from the targeted attacker playbook. In these attacks, the adversary moved laterally across the enterprise and leveraged specialized tools for scraping the process space memory on Point of Sales (POS) devices. The POS devices are where the actual credit and debit cards of customers are swiped. As this swipe occurs, the magnetic track on the card s read into memory and encoded to be transmitted to the payment processing systems. The adversaries behind these attacks understood that the POS devices were effective collection points for the track data, and they specifically targeted these devices in order to collect a substantial amount of credit card account information. The fallout from these attacks has been well publicized, and as a result it is likely that other criminal adversaries will develop tactics to leverage lateral movement and memory scraping techniques in the immediate future. Hardware/Firmware Attacks In 2013, CrowdStrike observed an uptick in conference talks and other publications on offensive and defensive hardware research. Hardware attacks historically have had a higher barrier for entry in that tools to support hardware instrumentation and testing have typically been prohibitively expensive. In recent years, various open platforms, such as affordable software-defined radio platforms like the Ettus Research Universal Software Radio Peripheral (USRP) and other projects, have lowered the cost for entry to within reach of unfunded researchers. Much of the research in the realm of offensive and defensive firmware-based attacks is centered around: • Gaining advanced and stealthy persistence using firmware modifications. This previously boutique-shop product is turning into a mainstream consideration with more attention and better widespread documentation. • Exploitation of firmware vulnerabilities for local privilege escalation and remote exploitation. Much firmware is rife with bugs, and researchers start to publicly demonstrate these vulnerabilities. Proliferation even into the commodity malware sector is possible. At the Observe, Hack, Make (OHM13) event, a researcher presented a talk on gaining persistence through hard-disk-drive firmware modifications. In this talk, the researcher demonstrated that it is possible to ultimately reflash the firmware from the host operating system and modify it to load attacker-controlled code during boot without that code being visible on the disk later on. Another researcher presented comparable research at 30C3 targeting microSD flash storage cards. At BlackHat USA 2013, a researcher presented on persistently hiding payloads in NAND flash based on flash controller properties and logic bugs. Additionally, he provided insight on the potential of software-induced NAND hardware failures. What is more, countless vulnerabilities in Small Office/Home Office (SOHO) router equipment have been published in 2013 as a result of researchers applying simple firmware analysis techniques on a more widespread basis. This is largely the result of leveraging static keys, or low-quality code resulting in implementation failures. CrowdStrike Intelligence expects this trend to continue for 2014, with proliferation of firmware-based attacks becoming available to actors with less-sophisticated tradecraft.

Conclusion

In retrospect, 2013 was a very busy year for the adversaries and network defenders who are responsible for fending off the multitude of attacks. Advanced adversaries targeted a number of critical sectors for espionage; at least one actor, SILENT CHOLIMMA, actively engaged in a destructive attack, and criminal and activist groups were able to impact billions of dollars of commerce.

As we look toward 2014, it certainly promises to be another exciting year in information security. The fight is being driven lower down the stack in terms of hardware security threats, and up the stack through high-level programming language malware at the same time. The threat actors are proliferating, and the ability to conduct these attacks is being made easier through regionalized malware packages and builder tools.

## 2AC

### 2ac circumvention

Self-restraint now disproves the link

Healey 11 (Jason Healey is the director of the Cyber Statecraft Initiative at the Atlantic Council of the United States, “Bringing a Gun to a Knife Fight: US Declaratory Policy and Striking Back in Cyber Conflict” September 2011, Atlantic Council; Cyber Statecraft Initiative)

Although not mentioned in the Strategy, the United States military appears to already have some such limitations at the operational level. For example, General Keith Alexander, the commander of US Cyber Command, testified before Congress that the “law of war principles of military necessity, proportionality, and distinction will apply” to cyber operations. This implies that **some** kinds of **targets may not be struck**—that the US military will not directly target hospitals or civilians not involved in an adversary’s war effort. Also, it means **the US would** forego **some** kinds of **cyber** military **capabilities**, such as those that cannot be adequately controlled after release and would therefore be more likely to cascade uncontrollably and disproportionately.

More specifically, General Alexander testified that it “is difficult for me to conceive of an instance where it would be appropriate to attack a bank or a financial institution, unless perhaps it was being used solely to support enemy military operations.” This view is likely driven by both legal considerations (such as not being proportional, because of the overall negative effect on civilians) and domestic pressure (since the US will suffer more than other nations if finance is considered a legitimate target).

### 2ac t – prohibit

We meet restrictions --- 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 rana

No impact to economic decline – prefer new data

Daniel Drezner 14, IR prof at Tufts, The System Worked: Global Economic Governance during the Great Recession, World Politics, Volume 66. Number 1, January 2014, pp. 123-164

The final significant outcome addresses a dog that hasn't barked: the effect of the Great Recession on cross-border conflict and violence. During the initial stages of the crisis, multiple analysts asserted that the financial crisis would lead states to increase their use of force as a tool for staying in power.42 They voiced genuine concern that the global economic downturn would lead to an increase in conflict—whether through greater internal repression, diversionary wars, arms races, or a ratcheting up of great power conflict. Violence in the Middle East, border disputes in the South China Sea, and even the disruptions of the Occupy movement fueled impressions of a surge in global public disorder. The aggregate data suggest otherwise, however. The Institute for Economics and Peace has concluded that "the average level of peacefulness in 2012 is approximately the same as it was in 2007."43 Interstate violence in particular has declined since the start of the financial crisis, as have military expenditures in most sampled countries. Other studies confirm that the Great Recession has not triggered any increase in violent conflict, as Lotta Themner and Peter Wallensteen conclude: "[T]he pattern is one of relative stability when we consider the trend for the past five years."44 The secular decline in violence that started with the end of the Cold War has not been reversed. Rogers Brubaker observes that "the crisis has not to date generated the surge in protectionist nationalism or ethnic exclusion that might have been expected."43

Prioritization claims are counter-productive and illogical – you should evaluate the veracity of the 1ac’s claims about the world while embracing a plurality of (methods / ontologies / theories)

Andrew Bennett 13, government prof at Georgetown, The mother of all isms: Causal mechanisms and structured pluralism in International Relations theory, European Journal of International Relations 2013 19:459

The political science subfield of International Relations (IR) continues to undergo debates on whether and in what sense it is a 'science,1 how it should organize its inquiry into international politics, and how it should build and justify its theories. On one level, an 'inter-paradigm' debate, while less prominent than during the 1990s, has continued to limp along among researchers who identify their work as fitting within the research agenda of a grand school of thought, or 'ism,' and the scholar most closely associated with it, including neorealism (Waltz, 1979), neoliberalism (Keohane, 1984), constructivism (Wendt, 1992), or occasionally Marxism (Wallerstein, 1974) or feminism (Tickner, 1992). Scholars participating in this debate have often acted as if their preferred 4 ism' and its competitors were either "paradigms" (following Kuhn, 1962) or "research programs' (as defined by Lakatos, 19701. and some have explicitly framed their approach as paradigmatic or programmatic (Hopf, 1998).

A second level of the debate involves post-positivist critiques of IR as a "scientific' enterprise (Lapid, 1989). While the vague label "post-positivist, encompasses a diverse group of scholars, frequent post-positivist themes include arguments that observation is theory-laden (Kuhn, 1962), that knowledge claims are always part of mechanisms of power and that meaning is always social (Foucault, 1978), and that individual agents and social structures are mutually constitutive (Wendt, 1992). Taken together, these arguments indicate that the social sciences face even more daunting challenges than the physical sciences.

A third axis of contestation has been methodological, involving claims regarding the strengths and limits of statistical, formal, experimental, qualitative case study, narrative, and other methods. In the last two decades the argument that there is 'one logic of inference1 and that this logic is 'explicated and formalized clearly in discussions of quantitative research methods' (King et al., 1994: 3) has generated a useful debate that has clarified the similarities, differences, uses, and limits of alternative methods ( Brady and Collier, 2010; George and Bennett, 2005; Goertz and Mahoney, 2006).

These debates have each in their own way proved fruitful, increasing the theoretical, epistemological, and methodological diversity of the field (Jordan el al., 2009). The IR subfield has also achieved considerable progress in the last few decades in its theoretical and empirical understanding of important policy-relevant issues, including the inter-democratic peace, terrorism, peacekeeping, international trade, human rights, international law, international organizations, global environmental politics, economic sanctions, nuclear proliteration, military intervention, civil and ethnic conflicts, and many other topics.

Yet there is a widespread sense that this progress has arisen in spite of interparadigmatic debates rather than because of them. Several prominent scholars, including Rudra Sil and Peter Katzenstein, have argued that although research cast within the framework of paradigmatic debates has contributed useful concepts and findings, framing the IR field around inter-paradigmatic debates is ultimately distracting and even counterproductive (Sil and Katzenstein, 2010; see also David Lake, 2011, and in this special issue, and Patrick Thaddeus Jackson and Daniel Nexon, 2009, and in this special issue). These scholars agree that IR researchers have misapplied Kuhn's notion of paradigms in ways that imply that grand theories of tightly connected ideas — the isms — are the central focus of IR theorizing, and that such isms should compete until one wins general consensus. Sil and Katzenstein argue that the remedy for this is to draw on pragmatist philosophers and build upon an 'eclectic' mix of theories and methods to better understand the world (Sil and Katzenstein, 2010). In this view, no single grand theory can capture the complexities of political life, and the real explanatory weight is carried by more fine-grained theories about 'causal mechanisms."

