# 1NC

### 1NC

#### Interpretation – restrictions are prohibitions on action

CJS 31

Volume 54, p. 735

RESTRICT: To confine; to limit; to prevent (a person or thing) from passing a certain limit in any kind of action; to restrain; to restrain without bounds.

#### Violation – the aff doesn’t prohibit – reporting, monitoring, or supervising don’t meet

Schiedler-Brown 12

Jean Schiedler-Brown 12, Attorney, Jean Schiedler-Brown & Associates, Appellant Brief of Randall Kinchloe v. States Dept of Health, Washington, The Court of Appeals of the State of Washington, Division 1, <http://www.courts.wa.gov/content/Briefs/A01/686429%20Appellant%20Randall%20Kincheloe%27s.pdf>

3. The ordinary definition of the term "restrictions" also does not include the reporting and monitoring or supervising terms and conditions that are included in the 2001 Stipulation. ¶ Black's Law Dictionary, 'fifth edition,(1979) defines "restriction" as; ¶ A limitation often imposed in a deed or lease respecting the use to which the property may be put. The term "restrict' is also cross referenced with the term "restrain." Restrain is defined as; To limit, confine, abridge, narrow down, restrict, obstruct, impede, hinder, stay, destroy. To prohibit from action; to put compulsion on; to restrict; to hold or press back. To keep in check; to hold back from acting, proceeding, or advancing, either by physical or moral force, or by interposing obstacle, to repress or suppress, to curb. ¶ In contrast, the terms "supervise" and "supervisor" are defined as; To have general oversight over, to superintend or to inspect. See Supervisor. A surveyor or overseer. . . In a broad sense, one having authority over others, to superintend and direct. The term "supervisor" means an individual having authority, in the interest of the employer, to hire, transfer, suspend, layoff, recall, promote, discharge, assign, reward, or discipline other employees, or responsibility to direct them, or to adjust their grievances, or effectively to recommend such action, if in connection with the foregoing the exercise of such authority is not of a merely routine or clerical nature, but required the use of independent judgment. ¶ Comparing the above definitions, it is clear that the definition of "restriction" is very different from the definition of "supervision"-very few of the same words are used to explain or define the different terms. In his 2001 stipulation, Mr. Kincheloe essentially agreed to some supervision conditions, but he did not agree to restrict his license.

#### Restrictions on authority are distinct from conditions

Connor 78

William Conner 78, former federal judge for the United States District Court for the Southern District of New York United States District Court, S. D. New York, CORPORACION VENEZOLANA de FOMENTO v. VINTERO SALES, <http://www.leagle.com/decision/19781560452FSupp1108_11379>

Plaintiff next contends that Merban was charged with notice of the restrictions on the authority of plaintiff's officers to execute the guarantees. Properly interpreted, the "conditions" that had been imposed by plaintiff's Board of Directors and by the Venezuelan Cabinet were not "restrictions" or "limitations" upon the authority of plaintiff's agents but rather conditions precedent to the granting of authority. Essentially, then, plaintiff's argument is that Merban should have known that plaintiff's officers were not authorized to act except upon the fulfillment of the specified conditions.

#### Voting issue –

#### Limits – dozens of tiny mechanisms and small subsets of areas create an infinite number of affs that core lit doesn’t check - only prohibitions on authority guarantee neg ground - their interpretation lets affs no link the best neg offense like deference and flexibility

#### Precision - only our interpretation defines “restrictions on authority” - that’s key to adequate preparation and policy analysis

### 1NC

#### Obama’s Syria maneuver has maximized presidential war powers because it’s on his terms

Posner 9/3

(Eric, Law Prof at University of Chicago, Obama Is Only Making His War Powers Mightier, www.slate.com/articles/news\_and\_politics/view\_from\_chicago/2013/09/obama\_going\_to\_congress\_on\_syria\_he\_s\_actually\_strengthening\_the\_war\_powers.html)

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

#### OCOs are the litmus test for Presidential war powers authority

Lorber ’13

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

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 [limit] 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.

#### The plan causes countries to doubt the credibility of our threats – collapses security guarantees and deterrence – causes nuclear war

Zeisberg 4

(MARIAH ZEISBERG, Research Fellow, The Political Theory Project, Department of Political Science, "INTERBRANCH CONFLICT AND CONSTITUTIONAL MAINTENANCE: THE CASE OF WAR POWERS" SEPTEMBER 22, 2004, KB)

The first significant argument of pro-Presidency insularists is that flexibility is a prime value in the conduct of foreign affairs, and especially war. Implicit in this argument is the recognition that the executive is functionally superior to Congress in achieving flexibility and swiftness in war operations, a recognition I share. The Constitution cannot be meant to curtail the very flexibility that may be necessary to preserve the nation; and yet, according to the insularists, any general norm which would include Congress in decision-making about going to war could only undermine that flexibility. Writing on the War Powers Act, Eugene Rostow predicts that it would, “put the Presidency in a straightjacket of a rigid code, and prevent new categories of action from emerging, in response to the necessities of a tense and unstable world.” In fact, Rostow believes, “[t]he centralization of authority in the president is particularly crucial in matters of national defense, war, and foreign policy, where a unitary executive can evaluate threats, consider policy choices, and mobilize national resources with a speed and energy that is far superior to any other branch.” Pro-presidency insularists are fond of quoting Hamilton, who argued that “[o]f all the cares or concerns of government, the direction of war most peculiarly demands those qualities which distinguish the exercise of power by a single hand.” ¶ This need for flexibility, some insularists argue, is especially acute given modern conditions, where devastating wars can develop quickly. Today, “many foreign states have the power to attack U.S. forces - and some even the U.S. mainland - almost instantly,” and in such a world it is impracticable to require the President to seek advance authorization for hostilities. Such a requirement would simply be too risky to U.S. security. We furthermore face a nuclear age, and the system of deterrence that operates to contain that threat requires that a single person be capable of responding to nuclear attack with nuclear weapons immediately. Rostow writes, “the requirement for advance authorization would collapse the system of deterrence, making preemptive strikes by our enemies more likely.” Hence, “modern conditions” require the President to “act quickly, and often alone.” ¶ While this does not mean that Congress has no role to play in moments of crisis, it does mean that Congress should understand its role largely in terms of cooperating with the President to support his negotiations and decisions regarding relationships with foreign powers. Rostow writes,¶ “Congress should be able to act effectively both before and after moments of crisis or potential crisis. It may join the President in seeking to deter crisis by publicly defining national policy in advance, through the sanctioning of treaties or other legislative declarations. Equally, Congress may participate formally in policymaking after the event through legislative authorization of sustained combat, either by means of a declaration of war, or through legislative action having more limited legal and political consequences. Either of these devices, or both in combination, should be available in situations where cooperation between the two branches is indicated at many points along an arc ranging from pure diplomacy at one end to a declaration of war at the other.” ¶ In other words, for Congress to understand itself as having any justifiable role in challenging executive security determinations, especially at moments of crisis, would be to undermine the strength that the executive requires in order to protect the nation. Conflict in this domain represents political degradation.¶ Flexibility is also a key value to support the stability of the global security order, some pro-Presidency insularists argue. International security systems require guarantees that an attack on an ally will be retaliated as quickly as possible. Given such a system, the requirement of congressional consultation “vitiates the security guarantee.” It is important to note that the US does not simply play a role in international collective security systems: it is a central player in those systems, and hence “it is necessary for the system that U.S. participation be assured and credible. But this means that in order to support collective security, the fundamental function for Congress is to support the executive in ways that send a clear message of national resolve, so unequivocal and unmistakable that international pillagers and those who advise them can have no doubts.” ¶ This value of flexibility is sometimes applied to the mechanisms for foreign policy themselves. John Yoo, for example, argues that there must be a diversity of mechanisms for going to war, including unilateral action by the President. On Yoo’s account, Congress is granted authority in foreign affairs in times of peace, the President for times of danger. Yoo interprets the understructured nature of war powers to indicate that “the Framers did not intend the Constitution to establish a single, correct method for going to war. . . [d]uring times of relative peace, Congress can use its authority over funding and the raising of the military to play a leading role in foreign policy. In times of emergency or national danger, however, the President can seize the initiative in warmaking.” ¶ A second insularist argument is that the “nature of foreign affairs” is such that this domain cannot be guided by law. Jefferson’s oft-cited quote, that “[t]he transaction of business with foreign nations is Executive altogether,” is sometimes used in support of this argument, although I do not believe Jefferson understood himself to be making this point. Robert Bork is instead the most prominent insularist arguing this position. Far from believing that the President’s use of force can be bound by law, Bork denies that law governing foreign affairs—whether domestic or international—even exists. In Bork’s own words,¶ “[T]here are areas of life, and the international use of armed force seems to be one of them, in which the entire notion of law—law conceived as a body of legal principles declared in advance to control decisions to be made in the future—where that conception of law is out of place. The pretense that there is such a law and that it has been constantly violated, has debilitating effects upon our foreign policy . . . [t]wo examples come to mind: one is international law about the use of force, and the other is domestic law, that is, the War Powers Act. These two bodies of ‘law’ arise from different sources, but they are alike in that they are not law in any recognizable sense. They are not enforceable.” ¶ Since law in this domain simply cannot exist, the idea of a legislative body playing any role in guiding decisions here is simply senseless. Bork points us to the simple fact of the matter—that “Presidential use or support of force abroad will succeed when the public approves and fail when it disapproves. Law has little to do with the outcome.” ¶ The third important argument on behalf of insularity is that Congress already possesses all the power it needs to contain a wayward executive. This power is wielded mainly through Congress’ “power of the purse,” but also through Congress’ power to raise the military and commission (or de-commission) troops. It is in the course of approving Presidential requests for funding measures that Congress discusses the merits of his actions, and Congress retains the simple power to block the president’s actions simply by refusing him funds or military resources. Yoo argues,¶ “One might respond that it is unreasonable to expect Congress to use its appropriations powers to cut off troops in the field. Surely members of Congress will not take actions that might be interpreted as undermining the safety and effectiveness of the military, once committed and in the midst of hostilities. We should not mistake a failure of political will, however, for a violation of the Constitution. Congress undoubtedly possessed the power to end the Kosovo war, it simply chose not to. Affirmatively providing funding for a war, or at the very least refusing to cut off previous appropriations, represents a political determination by Congress that it will provide minimal support for a war, but that ultimately it will leave it to the President to receive the credit either for success or failure.” ¶ Furthermore, it is simply a fact that the President relies upon Congress to wage the wars he wishes to pursue. As Bobbit points out, unless Congress “by statute, provides an army, transport, weapons, and materials . . . there is nothing for the President to command.” Bobbit insists, though, that this does not mean that Congress can appropriately “interfere in the operation of that power” once handed over. Just as Congress, once it has established and vested the judiciary, has no authority to interfere in the operation of the judicial power, so too Congress, once it vests the President with command of a military, has no authority to interfere in how that command is used. Hence Bobbit believes that the only constitutionally legitimate way for Congress to engage in decisionmaking on the use of the sovereign war power is to remove forces from the command of the President. Bobbit continues, “[a]s a structural matter, Congress has the first and last word. It must provide forces before the President can commence hostilities, and it can remove those forces, by decommissioning them or by forbidding their use in pursuit of a particular policy at any time.” Bobbit is quite explicit about the implications of his position:¶ “Does this mean that presidents can simply ransack the current Defense Appropriations Act for available forces and that Congress then has no way to stop a president from unilaterally making war so long as one-third plus one of the members of one House sustains his veto - for the balance of the biennium? It may well mean that.” ¶ The fourth argument is that the kind of challenging characteristic of interbranch deliberation would endanger the well-being of troops in the field, as foreign nations interpret Congressional challenging to mean that we lack the will to support our soldiers. This argument is not about the comparative advantages of the presidency as an institution, or about the meaning of law: rather, it directly challenges the value of conflict itself. In fact, as we saw in chapter two, settlement theorists and realists seem to believe that the conditions of war and insecurity are the most congenial territory for their claims about the importance of deference and settlement, precisely because peace, stability, and the very possibility of rights-protection are all at stake in this issue. Rostow cites Dean Acheson’s comments on the Korean War:¶ “An incredulous country and world held its breath and read the mounting casualties suffered by these gallant troops, most of them without combat experience. In the confusion of the retreat even their divisional commander, Major General William F. Dean, was captured. Congressional hearings on a resolution of approval at such a time, opening the possibility of endless criticism, would hardly be calculated to support the shaken morale of the troops or the unity that, for the moment, prevailed at home. The harm it could do seemed to me to outweigh the little good that might ultimately accrue.”