In this article I argue that those urging a pragmatic turn in IR are correct in their diagnosis of the drawbacks of paradigms and their prescription tor using theories about causal mechanisms as the basis for explanatory progress in IR. Yet scholars are understandably reluctant to jettison the "isms' and the inter-paradigmatic debate not only because they fear losing the theoretical and empirical contributions made in the name of the isms, but because framing the field around the isms has proven a useful shorthand for classroom teaching and field-wide discourse. The 'eclectic' label that Sil and Katzenstein propose can easily be misinterpreted in this regard, as the Merriam-Webster online dictionary defines 'eclectic\* as 'selecting what appears to be best in various doctrines, methods, or styles,' as Sil and Katzenstein clearly intend, but it also includes as synonyms "indiscriminate" and 'ragtag.'1 By using the term 'eclecticism' and eschewing any analytic structure for situating and translating among different examples of IR research, Sil and Katzenstein miss an opportunity to enable a discourse that is structured as well as pluralistic, and that reaches beyond IR to the rest of the social sciences.

I maintain that in order to sustain the genuine contributions made under the guise of the inter-paradigmatic debate and at the same time get beyond it to focus on causal mechanisms rather than grand theoretical isms, four additional moves are necessary. First, given that mechanism-based approaches are generally embedded within a scientific realist philosophy of science, it is essential to clarify the philosophical and definitional issues associated with scientific realism, as well as the benefits — and costs — of making hypothesized causal mechanisms the locus of explanatory theories. As Christian Reus-Smit argues in this special issue, IR theory cannot sidestep metatheoretical debates. Second, it is important to take post-positivist critiques seriously and to articulate standards for theoretical progress, other than paradigmatic revolutions, that are defensible even if they are fallible. Third, achieving a shift toward mechanismic explanations requires outlining the contributions that diverse methods can make to the study of causal mechanisms. Finally, it is vital to demonstrate that a focus on mechanisms can serve two key functional roles that paradigms played for the IR subfield: first, providing a framework for cumulative theoretical progress; and, second, constituting a useful, vivid, and structured vocabulary for communicating findings to fellow scholars, students, political actors, and the public (see also Stefano Guzzini's article in this special issue). I argue that the term 'structured pluralism' best captures this last move, as it conveys the sense that IR scholars can borrow the best ideas from different theoretical traditions and social science disciplines in ways that allow both intelligible discourse and cumulative progress.

Alter briefly outlining the problems associated with organizing the IR field around the "isms/ this article addresses each of these four tasks in turn. First, it takes on the challenges of defining "causal mechanisms' and using them as the basis of theoretical explanations. Second, it acknowledges the relevance and importance of post-positivist critiques of causal explanation, yet it argues that scientific realism and some approaches to interpretivism are compatible, and that there are standards upon which they can agree forjudging explanatory progress. Third, it very briefly clarifies the complementary roles that alternative methods can play in elucidating theories about causal mechanisms. Finally, the article presents a taxonomy of theories about social mechanisms to provide a pluralistic but structured framework for cumulative theorizing about politics. This taxonomy provides a platform for developing typological theories — or what others in this special issue, following Robert Merton, have called middle-range theories — on the ways in which combinations of mechanisms interact to produce outcomes. Here, I join Lake in this special issue in urging that IR theorizing be centered around middle-range theories, and I take issue with Jackson and Nexon's suggestion herein that such theorizing privileges correlational evidence, and their assertion that statistical evidence is inherently associated with Humean notions of causation. I argue that my taxonomy of mechanisms offers a conceptual bridge to the paradigmatic isms in IR. adopting and organizing their theoretical insights while leaving behind their paradigmatic pretensions. The article concludes that, among its other virtues, this taxonomy can help reinvigorate dialogues between IR theory and the fields of comparative and American politics, economics, sociology, psychology, and history, stimulating cross-disciplinary discourses that have been inhibited by the scholasticism of IR's ingrown 'isms.'

**No impact to threat con**

Eric A. **Posner and** Adrian **Vermeule 3**, law profs at Chicago and Harvard, Accommodating Emergencies, September, <http://www.law.uchicago.edu/files/files/48.eap-av.emergency.pdf>

Against the view that panicked government officials overreact to an emergency, and unnecessarily curtail civil liberties, we suggest a more constructive theory of the role of fear. Before the emergency, government officials are complacent. They do not think clearly or vigorously about the potential threats faced by the nation. After the terrorist attack or military intervention, their complacency is replaced by fear. Fear stimulates them to action. Action may be based on good decisions or bad: fear might cause officials to exaggerate future threats, but it also might arouse them to threats that they would otherwise not perceive. **It is impossible to say in the abstract whether decisions and actions provoked by fear are likely to be better than decisions and actions made in a state of calm**. But our limited point is that there is no reason to think that the fear-inspired decisions are likely to be worse. For that reason, the existence of fear during emergencies does not support the antiaccommodation theory that the Constitution should be enforced as strictly during emergencies as during non-emergencies.

C. The Influence of Fear during Emergencies

Suppose now that the simple view of fear is correct, and that it is an unambiguously negative influence on government decisionmaking. Critics of accommodation argue that this negative influence of fear justifies skepticism about emergency policies and strict enforcement of the Constitution. However, this argument is implausible. It is doubtful that fear, so understood, has more influence on decisionmaking during emergencies than decisionmaking during non-emergencies.

The panic thesis, implicit in much scholarship though rarely discussed in detail, holds that citizens and officials respond to terrorism and war in the same way that an individual in the jungle responds to a tiger or snake. The national response to emergency, because it is a standard fear response, is characterized by the same circumvention of ordinary deliberative processes: thus, (i) the response is instinctive rather than reasoned, and thus subject to error; and (ii) the error will be biased in the direction of overreaction. While the flight reaction was a good evolutionary strategy on the savannah, in a complex modern society the flight response is not suitable and can only interfere with judgment. Its advantage—speed—has minimal value for social decisionmaking. No national emergency requires an immediate reaction—except by trained professionals who execute policies established earlier—but instead over days, months, or years people make complex judgments about the appropriate institutional response. And the asymmetrical nature of fear guarantees that people will, during a national emergency, overweight the threat and underweight other things that people value, such as civil liberties.

But if decisionmakers rarely act immediately, then the tiger story cannot bear the metaphoric weight that is placed on it. Indeed, the flight response has nothing to do with the political response to the bombing of Pearl Harbor or the attack on September 11. The people who were there—the citizens and soldiers beneath the bombs, the office workers in the World Trade Center—no doubt felt fear, and most of them probably responded in the classic way. They experienced the standard physiological effects, and (with the exception of trained soldiers and security officials) fled without stopping to think. It is also true that in the days and weeks after the attacks, many people felt fear, although not the sort that produces a irresistible urge to flee. **But this kind of fear is not the kind in which cognition shuts down**. (Some people did have more severe mental reactions and, for example, shut themselves in their houses, but these reactions were rare.) The fear is probably better described as a general anxiety or jumpiness, an anxiety that was probably shared by government officials as well as ordinary citizens.53

While, as we have noted, there is psychological research suggesting that normal cognition partly shuts down in response to an immediate threat, we are aware of no research suggesting that people who feel anxious about a non-immediate threat are incapable of thinking, or thinking properly, or systematically overweight the threat relative to other values. Indeed, it would be surprising to find research that clearly distinguished “anxious thinking” and “calm thinking,” given that anxiety is a pervasive aspect of life. People are anxious about their children; about their health; about their job prospects; about their vacation arrangements; about walking home at night. No one argues that people’s anxiety about their health causes them to take too many precautions—to get too much exercise, to diet too aggressively, to go to the doctor too frequently—and to undervalue other things like leisure. So it is hard to see why anxiety about more remote threats, from terrorists or unfriendly countries with nuclear weapons, should cause the public, or elected officials, to place more emphasis on security than is justified, and to sacrifice civil liberties.

Fear generated by immediate threats, then, causes instinctive responses that are not rational in the cognitive sense, not always desirable, and not a good basis for public policy, but it is not this kind of fear that leads to restrictions of civil liberties during wartime. The internment of Japanese Americans during World War II may have been due to racial animus, or to a mistaken assessment of the risks; it was not the direct result of panic; indeed there was a delay of weeks before the policy was seriously considered.54 Post-9/11 curtailments of civil liberties, aside from immediate detentions, came after a significant delay and much deliberation. The civil libertarians’ argument that fear produces bad policy trades on the ambiguity of the word “panic,” which refers both to real fear that undermines rationality, and to collectively harmful outcomes that are driven by rational decisions, such as a bank run, where it is rational for all depositors to withdraw funds if they believe that enough other depositors are withdrawing funds. Once we eliminate the false concern about fear, it becomes clear that the panic thesis is indistinguishable from the argument that during an emergency people are likely to make mistakes. But if the only concern is that during emergencies people make mistakes, there would be no reason for demanding that the constitution be enforced normally during emergencies. Political errors occur during emergencies and nonemergencies, but the stakes are higher during emergencies, and that is the conventional reason why constitutional constraints should be relaxed.

**Threat construction in terms of terror is good – censorship precludes prevention**

**Rychlak 10** (Ronald, Professor of Law and Associate Dean for Academic Affairs, University of Mississippi School of Law; adviser to the Holy See's delegation to the United Nations., <http://newsweek.washingtonpost.com/onfaith/panelists/ronald_rychlak/2010/07/the_language_of_counter-terrorism.html>)

**What we call terrorists may not matter very much, but a restriction on what we can call them is of enormous importance**. In order to get to the truth of any issue, people have to be free to talk about it without fear of repercussion. Unfortunately, one of the issues around which many problems revolve - religion - is also a topic that is particularly hard to discuss freely. In our day-to-day life, we may avoid the topic with only minimal inconvenience. **When it comes to global terrorism, restricting what we say about religion can lead to devastating results**. Next month I will start the new semester by teaching a course called "Terrorism and the Law." On the very first day, I will explain to the students that we will be talking about religion even though we are at a state law school. Islam, or at least the way some people interpret Islam, is an important issue when it comes to modern terrorism. I will, of course, explain that not all Muslims agree with the terrorist tactics - or even their long term aims - and not all terrorists are Muslim, but **we can't really study modern terrorism without developing an understanding of the motivations.** Unfortunately, religion is a significant motivation underlying much modern terrorism. Four or five years ago I traveled with a group to Israel. Instead of studying the holy sites, however, the focus of our trip was on counter-terrorism. Most members of my group were college educators who taught courses on terrorism. One of them had authored a major textbook. He told me that his publisher forbid him from any discussion of religion in the book. He said that was common. Publishers were afraid that books would not be used if they ventured into that area. He also said that most experts in the field lacked the knowledge to write about religion anyway. **By keeping religion out of these textbooks and the related courses we were knowingly providing an insufficient education to our next generation of counter-terror experts**. The author said that when the book came out in its next edition (which was going to be its third), he planned to demand inclusion of religious issues. He felt that by then the book would be well enough established that he would be able to make that demand. Still, the very idea that we had been intentionally excluding important issues when discussing this topic was shocking. Of course, a private entity might fear a violent reaction such as the riots that followed the publication of those Danish political cartoons. It is not, however, only private publishing interests that feel unable to talk about religion. The United States government also has a very hard time doing it. After all, as an inclusive society, we can't really argue that a Christian or Judeo-Christian outlook is better than even "hard-line" Islam, can we? The government's inability to talk about religion reached almost comical proportions in 2003, when the Department of State launched a "cultural magazine" for young men and women in Arab-speaking countries. A special coordinator for public diplomacy in the State Department explained: "This is a long-term way to build a relationship with people who will be the future leaders of the Arab world.... This is, in a very subtle way, a vehicle for American values." "Hi" magazine focused on things like entertainment, technology, and sports. Among the early articles that I remember was one about sand-surfing and another about protecting against over-exposure to the sun. There was, of course, no direct discussion of religion or religious values. The magazine floundered for a year or two, added an English version, went online, and finally died a quiet death. It was a phenomenal waste of time and money. I don't know how we are going to resolve issues that surround our very different world views, but I am quite certain that **restricting what we say - whether that means barring topics from textbooks or rejecting the use of terms like 'Islamic terrorist' and 'jihad' - is not a good start.** Let's first be honest in our language and our discussions. That will be hard, but it is the surest way to the truth. If we get to the truth, let's hope that we can also find peace.

### 2ac executive cp

Congress is key to norm clarity – only statute is perceived and enforced

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

The bottom line is that a body of recent political science, while confirming the President’s dominant position in setting policy in this area, also reveals that policymaking with respect to threats of force is significantly shaped by domestic politics and that Congress is institutionally positioned to play a powerful role in influencing those politics, even without exercising its formal legislative powers. Given the centrality of threatened force to U.S. foreign policy strategy and security crises, this suggests that the practical war powers situation is not so imbalanced toward the President as many assume.

Congressional involved is key to check the perception of unchecked authority

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.

### 2ac deterrence da

#### Zero risk of Korean conflict

Ashley **Rowland**, 12/3/20**10**. Stars and Stripes. “Despite threats, war not likely in Korea, experts say,” http://www.stripes.com/news/despite-threats-war-not-likely-in-korea-experts-say-1.127344?localLinksEnabled=false.

Despite increasingly belligerent threats to respond swiftly and strongly to military attacks, analysts say there is one thing both North Korea and South Korea want to avoid: an escalation into war. The latest promise to retaliate with violence came Friday, when South Korea’s defense minister-to-be said during a confirmation hearing that he supports airstrikes against North Korea in the case of future provocations from the communist country. “In case the enemy attacks our territory and people again, we will thoroughly retaliate to ensure that the enemy cannot provoke again,” Kim Kwan-jin said, according to The Associated Press. The hearing was a formality because South Korea’s National Assembly does not have the power to reject South Korean president Lee Myung-bak’s appointment. Kim’s comments came 10 days after North Korea bombarded South Korea’s Yeonpyeong island near the maritime border, killing two marines and two civilians — the first North Korean attack against civilians since the Korean War. South Korea responded by firing 80 rounds, less than half of the 170 fired by North Korea. It was the second deadly provocation from the North this year. In March, a North Korean torpedo sank the South Korean warship Cheonan, killing 46 sailors, although North Korea has denied involvement in the incident. The South launched a series of military exercises, some with U.S. participation, intended to show its military strength following the attack. John Delury, a professor at Yonsei University in Seoul, said South Korea is using “textbook posturing” to deter another attack by emphasizing that it is tough and firm. But it’s hard to predict how the South would respond to another attack. The country usually errs on the side of restraint, he said. “I think they’re trying to send a very clear signal to North Korea: Don’t push us again,” Delury said. “For all of the criticism of the initial South Korean response that it was too weak, in the end I think people don’t want another hot conflict. I think the strategy is to rattle the sabers a bit to prevent another incident.” Meanwhile, Yonhap News reported Friday that North Korea recently added multiple-launch rockets that are capable of hitting Seoul, located about 31 miles from the border. The report was based on comments from an unnamed South Korean military source who said the North now has 5,200 multiple-launch rockets. A spokesman for South Korea’s Joint Chiefs of Staff would not comment on the accuracy of the report because of the sensitivity of the information. Experts say it is a question of when — not if — North Korea will launch another attack. But those experts doubt the situation will escalate into full-scale war. “I think that it’s certainly possible, but I think that what North Korea wants, as well as South Korea, is to contain this,” said Bruce Bechtol, author of “Defiant Failed State: The North Korean Threat to International Security” and an associate professor of political science at Angelo State University in Texas. He said North Korea typically launches small, surprise attacks that can be contained — not ones that are likely to escalate. Delury said both Koreas want to avoid war, and North Korea’s leaders have a particular interest in avoiding conflict — they know the first people to be hit in a full-scale fight would be the elites.

No link --- AFF doesn’t create new red lines but develops transparent doctrine – that’s key to deterrence

Lewis 9 (James, PhD – UChicago, senior fellow and director of the Technology and Public Policy Program at CSIS, where he writes on technology, security, and the international economy, “The “Korean” Cyber Attacks and Their Implications for Cyber Conflict” October 2009, CSIS)

Deterrence

Weak attribution and unpredictable collateral damage make deterrence ineffective in cyberspace. Deterrence is a threat of retaliation, but it is hard to credibly threaten unknown parties and counterproductive to threaten or damage the wrong party. The United States is widely recognized to have pre-eminent offensive cyber capabilities, but it obtains little deterrent effect from this.

In the absence of attribution, the response options for the United States to the July A events were extremely limited. We could not retaliate against an unknown attacker. Deterrence is the threat of violent retaliation. This threat changes the opponent's calculus of the benefits and costs of an attack. But it is hard to convincingly threaten an unknown attacker, and weak attribution makes traditional deterrent concepts those based on the threat of reprisal for an attack (either countcrforce or countcrvalue) largely irrelevant in cyberspace.

The intcrconnectivity of cyberspace makes predicting collateral damage difficult. Uncertainty about the scope of collateral damage involves both unintended effects on the target and also possible damage to third party networks connected to or dependent upon the target network. Disabling or disrupting one network may affect third parties; for example, an attack on an opponent's network might accidently degrade a neutral nation's satellite or telecommunications sen ices. Anecdotal reports suggest that Israeli cyber attacks on Syrian air defense networks also damaged domestic Israeli networks.

Classic deterrence accepted (in theory) a measure of collateral damage. Strikes on invading Soviet forces in Germany would have harmed civilian populations in both allied and enemy countries. But these strikes were reserved for extreme situations when sovereignty had been clearly violated by military force. The extent of collateral damage for nuclear weapons was in some ways easier to predict than is the case in cyber conflict the blast and radiation effect of nuclear weapons is limited to an area around impact: in cyberspace, collateral damage may not be contiguous with the target. Uncertainty about collateral damage may hobble deterrence in cyberspace, by reducing the willingness of political leaders to incur the risk of a retaliatory response that goes awry, widening a conflict or creating unfavorable political consequences.

The threat of counterstrike was the basis of deterrence in the Cold War. However, the rationale for this kind of deterrence is not applicable to cyber conflict. In the Cold War. there was symmetry in vulnerabilities each side had cities and populations that the other could hold hostage. That symmetry no longer exists. The United States is far more dependent on digital networks than its opponents and this asymmetric vulnerability means that the United States would come out worse in any cyber exchange. There was clear attribution in the Cold War that allowed for both credible threats and for "signaling" and tacit understandings between opponents on "redlines" and thresholds. We lack that clarity in cyber conflict. The combination of asymmetric vulnerability. weak attribution and unpredictable collateral damage limit our ability to make a credible threat against an opponent in cyberspace.