#### Restrictions turn cyber war

Baker 12

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

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

### 1NC

#### Restrictions on executive war powers DO NOTHING for the state of political legal exception we live in and only gives further justification for violent intervention on the basis of legality

Dyzenhaus 05

(David, is a professor of Law and Philosophy at the University of Toronto, and a Fellow of the Royal Society of Canada, “Schmitt v. Dicey: Are States of Emergency Inside or Outside the Legal Order?” Cardozo Law Review 27)

Rossiter had in mind Lincoln's actions during the Civil War, including the proclamation by which Lincoln, without the prior authority of Congress, suspended habeas corpus. n35 Lincoln, he said, subscribed to a theory that in a time of emergency, the President could assume whatever legislative, executive, and judicial powers he thought necessary to preserve the nation, and could in the process break the "fundamental laws of the nation, if such a step were unavoidable." n36 This power included one ratified by the Supreme Court: "an almost unrestrained power to act toward insurrectionary citizens as if they were enemies of the United States, and thus place them outside the protection of the Constitution." Rossiter's difficulties here illustrate rather than solve the tensions inherent in the idea of constitutional dictatorship. On the one hand, he wants to assert that emergency rule in a liberal democracy can be constitutional in nature. "Constitutional" implies restraints and limits in accordance not only with law, but with fundamental laws. These laws are not the constitution that is in place for ordinary times; rather, they are the laws that govern the management of exceptional times - the eleven criteria that he developed for constitutional dictatorship. The criteria are either put within the discretion of the dictator - they are judgments about necessity - or are couched as limits that should be enshrined either in the constitution or in legislation. However, Rossiter does not properly address the fact that judgments about necessity are for the dictator to make, which means that these criteria are not limits or constraints but merely factors about which the dictator will have to decide. Other criteria look more like genuine limits. Moreover, they are limits that could be constitutionally enshrined - for example, the second criterion, which requires that the person who makes the decision that there is an emergency should not be the person who assumes dictatorial powers. Yet, as we have seen, Rossiter's foremost example of the modern constitutional dictator, Lincoln, not only gave himself dictatorial powers but, Rossiter supposes, had no choice but to do this. Moreover, if these criteria are constitutionally enshrined, so that part of the constitution is devoted to the rules that govern the time when the rest of the constitution might be suspended, they still form part of the constitution. So, no less than the ordinary constitution, what we can think of as the exceptional or emergency constitution - the constitution that governs the state of emergency - is subject to suspension should the dictator deem this necessary. This explains why, on the other hand, Rossiter equated emergency rule with potentially unlimited dictatorship, with Locke's idea of prerogative. And Rossiter said, "whatever the theory, in moments of extreme national emergency the facts have always been with ... John Locke." So Rossiter at one and the same time sees constitutional dictatorship as unconstrained in nature and as constrainable by principles - his eleven criteria. The upshot is that "constitutional" turns out not to mean what we usually take it to mean; rather, it is a misleading name for the hope that the person who assumes dictatorial powers does so because of a good faith evaluation that this is really necessary and with the honest and steadfast intention to return to the ordinary way of doing things as soon as possible. Giorgio Agamben is thus right to remark that the bid by modern theorists of constitutional dictatorship to rely on the tradition of Roman dictatorship is misleading. n39 They rely on that tradition in an effort to show that dictatorship is constitutional or law-governed. But in fact they show that dictatorship is in principle absolute - the dictator is subject to whatever limits he deems necessary, which means to no limits at all. As H.L.A. Hart described the sovereign within the tradition of legal positivism, the dictator is an uncommanded commander. n40 He [\*2015] operates within a black hole, in Agamben's words, "an emptiness of law." n41 Agamben thus suggests that the real analogue to the contemporary state of emergency is not the Roman dictatorship but the institution of iustitium, in which the law is used to produce a "juridical void" - a total suspension of law. n42 And in coming to this conclusion, Agamben sides with Carl Schmitt, his principal interlocutor in his book. However, it is important to see that Schmitt's understanding of the state of exception is not quite a legal black hole, a juridically produced void. Rather, it is a space beyond law, a space which is revealed when law recedes, leaving the state, represented by the sovereign, to act. In substance, there might seem to be little difference between a legal black hole and space beyond law since neither is controlled by the rule of law. But there is a difference in that nearly all liberal legal theorists find the idea of a space beyond law antithetical, even if they suppose that law can be used to produce a legal void. This is so especially if such theorists want to claim for the sake of legitimacy that law is playing a role, even if it is the case that the role law plays is to suspend the rule of law. Schmitt would have regarded such claims as an attempt to cling to the wreckage of liberal conceptions of the rule of law brought about by any attempt to respond to emergencies through the law. They represent a vain effort to banish the exception from legal order. Because liberals cannot countenance the idea of politics uncontrolled by law, they place a veneer of legality on the political, which allows the executive to do what it wants while claiming the legitimacy of the rule of law. We have seen that Rossiter presents a prominent example which supports Schmitt's view, and as I will now show, it is a depressing fact that much recent post 9/11 work on emergencies is also supportive of Schmitt's view. II. Responding to 9/11 For example, Bruce Ackerman in his essay, The Emergency Constitution, n43 starts by claiming that we need "new constitutional concepts" in order to avoid the downward spiral in protection of civil liberties that occurs when politicians enact laws that become increasingly repressive with each new terrorist attack. n44 We need, he says, to rescue the concept of "emergency powers ... from fascist thinkers like Carl Schmitt, who used it as a battering ram against liberal [\*2016] democracy." n45 Because Ackerman does not think that judges are likely to do, or can do, better than they have in the past at containing the executive during an emergency, he proposes mainly the creative design of constitutional checks and balances to ensure, as did the Roman dictatorship, against the normalization of the state of emergency. Judges should not be regarded as "miraculous saviors of our threatened heritage of freedom." n46 Hence, it is better to rely on a system of political incentives and disincentives, a "political economy" that will prevent abuse of emergency powers. He calls his first device the "supramajoritarian escalator" n48 - basically the requirement that a declaration of a state of emergency requires legislative endorsement within a very short time, and thereafter has to be renewed at short intervals, with each renewal requiring the approval of a larger majority of legislators. The idea is that it will become increasingly easy with time for even a small minority of legislators to bring the emergency to an end, thus decreasing the opportunities for executive abuse of power. n49 The second device requires the executive to share security intelligence with legislative committees and that a majority of the seats on these committees belong to the opposition party. Ackerman does see some role for courts. They will have a macro role should the executive flout the constitutional devices. While he recognizes both that the executive might simply assert the necessity to suspend the emergency constitution and that this assertion might enjoy popular support, he supposes that if the courts declare that the executive is violating the constitution, this will give the public pause and thus will decrease incentives on the executive to evade the constitution. n51 In addition, the courts will have a micro role in supervising what he regards as the inevitable process of detaining suspects without trial for the period of the emergency. Suspects should be brought to court and some explanation should be given of the grounds of their detention, not so that they can contest it - a matter which Ackerman does not regard as practicable - but in order both to give the suspects a public identity so that they do not disappear and to provide a basis for compensation once the emergency is over in case the executive turns out to have fabricated [\*2017] its reasons. He also wishes to maintain a constitutional prohibition on torture, which he thinks can be enforced by requiring regular visits by lawyers. Not only is the judicial role limited, but it is clear that Ackerman does not see the courts as having much to do with preventing a period of "sheer lawlessness." n53 Even within the section on the judiciary, he says that the real restraint on the executive will be the knowledge that the supramajoritarian escalator might bring the emergency to an end, whereupon the detainees will be released if there is no hard evidence to justify detaining them. In sum, according to Ackerman, judges have at best a minimal role to play during a state of emergency. We cannot really escape from the fact that a state of emergency is a legally created black hole, a lawless void. It is subject to external constraints, controls on the executive located at the constitutional level and policed by the legislature. But internally, the rule of law does next to no work; all that we can reasonably hope for is decency. But once one has conceded that internally a state of emergency is more or less a legal black hole because the rule of law, as policed by judges, has no or little purchase, it becomes difficult to understand how external legal constraints, the constitutionally entrenched devices, can play the role Ackerman sets out. Recall that Ackerman accepts that the reason we should not give judges more than a minimal role is the history of judicial failure to uphold the rule of law during emergencies in the face of executive assertions of a necessity to operate outside of law's rule. For that reason, he constructs a political economy to constrain emergency powers. But that political economy still has to be located in law in order to be enforceable, which means that Ackerman cannot help but rely on judges. But why should we accept his claim that we can rely on judges when the executive asserts the necessity of suspending the exceptional constitution, the constitution for the state of emergency, when one of his premises is that we cannot so rely? Far from rescuing the concept of emergency powers from Schmitt, Ackerman's devices for an emergency constitution, an attempt to update Rossiter's model of constitutional dictatorship, fails for the same reasons that Rossiter's model fails. Even as they attempt to respond to Schmitt's challenge, they seem to prove the claim that Schmitt made in late Weimar that law cannot effectively enshrine a distinction between constitutional dictatorship and dictatorship. They appear to be vain attempts to find a role for law while at the same time conceding that law has no role. Of course, this last claim trades on an ambiguity in the idea of the rule of law between, on the one hand, the rule of law, understood as the rule of substantive principles, and, on the other, rule by law, where as long as there is a legal warrant for what government does, government will be considered to be in compliance with the rule of law. Only if one holds to a fairly substantive or thick conception of the rule of law will one think that there is a point on a continuum of legality where rule by law ceases to be in accordance with the rule of law. Ackerman's argument for rule by law, by the law of the emergency constitution, might not answer Schmitt's challenge. But at least it attempts to avoid dignifying the legal void with the title of rule of law, even as it tries to use law to govern what it deems ungovernable by law. The same cannot be said of those responses to 9/11 that seem to suggest that legal black holes are not in tension with the rule of law, as long as they are properly created. While it is relatively rare to find a position that articulates so stark a view, it is quite common to find positions that are comfortable with grey holes, as long as these are properly created. A grey hole is a legal space in which there are some legal constraints on executive action - it is not a lawless void - but the constraints are so insubstantial that they pretty well permit government to do as it pleases. And since such grey holes permit government to have its cake and eat it too, to seem to be governing not only by law but in accordance with the rule of law, they and their endorsement by judges and academics might be even more dangerous from the perspective of the substantive conception of the rule of law than true black holes.