Deterrence relics on more than the implied threat of the use of force in response to an attack. It requires statements about intentions and understanding among potential opponents that define and limit the environment for conflict. Deterrence in cyberspace is limited because we have not adequately assessed what combination of cyber capabilities, defensive measures, and international agreements will make the United States and its allies most secure. It would be useful to undertake a larger strategic calculation, preferably in a public dialogue, to determine the weighting and balance among offensive, defense and multilateral efforts in cyberspace that best reduces the risk of cvber attack.

### market da

No impact to EU

Bacevich, 10

Andrew, Bacevich, Boston University IR and History Professor, March/April 2010, Let Europe Be Europe,"http://www.foreignpolicy.com/articles/2010/02/22/let\_europe\_be\_europe?page=full, 2/28]

Europe, however, is another matter. By the dawn of this century, Europeans had long since lost their stomach for battle. The change was not simply political. It was profoundly cultural.

The cradle of Western civilization -- and incubator of ambitions that drenched the contemporary age in blood -- had become thoroughly debellicized. As a consequence, however willing they are to spend money updating military museums or maintaining war memorials, present-day Europeans have become altogether stingy when it comes to raising and equipping fighting armies.

**This pacification of Europe is** quite **likely to prove irreversible**. Yet even if reigniting an affinity for war among the people of, say, Germany and France were possible, why would any sane person even try? Why not allow Europeans to busy themselves with their never-ending European unification project? It keeps them out of mischief.

### 2ac politics

NSA thumps the disad or disproves the logic of the link.

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.

Zero risk of Iran strikes

Suzanne Maloney, Brookings Saban Center Senior Fellow, 1/13/14, Six Myths about Iran Sanctions, www.brookings.edu/blogs/iran-at-saban/posts/2014/01/7-iran-sanctions-nuclear-deal-myths?utm\_content=bufferb5045&utm\_medium=social&utm\_source=twitter.com&utm\_campaign=buffer#

Myth 6. Support for additional Iran sanctions is the equivalent of support for war.

No. With all due respect to the Obama administration officials who have been making this argument, **it is an overstatement** and, in many cases, patently untrue and unfair. It may be effective domestic politics, given the country's understandable weariness of Middle Eastern conflicts, but it is an ugly smear to accuse all those who are skeptical about the current diplomacy or who seek additional pressure on Iran of war-mongering.

More to the point, the outcome of new sanctions is almost certainly not war. Tehran has come to the negotiating table despite, and because of, severe economic pressure. Rouhani's determination to achieve a deal, the speed with which he has advanced this agenda, and the flimsy pushback (by the rough-and-tumble standards of Iranian internal politics) he has received from hard-liners suggests that there is a broad and deep consensus around ending the nuclear stand-off with the West. No one should doubt Foreign Minister Zarif's sincerity when he says sanctions will end the talks, but there is a reasonable chance that Tehran will continue to seek a diplomatic resolution under almost any circumstances — there simply is no better alternative for Iranian interests.

The same is true for Washington. Few in Congress are truly eager for another costly Middle Eastern conflict, and despite the tough talk from successive U.S. presidents on preventing a nuclear Iran, **there is nothing automatic about military action**. **Even if the current diplomacy collapses, Washington and the world will have an array of alternatives** for blunting Iran's nuclear advances, **including many that fall short of war**.

Obama is irrelevant—interim agreement success stopped sanction supporters

Patricia Zengerle, 1/13/14, Iran deal progress dampens push for new U.S. sanctions bill, www.reuters.com/article/2014/01/14/us-iran-nuclear-congress-idUSBREA0D02T20140114?feedType=RSS&feedName=topNews&utm\_source=dlvr.it&utm\_medium=twitter&dlvrit=992637

President Barack Obama is more likely to win his battle with the U.S. Congress to keep new sanctions on Iran at bay now that world powers and Tehran have made a new advance in talks to curb the Islamic Republic's nuclear program. Despite strong support for a bill in the Senate to slap new sanctions on the Islamic Republic, analysts, lawmakers and congressional aides said on Monday that **the agreement to begin implementing a nuclear deal on January 20 makes it harder** **for sanctions supporters to attract more backers.** Senator Richard Blumenthal, a Connecticut Democrat, was one of several of the 59 co-sponsors who said there is no clamor for a vote any time soon. "I want to talk to some of my colleagues. I'm encouraged and heartened by the apparent progress and certainly the last thing I want to do is impede that progress. But at the same time, sanctions are what has brought the Iranians to the table," he told reporters. Sixteen of Obama's fellow Democrats are among the co-sponsors of the measure requiring further cuts in Iran's oil exports if Tehran backs away from the interim agreement, despite Iran warning that it would back away from the negotiating table if any new sanctions measure passed. The current list of supporters is close to the 60 needed to pass most legislation in the 100-member Senate. But 67 votes would be required to overcome a veto, which Obama has threatened as he tries to reach a wider agreement with Iran to prevent it from developing an atomic bomb. "The prospects for a diplomatic solution could implode if Iran leaves the table or if Iran responds with their own provocative actions," said Colin Kahl, who served as a Middle East expert at the Pentagon until 2011 and now teaches security studies at Georgetown University. "Even if neither happens, Iran's moderate negotiators would likely harden their negotiating positions in the next phase to guard their right flank at home against inevitable charges of American 'bad faith,' making a final compromise harder to achieve," he said. The bill in the Senate would cut Iran's oil exports to almost zero two years after enactment, place penalties on other industries and reduce Obama's power to issue a waiver on Iran sanctions, if Iran were to break the interim deal. Supporters say it is necessary to pass a bill now rather than wait to see if Iran complies with the agreement in order to pressure Tehran to negotiate in good faith and not to keep developing nuclear weapons while talks continue. "If the Iranians have their way, they'll drag it out forever," Arizona Senator John McCain, a Republican co-sponsor of the measure, told reporters. Iranian officials say their nuclear program is peaceful. Democratic Senator Robert Menendez of New Jersey and Republican Mark Kirk of Illinois, the measure's lead sponsors, are trying to attract more supporters, hoping to pressure Senate Majority Leader Harry Reid to allow a vote on the legislation. Pro-Israel lobbying groups, convinced that Iran cannot be trusted, are also pushing lawmakers to sign on in the hope of increasing the pressure on Reid, a Nevada Democrat, to let the bill move ahead. But there is no guarantee that all the senators who co-sponsored the sanctions move would actually vote for any final bill, and even less that Democrats would override a veto by a president from their own party. Backers of the sanctions bill said they could force Reid's hand by putting a hold on nominations by the administration - such as dozens pending for State Department positions. But Senate leadership aides - including Republicans - acknowledge that the chamber's rules give Reid enough leeway to block any action. DEMOCRATS IN LINE Stopping - or delaying - new sanctions is also made easier because there is a strong core of lawmakers - including senior Democrats - who strongly oppose them. Ten powerful committee chairs signed a letter in December opposing the new sanctions, and none of those 10 has changed position. An aide to Menendez, who is chairman of the Senate Foreign Relations Committee, said there had been no indication by Monday on when the sanctions bill might come to the floor. Analysts said there had been real concern about a delay in implementing the interim agreement reached in Geneva between Iran and the so-called P5+1 powers in November. But **Sunday's announcement of the start date eases** those **fears**. "It shows that they are moving ahead, and what that means is that Iran's not delaying, which was a fear," said Michael Adler, an expert on Iran at the Wilson Center think tank in Washington.

Obama exerting capital on Iran ensures the sanction bill passes

Patrick Clawson, Washington Institute for Near East Research Director, 1/17/14, Why are congressional Democrats considering new Iran sanctions?, www.bbc.co.uk/news/world-us-canada-25749219

This week President Barack Obama met congressional Democrats, asking them to vote against sanctions on Iran and support continued negotiation.

But the administration's overtures may be too little, too late.

In a highly partisan atmosphere and with mid-term elections coming later this year, it would be very difficult for Democrats to go against a president of their own party, especially on foreign policy - an area where Congress mostly defers to the president.

That is particularly true when the president speaks repeatedly and publicly about the inappropriateness of the action Congress is considering.

But Mr **Obama's team is doing an impressive job of encouraging congressional Democrats to hand the president a stinging defeat**: namely, to pass legislation about the Iran nuclear negotiations which Mr Obama has described as sure to torpedo those talks.

'War'

The Obama team accuses those with whom they disagree of wanting war, posing the issue as: negotiate, or pass the legislation and leave war as the only option.

That enrages many in Congress who point out that the administration repeatedly opposed past congressional sanction initiatives and then, after those sanctions were enacted, went on to describe those sanctions as key elements in persuading Iran to come to the negotiating table.

Some in Congress suspect that the same dynamic seen over the last several years would apply to this new bill: the administration would strongly oppose it while it was under debate, and then once it was passed, would shift position 180 degrees to describe the new congressionally mandated pressure on Iran as central to persuading Iran to become more accommodating.

Bad cop?

In other words, most if not all of the congressional supporters of the proposed legislation see what they are doing as adding to US leverage in the negotiations.

Many of them think that they are playing the bad cop to the Obama administration's good cop in a way very similar to how Iranian Foreign Minister Javad Zarif and Iranian President Hassan Rouhani play the good cop to Supreme Leader Ayatollah Ali Khamenei's bad cop.

Each side can say to the other: "You have to help me do a deal I can sell to the hardliners who have much power in my country."