#### Our alternative is to recognize the necessity of the opposition. Sovereignty necessarily functions in exception to the law. This exception is necessary to avoid the universal violence of the Law and the affirmative.

Rasch 2k

(William. "Conflict as a Vocation: Carl Schmitt and the Possibility of Politics." Theory Culture Society 17.1)

It is not difficult to see that the polemical elevation of sovereignty over the rule of law replicates a lively historical opposition, one that can be perhaps best evoked by that happy pair, Hobbes and Locke. Within the liberal tradition, the rule of law invokes reason and calculability in its battles against the arbitrary and potentially despotic whim of an unrestrained sovereign. The legitimacy of the sovereign is thus replaced by a legality that claims to provide its own immanent and unforced legitimacy. Predictable and universally accessible reason - the normative validity of an "uncorked consensus", to use the words of a prominent modern exponent - gently usurps, so it is claimed, the place that would otherwise be occupied by a cynical, pragmatic utilitarianism and the tyranny of a dark, incalculable will. The rule of law brings all the comforts of an uncontroversial, rule-based, normative security as if legality preceded by way of simple logical derivation, abolishing above all the necessity of decisions. Schmitt clearly will have none of this and in various writings attempts to expose what he considers to be the two-fold fallacy of the liberal position. As we have seen, if taken at its word, legality, or the rule of law, is seen by Schmitt to be impotent; it can neither legitimize nor effectively defend itself against determined enemies in times of crisis. Were law truly the opposite of force, it would cease to exist. But this self-description is deceptive, for if judged by its deeds, the same liberal regime that enunciates the self-evidence validity of universal norms strives to enact a universal consensus that is, indeed, far from uncorked. The rule of law inevitably reveals itself, precisely during moments of crisis, as the force of law, perhaps, not every bit as violent and "irrational" as the arbitrary tyrant, but nonetheless compelling and irresistible - indeed, necessarily so. Thus, Schmitt would argue the distinction between "decision", "force" and sovereignty", on the one hand, and the "rule of law", on the other, is based on a blithe and simple illusion. What agitates Schmitt is not the force, but the deception. More precisely, what agitates Schmitt is what he perceives to be the elimination of politics in the name of a higher legal or moral order. In its claim to a universal, normative, rule-bound validity, the liberal sleight-of-hand reveals itself to be not the opposite of force, but a force that outlaws opposition. In resurrecting the notion of sovereignty, therefore, Schmitt sees himself as one who rescues a legitimate notion of politics. Of course, this rescue attempt is itself political, a battle over the correct definition of politics. That is, we are not merely dealing with a logical problem, and not merely dealing with a desire to provide constitutional mechanisms that would prevent the self-dissolution of the constitution. Rather, we are dealing with a contest between a particularist notion of politics, in which individual conflicts can be resolved, but in which antagonism as a structure and reservoir of possible future conflicts is never destroyed, versus politics as the historical unfolding and pacific expansion of the universal morality. To evoke the long shadows of an ongoing contemporary debate, we are dealing with the difference between a politics of dissensus and a politics of consensus. Whereas the latter ideology entails an explicit or implicit belief in the "highest good" that can be rationally discerned and achieved, a "right regime", to use Leo Strauss's term, or the "just society" that hopes to actualize aspects of the City of God here on earth, the former stresses the necessity of determining a workable order where no single order bears the mantle of necessity, in fact, where all order is contingent, hence imperfect, and thus seeks to make the best of an inherently contradictory world by erecting structures that minimize self-inflicted damage. In Schmitt's eyes, the elements of such a structure must be the manifold of sovereign states. The liberal says there can only be one world-wide sovereign, the sovereignty of a universal moral and legal order. Schmitt counters with a plurality of equal sovereigns, for only in this way, he believes, can the economic and moral extinction of politics be prevented. Politics, on this view, is not the means by which the universally acknowledged good is actualized, but the mechanism that negotiates and limits disputes in the absence of any universally acknowledged good. Politics exists, in other words, because the just society does not.

#### This requires the unchecked authority of the executive to respond to the exception.

Nagan and Haddad 12

(Winston and Aitza, "Sovereignty in Theory and Practice." San Diego International Law Journal 13)

Although Schmitt was German, his ideas about sovereignty, and the political exception have had influence on the American theory and practice of sovereignty. Carl Schmitt was a philosophic theorist of sovereignty during the Third Reich. n375 His ideas about sovereignty and its above the law placement in the political culture of the State have important parallels in the developing discourse in the United States about the scope of presidential authority and power. His views have attracted the attention of American theorists. Schmitt developed his view of sovereignty on the concept described as "the exception". n376 This idea suggests that the sovereign or executive may invoke the idea of exceptional powers which are distinct from the general theory of the State. In Schmitt's view, the normal condition of the functions of the theory of a State, rides with the existence of the idea of the "exception." The exception is in effect intrinsic to the idea of a normal State. In his view, [\*487] the normal legal order of a State depends on the existence of an exception. n377 The exception is based on the continuing existence of an existential threat to the State and it is the sovereign that must decide on the exception. n378 In short, the political life of a State comprises allies and enemies. For the purpose of Statecraft, "an enemy exists only when at least potentially, one fighting collectivity of people confronts another similar collectivity." n379 In this sense, the political reality of the State always confronts the issue of the survival of the group. This reality is explained as follows. The political is the most intense and extreme antagonism, and every concrete antagonism becomes that much more political the closer it approaches the most extreme point, that of the friend-enemy grouping. \*\*\* As an ever present possibility [war] is the leading presupposition which determines in a characteristic way human action and thinking and hereby creates a specifically political behavior.\*\*\* A world in which the possibility of war is utterly eliminated, a completely pacified globe, would be a world without the distinction between friend and enemy and hence a world without politics. n380 Schmitt's view bases the supremacy of the exception on the supremacy of politics and power. n381 Thus, the exception, as rooted in the competence of the executive, is not dependent on law for its authority but on the conditions of power and conflict, which are implicitly pre-legal. n382 The central idea is that in an emergency, the power to decide based on the exception accepts its normal superiority over law on the basis that the suspension of the law is justified by the pre-legal right to self-preservation. n383 Schmitt's view is a powerful justification for the exercise of extraordinary powers, which he regards as ordinary, by executive authority. This is a tempting view for executive officers but it may not be an adequate explanation of the interplay of power, legitimacy, and the constitutional foundations of a rule of law State. In a later section, we draw on insights from the New Haven School, which deals empirically with the problem of power and the problem of constituting authority using the methods of contextual mapping. Nonetheless, Schmitt's view provides support for theorists who seek to enlarge executive power on the unitary presidency theory.

### 1NC

#### The 1ACs attempt to restrict OFFENSIVE cyber operations may be good in policy but their apocalyptic justification for doing so is based on a flawed epistemology that ensures serial policy failure and self-fulfilling prophecies

Lawson 2012 (Sean Lawson is Assistant Professor in the Department of Communication at the University of Utah. His essays on science, technology, and security have appeared in the journals Social Studies of Science, Security Dialogue, Cold War History and Journal of Information Technology & Politics. "Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States"; First Monday, <http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270>)

Although in the case of the law of war, cyber war proponents have too quickly abandoned definitions, rules, and norms of war that are and should still be relevant to cyber conflict, in the case of cyber deterrence, many of these same individuals have too quickly adopted a framework that is “deeply flawed and largely unworkable” (Lewis, 2009b). First and foremost, this is the case because, as Martin Libicki of RAND notes, “Cyberspace is its own medium with its own rules. [...] Thus, deterrence and warfighting tenets established in other media do not necessarily translate reliably into cyberspace” [30]. Not only does the nuclear deterrence analogy tend to lead its users to “exaggerate the destructive capacity of cyber weapons,” it also results in a tendency to focus on hypothetical worst cases while ignoring actual threats (Lewis, 2009b). For example, while Raduege admitted that “low–level” attacks are predominant, he nonetheless advocated that national policy should focus on “strategic attacks” that “could one day” occur (Raduege, 2011). This tendency presents several problems. First, if cyber weapon capabilities have been exaggerated, then it is unlikely that strategic cyber attacks, if they did occur, could be decisive in the way that nuclear weapons could be [31]. Ironically, however, without the potential for decisiveness, the threat of cyber retaliation alone would likely have little deterrent value, meaning that one would have to rely upon threats of physical retaliation to deter cyber attacks. In turn, this could encourage an escalation to physical confrontation — that is, assuming the defender follows through on his threat of retaliation, without which any future threats would lose credibility. Second, the threat of massive retaliation, either cyber or physical, has not and will not deter the actual and pervasive “low–level” cyber attacks experienced on a daily basis. It is important to remember that during the Cold War, the threat of massive retaliation did not deter all war. It only deterred all–out nuclear war. As Raduege (2011) notes, the Cold War ended up taking the form of numerous proxy wars fought around the globe, from Southeast Asia to Latin America. Similarly, not only will U.S. capabilities for and threats of massive retaliation in response to cyber attacks not deter the daily occurrence of low–level attacks, it will likely encourage potential adversaries to constantly seek to pose challenges that fall below the threshold that would trigger massive retaliation, either cyber or kinetic. Finally, all of this points to another problem: a simplification of nuclear deterrence and Cold War history. Nuclear strategists confronted these same problems in the 1960s as it became increasingly clear that Eisenhower era threats of “massive retaliation” had lost their credibility and value. This resulted in a robust debate about “flexible response,” escalation, the role of conventional forces in promoting nuclear deterrence, and much more. In short, there was no one nuclear deterrence strategy during the Cold War. Nuclear strategy evolved over time (Freedman, 1989). Unfortunately, current notions of cyber deterrence are more akin to the 1950s strategy of massive retaliation that was ultimately deemed incredible and dangerous in comparison to the later, more nuanced variants of deterrence. Finally, a number of other differences between nuclear weapons and cyber weapons render the quest for cyber deterrence inappropriate at best and even potentially counterproductive. Cyber attacks generally suffer from a crisis of cause and effect. In one variant, this is what cyber war experts call the “attribution problem” — i.e., it is difficult to know who the attacker is because of online anonymity. As Mike McConnell and others have noted, deterrence is impossible without the ability to credibly threaten the attacker. But deterrence is also difficult if one cannot reliably know in advance the effects of one’s response. In cyberspace, the “collateral damage” caused by cyber attacks can be unpredictable, which could reduce “the willingness of political leaders to incur the risk of a retaliatory response that goes awry, widening a conflict or creating unfavorable political consequences” (Lewis, 2009a). The unpredictable results of a cyber response could encourage the use of a more predictable but more deadly physical response. It is for all of these reasons that Myriam Dunn Cavelty warns against the use of the language of deterrence and aggression with respect to cyber threats. Such language is counterproductive because it results in a self–fulfilling prophecy: actions taken by one state to increase its security can make others feel less secure, resulting in their taking similar actions, which confirms to the first state that it is insecure, and so on (Dunn Cavelty, 2010).