Perhaps this time, unlike the previous several times when Congress adopted sanctions legislation over the objections of the White House, the new measures would actually hurt the negotiations.

But Congress is not well-disposed to believe the administration's protestations that this is the case.

Personal relations

It does not help that **this comes against a background of congressional Democrats often being unhappy about** a perceived **lack of co-ordination and co-operation with the White House on a wide range of issues**, such as how to respond when the healthcare rollout had so many problems.

Mr Obama does not have the strong personal relations with Congress members that some past presidents had, nor has he established consistently effective means for working out deals with Congress.

Further **infuriating** some of the congressional sponsors has been the Obama team's strong public stance about how Iran is sure to react to the bill if passed. This seems like a self-fulfilling prophecy.

After all, if President Obama predicts Iran will strenuously object if the bill becomes law, that puts Zarif and Rouhani in a position where they must react strongly or else they will attract domestic criticism.

In fact, they must show that they are taking an even tougher stance than Mr Obama predicts they will.

This dynamic has been seen before in Obama Middle East policy.

Criticism

When President Obama said that Palestinian-Israeli peace talks could continue only if Israel froze settlement activities, that put Palestinian Authority Chairman Mahmoud Abbas into a position where he had to be firmer than Obama on the issue of settlements, even though many analysts have suggested that prior to Obama's statement he was willing to proceed even if settlement activity continued.

He had seemed to care at least as much or more about Israeli release of Palestinian prisoners.

Many in Congress have been highly critical in private of President Obama's stance on the settlement issue - which did not in fact bring an end to settlements and which long impeded the resumption of Palestinian-Israeli talks - and they see the president's stance on the Iran sanctions legislation as repeating the same mistake.

Tough sell

Compounding the problem, the Obama team has not engaged with Congress about how to craft a more acceptable bill, instead gambling on killing the bill.

Having put so much energy into the issue, congressional supporters of the legislation want to be able to show they accomplished something: they need to be able to vote in favour of a bill that they can claim preserves their core objectives.

If the Obama team insists that instead these members of Congress fall on their sword for the president, **that is a tough sell**.

Obama will use unilateral sanctions relief—solves

Adam Kredo, 1/21/14, White House Seeks to Bypass Congress on Iran Deal, freebeacon.com/white-house-seeks-to-bypass-congress-on-iran-deal/

The White House has been exploring ways to circumvent Congress and unilaterally lift sanctions on Iran once a final nuclear agreement is reached, according to sources with knowledge of White House conversations and congressional insiders familiar with its strategy.

The issue of sanctions relief has become one of the key sticking points in the Iran debate, with lawmakers pushing for increased economic penalties and the White House fighting to roll back regulations.

While many in Congress insist that only the legislative branch can legally repeal sanctions, senior White House officials have been examining strategies to skirt Congress, according to those familiar with internal conversations.

Sen. Mark Kirk (R., Ill.), who is leading the charge on new sanctions legislation, said that it is unacceptable for the White House to try to bypass Congress on such a critical global issue.

“The American people must get a say in any final nuclear agreement with Iran to ensure the mullahs never get the bomb,” Kirk told the Washington Free Beacon. “The administration cannot just ignore U.S. law and lift sanctions unilaterally.”

Congressional insiders say that the White House is worried Congress will exert oversight of the deal and demand tougher nuclear restrictions on Tehran in exchange for sanctions relief.

Top White House aides have been “talking about ways to do that [lift sanctions] without Congress and we have no idea yet what that means,” said one senior congressional aide who works on sanctions. “They’re looking for a way to lift them by fiat, overrule U.S. law, drive over the sanctions, and declare that they are lifted.”

Under the interim nuclear deal with Iran that began on Monday, Tehran will receive more than $4 billion in cash, according to the White House.

President Barack Obama could unilaterally unravel sanctions through several executive channels, according to former government officials and legal experts.

Executive orders grant the president significant leverage in the how sanctions are implemented, meaning that Obama could choose to stop enforcing many of the laws on the books, according to government insiders.

Those familiar with the ins and outs of sanctions enforcement say that the White House has long been lax with its enforcement of sanctions regulations already on the books.

“It’s no secret that the president, with executive power, can determine sanctions implementation, particularly with waivers and the decision not to sanction certain entities,” said Jonathan Schanzer, a former terrorism finance analyst at the Treasury Department, which is responsible for enforcing sanctions.

“The financial pressure has always been about closing loopholes and identifying new ones to close,” Schanzer added. “If you stop that process of constant gardening, you leave a backdoor open.”

Obama could also use executive waivers to “bypass restrictions imposed by the law,” according to a report by Patrick Clawson, director of research at the Washington Institute for Near East Policy (WINEP).

The president has a lot of leverage when it comes to sanctions and could effectively “turn a blind eye” to Iranian infractions.

“In the case of Iran, such an approach could allow Washington to reach a nuclear accord without Congress having to vote on rescinding, even temporarily or conditionally, certain sanctions,” Clawson wrote. “No matter how stiff and far-reaching sanctions may be as embodied in U.S. law, they would have less bite if the administration stopped enforcing them.”

One former senior government official said that President Obama’s legal team has likely been investigating the issue for quite some time.

“I’d be shocked if they weren’t putting the various sanctions laws under a microscope to see how they can waive them or work around them in order to deliver to Iran sanctions relief without having to worry about Congress standing in their way,” said Stephen Rademaker, who served as deputy legal adviser to former President George H.W. Bush’s National Security Council (NSC).

Executive branch lawyers are often tasked with finding ways to get around existing legislation, Rademaker said.

“I’m sure pretty early in the negotiating process they developed a roadmap” to ensure the president has the authority to promise Iran significant relief from sanctions, said Rademaker, who also served as chief council for the House Committee on International Relations. “I’m sure they’ve come up with an in depth analysis of what they can do relying exclusively on the president’s legal authority.”

The White House has been known to disregard portions of the sanctions laws that it disagrees with, according to Schanzer.

No chance of Iran negotiation success

Jessica Tuchman Mathews, Carnegie Endowment, 12/31/13, Washington’s World in 2014, carnegieendowment.org/2013/12/31/washington-s-world-in-2014/gxda

If this six-month nuclear accord can be turned into a permanent one that replaces the imminent threat of a nuclear-armed Iran with a transparent, internationally monitored civilian nuclear program, that achievement alone is how 2013 and 2014 will deserve to be remembered.

**That “if” looms large, however.** Unlike the key talks in the first phase, which were carried out in secret between the United States and Iran, the next phase of negotiations will feature six parties trying to agree on one side of the table—hardly a prescription for agile or effective bargaining. Across the table, Tehran will want more give on sanctions than the United States can offer. Moreover, negotiations will have to go beyond the fuel-cycle issues of uranium enrichment and plutonium production addressed in the first phase to the even more sensitive weapons technologies that have no civilian purpose. Deep-seated mistrust on both sides will frustrate every step.

Hard as it will be in the negotiating room, the greater impediment will be the self-fulfilling exchange of threat and counterthreat between those in Washington, Jerusalem, and Tehran who want this effort to fail. **The negotiators—especially Iran’s—will be working with one eye over their shoulders, watching for threats from domestic opponents**. Israel’s Prime Minister Benjamin **Netanyhau has made it plain that no negotiated settlement will satisfy him**, **and he has an overly attentive audience in the U.S. Congress**. The longer the negotiations take, the greater the pressure will be on Iran’s President Hassan Rouhani to show results that bring economic relief at home. At some point, the Revolutionary Guard and others in Iran’s powerful right wing who profit from the country’s economic isolation will try to retake the political initiative. The supreme leader has made his support for the negotiations absolutely clear—**for the time being.** But he is less of a leader and more of a follower than his grand title implies. For decades he has believed that what the United States really wants in Iran is regime change. The supreme leader’s support for the path of reintegration with the outside world that Rouhani campaigned on and overwhelmingly won on last summer is unlikely to survive prolonged stalemate or breakup of the talks.

### 2ac relations

U.S.-China relations solve every scenario for extinction

Cohen 9 (William S. Cohen is chairman and CEO of The Cohen Group, a strategic business consulting firm based in Washington, D.C. Secretary Cohen served as U.S. secretary of defense, Maurice R. Greenberg is chairman and CEO of C.V. Starr & Co., Inc. Mr. Greenberg retired four years ago as chairman and CEO of American International Group (AIG) after more than 40 years of leadership, creating the largest insurance company in history, “Smart Power in U.S.-China Relations,” pg online @ http://csis.org/files/media/csis/pubs/090309\_mcgiffert\_uschinasmartpower\_web.pdf //ef)