#### The PARADOX OF RISK makes this NOT resolvable by weighing the plan.  If impact is calculated by multiplying probability and magnitude, any probability of an infinite impact irrationally registers as infinite

Kessler 2008 (Oliver Kessler, Sociology at University of Bielefeld, “From Insecurity to Uncertainty: Risk and the Paradox of Security Politics” *Alternatives*  33 (2008), 211-232)

The problem of the second method is that it is very difficult to  "calculate" politically unacceptable losses. If the risk of terrorism is  defined in traditional terms by probability and potential loss, then  the focus on dramatic terror attacks leads to the marginalization of  probabilities. The reason is that even the highest degree of improbability becomes irrelevant as the measure of loss goes to infinity.^o  The mathematical calculation of the risk of terrorism thus tends to  overestimate and to dramatize the danger. This has consequences  beyond the actual risk assessment for the formulation and execution  of "risk policies": If one factor of the risk calculation approaches  infinity (e.g., if a case of nuclear terrorism is envisaged), then there  is no balanced measure for antiterrorist efforts, and risk management as a rational endeavor breaks down. Under the historical con-  dition of bipolarity, the "ultimate" threat with nuclear weapons could  be balanced by a similar counterthreat, and new equilibria could be  achieved, albeit on higher levels of nuclear overkill. Under the new  condition of uncertainty, no such rational balancing is possible since  knowledge about actors, their motives and capabilities, is largely  absent.  The second form of security policy that emerges when the deter-  rence model collapses mirrors the "social probability" approach. It  represents a logic of catastrophe. In contrast to risk management  framed in line with logical probability theory, the logic of catastro- phe does not attempt to provide means of absorbing uncertainty.  Rather, it takes uncertainty as constitutive for the logic itself; uncertainty is a crucial precondition for catastrophies. In particular, cata-  strophes happen at once, without a warning, but with major impli-  cations for the world polity. In this category, we find the impact of  meteorites. Mars attacks, the tsunami in South East Asia, and 9/11.  To conceive of terrorism as catastrophe has consequences for the  formulation of an adequate security policy. Since catastrophes hap-  pen irrespectively of human activity or inactivity, no political action  could possibly prevent them. Of course, there are precautions that  can be taken, but the framing of terrorist attack as a catastrophe  points to spatial and temporal characteristics that are beyond "ratio-  nality." Thus, political decision makers are exempted from the  responsibility to provide security—as long as they at least try to pre-  empt an attack. Interestingly enough, 9/11 was framed as catastro-  phe in various commissions dealing with the question of who was  responsible and whether it could have been prevented.  This makes clear that under the condition of uncertainty, there  are no objective criteria that could serve as an anchor for measur-  ing dangers and assessing the quality of political responses. For ex-  ample, as much as one might object to certain measures by the US  administration, it is almost impossible to "measure" the success of  countermeasures. Of course, there might be a subjective assessment  of specific shortcomings or failures, but there is no "common" cur-  rency to evaluate them. As a consequence, the framework of the  security dilemma fails to capture the basic uncertainties.  Pushing the door open for the security paradox, the main prob-  lem of security analysis then becomes the question how to integrate  dangers in risk assessments and security policies about which simply  nothing is known. In the mid 1990s, a Rand study entitled "New  Challenges for Defense Planning" addressed this issue arguing that  "most striking is the fact that we do not even know who or what will  constitute the most serious future threat, "^i In order to cope with  this challenge it would be essential, another Rand researcher wrote,  to break free from the "tyranny" of plausible scenario planning. The  decisive step would be to create "discontinuous scenarios ... in  which there is no plausible audit trail or storyline from current  events"52 These nonstandard scenarios were later called "wild cards"  and became important in the current US strategic discourse. They  justified the transformation from a threat-based toward a capability-  based defense planning strategy.53  The problem with this kind of risk assessment is, however, that  even the most absurd scenarios can gain plausibility. By construct-  ing a chain of potentialities, improbable events are linked and brought into the realm of the possible, if not even the probable.  "Although the likelihood of the scenario dwindles with each step,  the residual impression is one of plausibility. "54 This so-called Oth-  ello effect has been effective in the dawn of the recent war in Iraq.   The connection between Saddam Hussein and Al Qaeda that the  US government tried to prove was disputed from the very begin-  ning. False evidence was again and again presented and refuted,  but this did not prevent the administration from presenting as the  main rationale for war the improbable yet possible connection  between Iraq and the terrorist network and the improbable yet  possible proliferation of an improbable yet possible nuclear  weapon into the hands of Bin Laden. As Donald Rumsfeld  famously said: "Absence of evidence is not evidence of absence."  This sentence indicates that under the condition of genuine uncer-  tainty, different evidence criteria prevail than in situations where  security problems can be assessed with relative certainty.

#### **The alternative is to affirm the 1AC absent its apocalyptic representations - reject the 1AC to open space for a policy opposed to the security ideology of the status quo. Maintaining the threat logic of the 1AC results in endless war and an ever-expanding presidency.**

#### **Rana 2011** (Aziz, Assistant Professor of Law @ Cornell. “Responses to the Ten Questions.” William Mitchell Law Review, 37 Wm. Mitchell L. Rev. 5099)

The only way ultimately to produce lasting reform is to shift American political identity away from the national security frame shared by both the Bush and Obama administrations. In emphasizing the sense of permanent threat, this frame has not only generated an American polity continuously under arms, but it has also led to a global military footprint perhaps unparalleled in human history. As of 2009, some 516,273 military service members-not including Department of Defense civilian officials were deployed abroad, stationed across 716 reported overseas bases (the true number is likely over 1000), and present in approximatey 150 foreign states (nearly eighty percent of the world's countries). This worldwide military network is sustained by tremendous expenditures, which account for almost half of global defense spending-a number equal to the following twenty nations combined.48 Simply maintaining and protecting this global defense infrastructure has the inevitable consequence of strengthening executive power and promoting the further entrenchment of emergency rhetoric and rationales. Most troubling, in order to extend its footprint and international primacy, the United States finds itself engaging in practices that often actually promote, rather than inhibit, instability at the fringes of American power. The ever-present concern with national security means that policymakers view the United States as enjoying a right to act covertly or overtly in all parts of the world in order to quell presumed threats. Yet, in doing so, American actions have the tendency to produce their own backlashes, with the United States subject to local insurrections and new potential dangers. Rather than recognizing how the projection of American power itself participates in generating these crises, the talismanic logic of national security works to rationalize yet further territorial presence. This cycle of intervention, backlash, instability, and more intervention promotes a deep distortion in the actual meaning of local events-which oftentimes have little direct relation to American interests. It also serves as a continual justification for yet further constitutional flexibility and presidential prerogative, precisely because new dangers seem omnipresent. One clear consequence is that, as the local meaning of events disappears, the actual severity of foreign threats can often be greatly exaggerated. In 2009, only twenty-five United States civilians (sixteen at home and nine abroad) were killed in terrorist 49 attacks according to the State Department. While the fear of a terrorist attack is a legitimate concern, such numbers-which have been consistent in recent years-place the gravity of the threat in perspective and suggest the disconnect between the rhetoric of existential danger (one presumably comparable to Pearl Harbor) and the reality of relative security. Moreover, the persistent alteration of basic constitutional values to fit national security aims, regardless of objective consequences, for actual American physical safety, speaks to a profound imbalance in the United States's political priorities. It highlights just how entrenched Herring's old vision of security as pre-political (a lodestar around which to calibrate fundamental rights and collective interests) has become. Ultimately, the failure of the Obama administration to offer a meaningful legal correction is because at root the current administration-like its predecessor-remains committed to this vision of security and to the larger political framework produced by it. Thus, the question for Americans is whether there exists the public will to challenge the prevailing consensus, with its account of permanent threat and the need for a continuous projection of American power. Without such a will, there can be no substantive shift in our constitutional politics.

### Preemption

#### No US preemptive cyber-attack – policymakers default to conventional weapons

Dunlap ‘12

[Maj. Gen. Charles J. Dunlap Jr. (Ret.), Professor of the Practice of Law¶ Executive Director, Center on Law, Ethics and National Security @ Duke. In Patriot Debates: Contemporary Issues in National Security Law. <http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch9/ch9_ess2.html> ETB]

Of course, such decisions are never exclusively about legal matters. Policy makers and commanders rightly take into account a variety of factors beyond the law. In actual practice, it appears that such considerations often are more limiting than the law.¶ For example, the Washington Post reported that U.S. cyber weapons “had been considered to disrupt Gaddafi’s air defenses” early in NATO’s UN-sanctioned operations aimed at protecting Libyan civilians.33 However, the effort “was aborted,” the Post said, “when it became clear that there was not enough time for a cyber attack to work.” Conventional weapons, it was said, were “faster, and more potent,” a pure military rationale.¶ None of this reflects even the slightest suggestion that “lawyers” or the law frustrated the execution of a cyber operation in Libya.¶ No doubt there was discussion about cyber-reporting obligations under the War Powers Resolution, but Presidents have almost never seen that as a bar to military actions, so it can hardly be said to be something unique to cyber operations or that operated to actually block a cyber attack, per se. Rather, it is but one of the many political considerations applicable to military actions generally, cyber or otherwise.

#### Zero impact to cyber arms race --- overwhelming consensus of qualified authors goes neg

- No motivation---can’t be used for coercive leverage

- Defenses solve---benefits of offense are overstated

- Too difficult to execute/mistakes in code are inevitable

- AT: Infrastructure attacks

- Military networks are air-gapped/difficult to access

- Overwhelming consensus goes neg

Colin S. Gray 13, Prof. of International Politics and Strategic Studies @ the University of Reading and External Researcher @ the Strategic Studies Institute @ the U.S. Army War College, April, “Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling,” U.S. Army War College Press, <http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1147.pdf>