The evolution of Sino-U.S. relations over the next months, years, and decades has the potential to have a greater impact on global security and prosperity than any other bilateral or multilateral arrangement. In this sense, many analysts consider the US.-China diplomatic relationship to be the most influential in the world. Without question, strong and stable U.S. alliances provide the foundation for the protection and promotion of U.S. and global interests. Yet within that broad framework, the trajectory of U.S.-China relations will determine the success, or failure, of efforts to address the toughest global challenges: global financial stability, energy security and climate change, nonproliferation, and terrorism, among other pressing issues. Shepherding that trajectory in the most constructive direction possible must therefore be a priority for Washington and Beijing. Virtually no major global challenge can be met without U.S.-China cooperation. The uncertainty of that future trajectory and the "strategic mistrust" between leaders in Washington and Beijing necessarily concerns many experts and policymakers in both countries. Although some U.S. analysts see China as a strategic competitor—deliberately vying with the United States for energy resources, military superiority, and international political influence alike— analysis by the Center for Strategic and International Studies (CSIS) has generally found that China uses its soft power to pursue its own, largely economic, international agenda primarily to achieve its domestic objectives of economic growth and social stability.1 Although Beijing certainly has an eye on Washington, not all of its actions are undertaken as a counterpoint to the United States. In addition, CSIS research suggests that growing Chinese soft power in developing countries may have influenced recent U.S. decisions to engage more actively and reinvest in soft-power tools that have atrophied during the past decade. To the extent that there exists a competition between the United States and China, therefore, it may be mobilizing both countries to strengthen their ability to solve global problems. To be sure, U.S. and Chinese policy decisions toward the respective other power will be determined in large part by the choices that leaders make about their own nations interests at home and overseas, which in turn are shaped by their respective domestic contexts. Both parties must recognize—and accept—that the other will pursue a foreign policy approach that is in its own national interest.  Yet, in a globalized world, challenges are increasingly transnational, and so too must be their solutions. As demonstrated by the rapid spread of SARS from China in 2003, pandemic flu can be spread rapidly through air and via international travel. Dust particulates from Asia settle in Lake Tahoe. An economic downturn in one country can and does trigger an economic slowdown in another. These challenges can no longer be addressed by either **containment** or isolation. What constitutes the national interest today necessarily encompasses a broader and more complex set of considerations than it did in the past   As a general principle, the United States seeks to promote its national interest while it simultaneously pursues what the CSIS Commission on Smart Power called in its November 2007 report the "global good."3 This approach is not always practical or achievable, of course. But neither is it pure benevolence. Instead, a strategic pursuit of the global good accrues concrete benefits for the United States (and others) in the form of building confidence, legitimacy, and political influence in key countries and regions around the world in ways that enable the United States to better confront global and transnational challenges. In short, the global good comprises those things that all people and governments want but have traditionally not been able to attain in the absence of U.S. leadership. Despite historical, cultural, and political differences between the United States and China, Beijing's newfound ability, owing to its recent economic successes, to contribute to the global good is a matter for common ground between the two countries. Today there is increasing recognition that no major global challenge can be addressed effectively, much less resolved, without the active engagement of—and cooperation between—the United States and China. The United States and China—the worlds first- and third-largest economies—are inextricably linked, a fact made ever more evident in the midst of the current global financial crisis. Weak demand in both the United States and China, previously the twin engines of global growth, has contributed to the global economic downturn and threatens to ignite simmering trade tensions between the two countries. Nowhere is the interconnectedness of the United States and China more clear than in international finance. China has $2 trillion worth of largely U.S. dollar-denominated foreign exchange reserves and is the world's largest holder—by far—of U.S. government debt. Former treasury secretary Henry M. Paulson and others have suggested that the structural imbalances created by this dynamic fueled the current economic crisis. Yet. China will almost certainly be called on to purchase the lion's share of new U.S. debt instruments issued in connection with the U.S. stimulus and recovery package. Secretary of State Hillary Rodham Clinton's February 23.2009, reassurance to Beijing that U.S. markets remain safe and her call for continued Chinese investment in the U.S. bond market as a means to help both countries, and the world, emerge  from global recession underscored the shared interest—and central role—that both countries have in turning around the global economy quickly. Although China's considerable holdings of U.S. debt have been seen as a troubling problem, they are now being perceived as a necessary part of a global solution. Similarly, as the worlds two largest emitters of greenhouse gases, China and the United States share not only the collateral damage of energy-inefficient economic growth, but a primary responsibility to shape any ultimate global solutions to climate change. To date, cooperation has been elusive, owing as much to Washington's reluctance as to Beijing's intransigence. Painting China as the environmental bogeyman as an excuse for foot-dragging in policymaking is no longer an option; for its part, China, as the world's top polluter, must cease playing the developing-economy card. Yet energy security and climate change remain an area of genuine opportunity for joint achievement. Indeed, U.S.-China cooperation in this field is a sine qua non of any response to the energy and climate challenges. The sheer size of the Chinese economy means that collaboration with the United States could set the de facto global standards for etficiency and emissions in key economic sectors such as industry and transportation. Climate change also provides an area for cooperation in previously uncharted policy waters, as in emerging Arctic navigational and energy exploration opportunities. Washington and Beijing also share a deep and urgent interest in international peace and stability. The resumption of U.S.-China military contacts is a positive development. As two nuclear powers with worldwide economic and strategic interests, both countries want to minimize instability and enhance maritime security, as seen by parallel antipiracy missions in the waters otT Somalia. Joint efforts in support of United Nations peacekeeping, nonproliferation, and counterterrorism offer critical areas for bilateral and multilateral cooperation. Certainly, regional and global security institutions such as the Six-Party Talks concerning North Korea or the UN Security Council require the active engagement of both Washington and Beijing. Even more broadly, crisis management in geographic regions of mutual strategic interest like the Korean peninsula, Iran, or Burma require much more Sino-U.S. communication if the two countries are to avoid miscalculation and maximize opportunities to minimize human sutfering. Increasing the number of mid-level military-to-military exchanges would help in this regard. The United States and China could do more to cooperate on law enforcement to combat drug trafficking and organized crime in Western China. Afghanistan is competing with Burma as the main provider of narcotics to China; Washington could use its influence with the International Security Assistance Force in Kabul to develop a joint antinarcotics program. This could potentially build networks and joint capabilities that might be useful for U.S.-China cooperation on the issue of Pakistan. In addition, Washington should also encourage NATO-China cooperation along the Afghan border. Collaborating under the auspices of the Shanghai Cooperation Organization (SCO) might provide an additional framework for Beijing and Washington to address Central Asian security issues in a cooperative manner. 1he SCO, which includes Pakistan as an observer and will convene a multinational conference on Afghanistan in March 2009, has long made curbing narcoterrorism in Afghanistan a priority. In addition, the VS. Drug Enforcement Agency and the Chinese Anti-Narcotics Bureau should expand cooperation on interdiction and prosecution of heroin and meth traffickers. To be sure, there are a number of areas of serious divergence between Washington and Beijing. This should surprise no one. The United States has disagreements with even its allies. Two large powers with vastly dilferent histories, cultures, and political systems are bound to have challenges. History has shown, however, that the most effective way of addressing issues is for the U.S. and Chinese governments to engage in quiet diplomacy rather than public recrimination. In the U.S.-China context, there is often little to be gained—and much to be lost in terms of trust and respect—by a polarizing debate. Any differences, moreover, must not necessarily impede Sino-U.S. cooperation when both sides share strong mutual interests. I;. Scott Fitzgerald wrote that "the test of a first-rate intelligence is the ability to hold two opposed ideas in the mind at the same time, and still retain the ability to function."3 Effective policy toward China by the United States, and vice versa, will require this kind of dual-minded intelligence. Moreover, working together on areas of mutual and global interest will help promote strategic trust between China and the United States, facilitating possible cooperation in other areas. Even limited cooperation on specific areas will help construct additional mechanisms for bilateral communication on issues of irreconcilable disagreement. In fact, many of the toughest challenges in U.S.-China relations in recent years have been the result of unforeseen events, such as the accidental bombing of the Chinese embassy in Belgrade in May 1999 and the EP-3 reconnaissance plane collision in April 2001. Building trust and finding workable solutions to tough problems is the premise behind the Obama administrations foreign policy of smart power, as articulated by Secretary of State Clinton. Smart power is based on, as Secretary Clinton outlined in her confirmation hearing, the fundamental belief that 'We must use... the full range of tools at our disposal—diplomatic, economic, military, political and cultural—picking the right tool, or combination of tools, for each situation."' As the CS1S Commission on Smart Power noted in November 2007, "Smart Power is neither hard nor soft—it is the skillful combination of both\_\_\_\_It is an approach that underscores the necessity of a strong military, but also invests heavily in alliances, partnerships and institutions at all levels... .°5 As such, smart power necessarily mandates a major investment in a U.S.-China partnership on key issues. 'The concept enjoys broad support among the Chinese and American people and, by promoting the global good, it reaps concrete results around the world. There should be no expectation that Washington and Beijing will or should agree on all, or even most, questions. But the American and Chinese people should expect their leaders to come together on those vital issues that require their cooperation. U.S.-China partnership, though not inevitable, is indispensable.

## 1AR

### case

**Congress solves circumvention---raises political costs**

Ilya **Somin 11**, Professor of Law at George Mason University School of Law, June 21 2011, “Obama, the OLC, and the Libya Intervention,” http://www.volokh.com/2011/06/21/obama-the-olc-and-the-libya-intervention/

But I am more skeptical than Balkin that illegal presidential action can be constrained through better consultation with legal experts within the executive branch. The fact is that the president can almost always find respectable lawyers within his administration who will tell him that any policy he really wants to undertake is constitutional. Despite the opposition of the OLC, Obama got the view he wanted from the White House Counsel and from State Department Legal Adviser Harold Koh. Bush, of course, got it from within the OLC itself, in the form of John Yoo’s “torture memo.” This isn’t just because administration lawyers want to tell their political masters what they want to hear. It also arises from the understandable fact that administrations tend to appoint people who share the president’s ideological agenda and approach to constitutional interpretation. By all accounts, John Yoo was and is a true believer in nearly unlimited wartime executive power. He wasn’t simply trying to please Bush or Dick Cheney.¶ Better and more thorough consultation with executive branch lawyers can prevent the president from undertaking actions that virtually all legal experts believe to be unconstitutional. But on the many disputed questions where there is no such consensus, the president will usually be able find administration lawyers who will tell him what he wants to hear. To his credit, Ackerman is aware of this possibility, and recommends a creative institutional fix in his recent book: a new quasi-independent tribunal for assessing constitutional issues within the executive branch. I am somewhat skeptical that his approach will work, and it may well require a constitutional amendment to enact. I may elaborate these points in a future post, if time permits.¶ Regardless, for the foreseeable future, the main constraints on unconstitutional presidential activity must come from outside the executive branch – that is, from Congress, the courts, and public opinion. These constraints are highly imperfect. But they do impose genuine costs on presidents who cross the line. Ackerman cites the Watergate scandal, Iran-Contra and the “torture memo” as examples of the sorts of abuses of executive power that need to be restricted. True enough. But it’s worth remembering that Nixon was forced to resign over Watergate, Reagan paid a high political price for Iran-Contra, and the torture memo was a public relations disaster for Bush, whose administration eventually ended up withdrawing it (thanks in large part to the efforts of Jack Goldsmith). On the other side of the ledger, Bill Clinton paid little price for waging an illegal war in Kosovo, though he avoided it in part by keeping that conflict short and limited. It remains to be seen whether President Obama will suffer any political damage over Libya.

### 1ar – interp

Requiring Congressional approval is a statutory restriction on the President

Veravanich, JD King Hall, December 1996

(Paul, “The Propriety of President Bill Clinton's Establishment of the Grand Staircase Escalante National Monument,” *Environs*, Vol. 20, No. 1, pg. 5)

For example, in United States v. Cappaert the Supreme Court upheld the protection of Devil's Hole and its incorporation into the Death Valley National Monument on the grounds that not only did the Devil's Hole pool contain unique limestone formations, but it also contained pupfish, an endangered species.2 i The Grand Canyon National Monument 22 and the Jackson Hole National Monument 23 were also able to be classified as objects of historic or scientific interest, thus enabling the President to invoke the Antiquities Act. It should be noted that the proclamation of Jackson Hole as a national monument created such an uproar that Congress passed a statute eliminating the further establishment of national monuments in Wyoming **without congressional authority**.24 To date, Wyoming is the only state protected in this manner and **this statute is one of the few restrictions on the President's power** under the Antiquities Act.

That excludes oversight but includes the plan

Kaiser 80 The Official Specialist in American National Government, Congressional Research Service, the Library of Congress [Congressional Action to Overturn Agency Rules: Alternatives to the Legislative Veto; Kaiser, Frederick M., 32 Admin. L. Rev. 667 (1980)]

In addition to direct statutory overrides, there are a variety of statutory and nonstatutory techniques that have the effect of overturning rules, that prevent their enforcement, or that seriously impede or even preempt the promulgation of projected rules. For instance, a statute may alter the jurisdiction of a regulatory agency or extend the exemptions to its authority, thereby affecting existing or anticipated rules. Legislation that affects an agency's funding may be used to prevent enforcement of particular rules or to revoke funding discretion for rulemaking activity or both. Still other actions, less direct but potentially significant, are mandating agency consultation with other federal or state authorities and requiring prior congressional review of proposed rules (separate from the legislative veto sanctions). These last two provisions may change or even halt proposed rules by interjecting novel procedural requirements along with different perspectives and influences into the process.

It is also valuable to examine nonstatutory controls available to the Congress:

1. legislative, oversight, investigative, and confirmation hearings;

2. establishment of select committees and specialized subcommittees to oversee agency rulemaking and enforcement; 3. directives in committee reports, especially those accompanying legislation, authorizations, and appropriations, regarding rules or their implementation; 4. House and Senate floor statements critical of proposed, projected, or ongoing administrative action; and 5. direct contact between a congressional office and the agency or office in question. Such mechanisms are all indirect influences; unlike statutory provisions, they are neither self-enforcing nor legally binding by themselves. Nonetheless, nonstatutory devices are more readily available and more easily effectuated than controls imposed by statute. And some observers have attributed substantial influence to nonstatutory controls in regulatory as well as other matters.3 It is impossible, in a limited space, to provide a comprehensive and exhaustive listing of congressional actions that override, have the effect of overturning, or prevent the promulgation of administrative rules. Consequently, this report concentrates upon the more direct statutory devices, although it also encompasses committee reports accompanying bills, the one nonstatutory instrument that is frequently most authoritatively connected with the final legislative product. The statutory mechanisms surveyed here cross a wide spectrum of possible congressional action: 1. single-purpose provisions to overturn or preempt a specific rule; 2. alterations in program authority that remove jurisdiction from an agency; 3. agency authorization and appropriation limitations; 4. inter-agency consultation requirements; and 5. congressional prior notification provisions

That includes conditions

CAA 8,COURT OF APPEALS OF ARIZONA, DIVISION ONE, DEPARTMENT A, STATE OF ARIZONA, Appellee, v. JEREMY RAY WAGNER, Appellant., 2008 Ariz. App. Unpub. LEXIS 613

P10 The term "restriction" is not defined by the Legislature for the purposes of the DUI statutes. See generally A.R.S. § 28-1301 (2004) (providing the "[d]efinitions" section of the DUI statutes). In the absence of a statutory definition of a term, we look to ordinary dictionary definitions and do not construe the word as being a term of art. Lee v. State, 215 Ariz. 540, 544, ¶ 15, 161 P.3d 583, 587 (App. 2007) ("When a statutory term is not explicitly defined, we assume, unless otherwise stated, that the Legislature intended to accord the word its natural and obvious meaning, which may be discerned from its dictionary definition.").

P11 The dictionary definition of "restriction" is "[a] limitation or qualification." Black's Law Dictionary 1341 (8th ed. 1999). In fact, "limited" and "restricted" are considered synonyms. See Webster's II New Collegiate Dictionary 946 (2001). Under these commonly accepted definitions, Wagner's driving privileges were "restrict[ed]" when they were "limited" by the ignition interlock requirement. Wagner was not only [\*7] statutorily required to install an ignition interlock device on all of the vehicles he operated, A.R.S. § 28-1461(A)(1)(b), but he was also prohibited from driving any vehicle that was not equipped with such a device, regardless whether he owned the vehicle or was under the influence of intoxicants, A.R.S. § 28-1464(H). These limitations constituted a restriction on Wagner's privilege to drive, for he was unable to drive in circumstances which were otherwise available to the general driving population. Thus, the rules of statutory construction dictate that the term "restriction" includes the ignition interlock device limitation

Our definition is most legally precise

Plummer 29 J., Court Justice, MAX ZLOZOWER, Respondent, v. SAM LINDENBAUM et al., Appellants Civ. No. 3724COURT OF APPEAL OF CALIFORNIA, THIRD APPELLATE DISTRICT100 Cal. App. 766; 281 P. 102; 1929 Cal. App. LEXIS 404September 26, 1929, Decided, lexis

The word "restriction," when used in connection with the grant of interest in real property, is construed as being the legal equivalent of "condition." Either term may be used to denote a limitation upon the full and unqualified enjoyment of the right or estate granted. The words "terms" and "conditions" are often used synonymously when relating to legal rights. "Conditions and restrictions" are that which limits or modifies the existence or character of something; § Marked 10:27 § a restriction or qualification. It is a restriction or limitation modifying or destroying the original act with which it is connected, or defeating, terminating or enlarging an estate granted; something which defeats or qualifies an estate; a modus or quality annexed by him that hath an estate, or interest or right to the same, whereby an estate may be either defeated, enlarged, or created upon an uncertain event; a quality annexed to land whereby an estate may be defeated; a qualification or restriction annexed to a deed or device, by virtue of which an estate is made to vest, to be enlarged or defeated upon the happening or not happening of a particular event, or the performance or nonperformance of a particular act.

Hains, JD from Brigham Young University, 2011

(William M., “Challenging the Executive: The Constitutionality of Congressional Regulation of the President's Wartime Detention Policies,” 2011 B.Y.U.L. Rev. 2283, Lexis)

In response to the public outcry, Congress cut off funds for the release or transfer of Guantanamo Bay detainees into the United States. Congress placed funding restrictions in six separate laws in 2009 and 2010. n11 Each law made exceptions that allowed the [\*2286] President to transfer detainees to the United States "for the purposes of prosecuting such individual, or detaining such individual during legal proceedings." n12 Despite this allowance, the laws contained some restrictions on transfers for the purpose of prosecution. For example, the first law to impose these restrictions only allowed the President to transfer detainees to the United States forty-five days after submitting to Congress a classified "plan" for each detainee. n13 The plan had to include a national security risk assessment, steps to mitigate that risk, a cost analysis, and a statement of the "legal rationale and associated court demands." n14 The law also required the President to notify the governor of the receiving state two weeks before the transfer and certify "that the individual poses little or no security risk." n15 While subsequent laws added a few elements to the reporting requirement, they did not **significantly increase** the burden on the President. n16 **The only restriction placed on releasing or transferring detainees to other countries was a reporting requirement**: fifteen days before the move, the President had to notify Congress of the detainees' identities and destinations and provide risk assessments, risk mitigation plans, and the "terms of any agreement" - including any financial agreement - with the receiving countries. n17

### at: merlini

Merlini’s not an impact card

Cesare Merlini 11, nonresident senior fellow at the Center on the United States and Europe and chairman of the Board of Trustees of the Italian Institute for International Affairs, May 2011, “A Post-Secular World?”, Survival, Vol. 53, No. 2

Two scenarios

Two neatly opposed scenarios for the future of the world order illustrate the range of possibilities, albeit at the risk of oversimplification. The first scenario entails the premature crumbling of the post-Westphalian system. One or more of the acute tensions apparent today evolves into an open and traditional conflict between states, perhaps even involving the use of nuclear weapons. The crisis might be triggered by a collapse of the global economic and financial system, the vulnerability of which we have just experienced, and the prospect of a second Great Depression, with consequences for peace and democracy similar to those of the first. Whatever the trigger, the unlimited exercise of national sovereignty, exclusive self-interest and rejection of outside interference would likely be amplified, emptying, perhaps entirely, the half-full glass of multilateralism, including the UN and the European Union. Many of the more likely conflicts, such as between Israel and Iran or India and Pakistan, have potential religious dimensions. Short of war, tensions such as those related to immigration might become unbearable. Familiar issues of creed and identity could be exacerbated. One way or another, the secular rational approach would be sidestepped by a return to theocratic absolutes, competing or converging with secular absolutes such as unbridled nationalism.

One symptom that makes such a scenario plausible has become visible. Many commentators have identified anger or anxiety as a common driver of the Tea Party movement in the United States and the rise of xenophobic parties in Europe, perhaps stemming from a self-perception of decline. Anger (directed towards the neo-colonialist or pro-Israeli West or – especially recently – domestic authoritarian regimes) has also been associated with grievances in the Middle East, following the failure of earlier reformist and secular movements.10 Despite relative popular optimism, anger can also be detected in Asia, hand in hand with chauvinism and a sense of lack of appropriate recognition by others, stemming from a self-perception of rising influence and power.

The opposite scenario contemplates not an unprecedented era of peace

and prosperity, but rather continuity in the international system, with

further consolidation rather than rupture. Current conflicts and those most

likely to emerge from existing tensions are contained, thanks to diplomatic

or coercive instruments, and **major wars are avoided.** Economic and financial

give-and-take is kept under control and gives way to a more stable

global game, including increased safeguarding of public goods such as

the health of the planet. This scenario does not entail the United Nations

becoming a global government, nor the European Union turning into a

fully fledged federation, nor the various ‘Gs’ becoming boards of a global

corporation. But these international organisations, reformed to improve

representativeness and effectiveness, would remain to strengthen the rule

of law globally.

A major factor in the unfolding of this scenario might be the trend towards increased societal interaction, or even empathy. But there is also a risk that this transformation might lead to chaos. Domestically, civil society could become a challenge to the legitimacy and effectiveness of parliaments in representative democracies or an excuse for authoritarian repression. Internationally, governance may become more difficult if states are not fully in control. However, social revolutions driven by advances in science and technology (particularly telecommunications and the Internet) and improvements in the status of women worldwide (access to the labour market and above all control over reproduction), may also gradually enhance transnational relations and understanding and privilege a conciliatory approach to human relations over a confrontational one, with obvious but not radical differences from nation to nation.11

### 2ac discourse

**Reality outweighs representations**

**Wendt, 1999**

Alexander Wendt, Professor of International Security at Ohio State University, 1999, “Social theory of international politics,” gbooks

The effects of holding a relational theory of meaning on theorizing about world politics are apparent in **David Campbell's** provocative study of US foreign policy, which **shows** how the **threats** posed by the Soviets, immigration, drugs, and so on, **were constructed** out of US national security discourse.29 The book clearly shows that material things in the world did not force US decision-makers to have particular representations of them - the picture theory of reference does not hold. In so doing it highlights the discursive aspects of truth and reference, the sense in which objects are relationally "constructed."30 On the other hand, while emphasizing several times that he is not denying the reality of, for example, Soviet actions, he specifically eschews (p. 4) any attempt to assess the extent to which they caused US representations. Thus **he cannot address the extent to which US representations of the Soviet threat were accurate or true** (questions of correspondence). **He can only focus on the nature and consequences of the representations**.31 Of course, there is nothing in the social science rule book which requires an interest in causal questions, and the nature and consequences of representations are important questions. In the terms discussed below he is engaging in a constitutive rather than causal inquiry. However, I suspect **Campbell thinks that any attempt to assess the correspondence of discourse to reality is inherently pointless.** According to the relational theory of reference **we simply have no access to what the Soviet threat "really" was, and as such its truth is established entirely within discourse**, not by the latter's correspondence to an extra-discursive reality 32 **The main problem** with the relational theory of reference **is that it cannot account for the resistance of the world to certain representations, and thus for representational failures or m/'sinterpretations**. Worldly resistance is most obvious in nature: whether our discourse says so or not, pigs can't fly. But examples abound in society too. **In 1519 Montezuma faced the same kind of epistemological problem facing social scientists today: how to refer to people who, in his case, called themselves Spaniards. Many representations were conceivable**, and no doubt the one he chose - that they were **gods - drew on the discursive materials available to him. So why was he killed and his empire destroyed by an army hundreds of times smaller than his own**? The realist answer is that **Montezuma was simply wrong: the Spaniards were not gods, and had come instead to conquer his empire. Had Montezuma adopted this alternative representation of what the Spanish were, he might have prevented this outcome because that representation would have corresponded more to reality. The reality of the conquistadores did not force him to have a true representation**, as the picture theory of reference would claim, **but it did have certain effects - whether his discourse allowed them or not.** The external world to which we ostensibly lack access, in other words. often frustrates or penalizes representations. **Postmodernism gives us no insight into why this is so, and indeed, rejects the question altogether.33** The description theory of reference favored by empiricists focuses on sense-data in the mind while the relational theory of the postmoderns emphasizes relations among words, but they are similar in at least one crucial respect: neither grounds meaning and truth in an external world that regulates their content.34 Both privilege epistemology over ontology. What is needed is a theory of reference that takes account of the contribution of mind and language yet is anchored to external reality. The realist answer is the causal theory of reference. According to the causal theory the meaning of terms is determined by a two-stage process.35 First there is a "baptism/' in which some new referent in the environment (say, a previously unknown animal) is given a name; then this connection of thing-to-term is handed down a chain of speakers to contemporary speakers. Both stages are causal, the first because the referent impressed itself upon someone's senses in such a way that they were induced to give it a name, the second because the handing down of meanings is a causal process of imitation and social learning. Both stages allow discourse to affect meaning, and as such do not preclude a role for "difference" as posited by the relational theory. Theory is underdetermined by reality, and as such the causal theory is not a picture theory of reference. However, conceding these points does not mean that meaning is entirely socially or mentally constructed. In the realist view beliefs are determined by discourse and nature.36 This solves the key problems of the description and relational theories: our ability to refer to the same object even if our descriptions are different or change, and the resistance of the world to certain representations. **Mind and language help determine meaning, but meaning is also regulated by a mind-independent, extra-linguistic world**.

### AT: roleplaying bad

**Simulation allows us to influence state policy AND is key to agency**

**Eijkman 12**

The role of simulations in the authentic learning for national security policy development: Implications for Practice / Dr. Henk Simon Eijkman. [electronic resource] <http://nsc.anu.edu.au/test/documents/Sims_in_authentic_learning_report.pdf>. Dr Henk Eijkman is currently an independent consultant as well as visiting fellow at the University of New South Wales at the Australian Defence Force Academy and is Visiting Professor of Academic Development, Annasaheb Dange College of Engineering and Technology in India. As a sociologist he developed an active interest in tertiary learning and teaching with a focus on socially inclusive innovation and culture change. He has taught at various institutions in the social sciences and his work as an adult learning specialist has taken him to South Africa, Malaysia, Palestine, and India. He publishes widely in international journals, serves on Conference Committees and editorial boards of edited books and international journal

However, whether as an approach to learning, innovation, persuasion or culture shift, policy simulations derive their power from two central features: their combination of simulation and gaming (Geurts et al. 2007). 1. The simulation element: the unique combination of simulation with role-playing.The unique simulation/role-play mix enables participants to create **possible futures** relevant to the topic being studied. This is diametrically opposed to the more traditional, teacher-centric approaches in which a future is produced for them. In policy simulations, possible futures are much more than an object of tabletop discussion and verbal speculation. ‘**No other technique** allows a group of participants to engage in collective action in a safe environment to create and analyse the futures they want to explore’ (Geurts et al. 2007: 536). 2. **The game element:** the interactive and tailor-made modelling and design of the policy game. The actual run of the policy simulation is only one step, though a most important and visible one, in a collective process of investigation, communication, and evaluation of performance. In the context of a post-graduate course in public policy development, for example, a policy simulation is a dedicated game constructed in collaboration with practitioners to achieve a high level of proficiency in relevant aspects of the policy development process. To drill down to a level of finer detail, **policy development simulations**—as forms of interactive or participatory modelling— are particularly effective in developing participant knowledge and skills in the five key areas of the policy development process (and success criteria), namely: Complexity, Communication, Creativity, Consensus, and Commitment to action (‘the five Cs’). The capacity to provide effective learning support in these five categories has proved to be particularly helpful in strategic decision-making (Geurts et al. 2007). Annexure 2.5 contains a detailed description, in table format, of the synopsis below.

### 2ac nukes feasible

We’re not overhyping threats----Hellman says nuke terror feasible—means and motives

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; § Marked 10:27 § 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.