CONCLUSIONS AND RECOMMENDATIONS: THE SKY IS NOT FALLING¶ This analysis has sought to explore, identify, and explain the strategic meaning of cyber power. The organizing and thematic question that has shaped and driven the inquiry has been “So what?” Today we all do cyber, but this behavior usually has not been much informed by an understanding that reaches beyond the tactical and technical. I have endeavored to analyze in strategic terms what is on offer from the largely technical and tactical literature on cyber. What can or might be done and how to go about doing it are vitally important bodies of knowledge. But at least as important is understanding what cyber, as a fifth domain of warfare, brings to national security when it is considered strategically. Military history is stocked abundantly with examples of tactical behavior un - guided by any credible semblance of strategy. This inquiry has not been a campaign to reveal what cy ber can and might do; a large literature already exists that claims fairly convincingly to explain “how to . . .” But what does cyber power mean, and how does it fit strategically, if it does? These Conclusions and Rec ommendations offer some understanding of this fifth geography of war in terms that make sense to this strategist, at least. ¶ 1. Cyber can only be an enabler of physical effort. Stand-alone (popularly misnamed as “strategic”) cyber action is inherently grossly limited by its immateriality. The physicality of conflict with cyber’s human participants and mechanical artifacts has not been a passing phase in our species’ strategic history. Cyber action, quite independent of action on land, at sea, in the air, and in orbital space, certainly is possible. But the strategic logic of such behavior, keyed to anticipated success in tactical achievement, is not promising. To date, “What if . . .” speculation about strategic cyber attack usually is either contextually too light, or, more often, contextually unpersuasive. 49 However, this is not a great strategic truth, though it is a judgment advanced with considerable confidence. Although societies could, of course, be hurt by cyber action, it is important not to lose touch with the fact, in Libicki’s apposite words, that “[i]n the absence of physical combat, cyber war cannot lead to the occupation of territory. It is almost inconceivable that a sufficiently vigorous cyber war can overthrow the adversary’s government and replace it with a more pliable one.” 50 In the same way that the concepts of sea war, air war, and space war are fundamentally unsound, so also the idea of cyber war is unpersuasive. ¶ It is not impossible, but then, neither is war conducted only at sea, or in the air, or in space. On the one hand, cyber war may seem more probable than like environmentally independent action at sea or in the air. After all, cyber warfare would be very unlikely to harm human beings directly, let alone damage physically the machines on which they depend. These near-facts (cyber attack might cause socially critical machines to behave in a rogue manner with damaging physical consequences) might seem to ren - der cyber a safer zone of belligerent engagement than would physically violent action in other domains. But most likely there would be serious uncertainties pertaining to the consequences of cyber action, which must include the possibility of escalation into other domains of conflict. Despite popular assertions to the contrary, cyber is not likely to prove a precision weapon anytime soon. 51 In addition, assuming that the political and strategic contexts for cyber war were as serious as surely they would need to be to trigger events warranting plausible labeling as cyber war, the distinctly limited harm likely to follow from cyber assault would hardly appeal as prospectively effective coercive moves. On balance, it is most probable that cyber’s strategic future in war will be as a contribut - ing enabler of effectiveness of physical efforts in the other four geographies of conflict. Speculation about cyber war, defined strictly as hostile action by net - worked computers against networked computers, is hugely unconvincing.¶ 2. Cyber defense is difficult, but should be sufficiently effective. The structural advantages of the offense in cyber conflict are as obvious as they are easy to overstate. Penetration and exploitation, or even attack, would need to be by surprise. It can be swift almost beyond the imagination of those encultured by the traditional demands of physical combat. Cyber attack may be so stealthy that it escapes notice for a long while, or it might wreak digital havoc by com - plete surprise. And need one emphasize, that at least for a while, hostile cyber action is likely to be hard (though not quite impossible) to attribute with a cy - berized equivalent to a “smoking gun.” Once one is in the realm of the catastrophic “What if . . . ,” the world is indeed a frightening place. On a personal note, this defense analyst was for some years exposed to highly speculative briefings that hypothesized how unques - tionably cunning plans for nuclear attack could so promptly disable the United States as a functioning state that our nuclear retaliation would likely be still - born. I should hardly need to add that the briefers of these Scary Scenarios were obliged to make a series of Heroic Assumptions. ¶ The literature of cyber scare is more than mildly reminiscent of the nuclear attack stories with which I was assailed in the 1970s and 1980s. As one may observe regarding what Winston Churchill wrote of the disaster that was the Gallipoli campaign of 1915, “[t]he terrible ‘Ifs’ accumulate.” 52 Of course, there are dangers in the cyber domain. Not only are there cyber-competent competitors and enemies abroad; there are also Americans who make mistakes in cyber operation. Furthermore, there are the manufacturers and constructors of the physical artifacts behind (or in, depending upon the preferred definition) cyber - space who assuredly err in this and that detail. The more sophisticated—usually meaning complex—the code for cyber, the more certain must it be that mistakes both lurk in the program and will be made in digital communication.¶ What I have just outlined minimally is not a reluc - tant admission of the fallibility of cyber, but rather a statement of what is obvious and should be anticipat - ed about people and material in a domain of war. All human activities are more or less harassed by friction and carry with them some risk of failure, great or small. A strategist who has read Clausewitz, especially Book One of On War , 53 will know this. Alternatively, anyone who skims my summary version of the general theory of strategy will note that Dictum 14 states explicitly that “Strategy is more difficult to devise and execute than are policy, operations, and tactics: friction of all kinds comprise phenomena inseparable from the mak - ing and execution of strategies.” 54 Because of its often widely distributed character, the physical infrastruc - ture of an enemy’s cyber power is typically, though not invariably, an impracticable target set for physical assault. Happily, this probable fact should have only annoying consequences. The discretionary nature and therefore the variable possible characters feasible for friendly cyberspace(s), mean that the more danger - ous potential vulnerabilities that in theory could be the condition of our cyber-dependency ought to be avoidable at best, or bearable and survivable at worst. Libicki offers forthright advice on this aspect of the subject that deserves to be taken at face value: ¶ [T]here is no inherent reason that improving informa - tion technologies should lead to a rise in the amount of critical information in existence (for example, the names of every secret agent). Really critical information should never see a computer; if it sees a computer, it should not be one that is networked; and if the computer is networked, it should be air-gapped.¶ Cyber defense admittedly is difficult to do, but so is cyber offense. To quote Libicki yet again, “[i]n this medium [cyberspace] the best defense is not necessarily a good offense; it is usually a good defense.” 56 Unlike the geostrategic context for nuclear-framed competition in U.S.–Soviet/Russian rivalry, the geographical domain of cyberspace definitely is defensible. Even when the enemy is both clever and lucky, it will be our own design and operating fault if he is able to do more than disrupt and irritate us temporarily.¶ When cyber is contextually regarded properly— which means first, in particular, when it is viewed as but the latest military domain for defense planning—it should be plain to see that cyber performance needs to be good enough rather than perfect. 57 Our Landpower, sea power, air power, and prospectively our space systems also will have to be capable of accepting combat damage and loss, then recovering and carrying on. There is no fundamental reason that less should be demanded of our cyber power. Second, given that cyber is not of a nature or potential character at all likely to parallel nuclear dangers in the menace it could con - tain, we should anticipate international cyber rivalry to follow the competitive dynamic path already fol - lowed in the other domains in the past. Because the digital age is so young, the pace of technical change and tactical invention can be startling. However, the mechanization RMA of the 1920s and 1930s recorded reaction to the new science and technology of the time that is reminiscent of the cyber alarmism that has flour - ished of recent years. 58 We can be confident that cyber defense should be able to function well enough, given the strength of political, military, and commercial motivation for it to do so. The technical context here is a medium that is a constructed one, which provides air-gapping options for choice regarding the extent of networking. Naturally, a price is paid in convenience for some closing off of possible cyberspace(s), but all important defense decisions involve choice, so what is novel about that? There is nothing new about accepting some limitations on utility as a price worth paying for security.¶ 3. Intelligence is critically important, but informa - tion should not be overvalued. The strategic history of cyber over the past decade confirms what we could know already from the science and technology of this new domain for conflict. Specifically, cyber power is not technically forgiving of user error. Cyber warriors seeking criminal or military benefit require precise information if their intended exploits are to succeed. Lucky guesses should not stumble upon passwords, while efforts to disrupt electronic Supervisory Con - trol and Data Acquisition (SCADA) systems ought to be unable to achieve widespread harmful effects. But obviously there are practical limits to the air-gap op - tion, given that control (and command) systems need to be networks for communication. However, Internet connection needs to be treated as a potential source of serious danger.¶ It is one thing to be able to be an electronic nuisance, to annoy, disrupt, and perhaps delay. But it is quite another to be capable of inflicting real persisting harm on the fighting power of an enemy. Critically important military computer networks are, of course, accessible neither to the inspired amateur outsider, nor to the malignant political enemy. Easy passing reference to a hypothetical “cyber Pearl Harbor” reflects both poor history and ignorance of contemporary military common sense. Critical potential military (and other) targets for cyber attack are extremely hard to access and influence (I believe and certainly hope), and the technical knowledge, skills, and effort required to do serious harm to national security is forbiddingly high. This is not to claim, foolishly, that cyber means absolutely could not secure near-catastrophic results. However, it is to say that such a scenario is extremely improbable. Cyber defense is advancing all the time, as is cyber offense, of course. But so discretionary in vital detail can one be in the making of cyberspace, that confidence—real confidence—in cyber attack could not plausibly be high. It should be noted that I am confining this particular discussion to what rather idly tends to be called cyber war. In political and strategic practice, it is unlikely that war would or, more importantly, ever could be restricted to the EMS. Somewhat rhetorically, one should pose the question: Is it likely (almost anything, strictly, is possible) that cyber war with the potential to inflict catastrophic damage would be allowed to stand unsupported in and by action in the other four geographical domains of war? I believe not.¶ Because we have told ourselves that ours uniquely is the Information Age, we have become unduly respectful of the potency of this rather slippery catch-all term. As usual, it is helpful to contextualize the al - legedly magical ingredient, information, by locating it properly in strategic history as just one important element contributing to net strategic effectiveness. This mild caveat is supported usefully by recognizing the general contemporary rule that information per se harms nothing and nobody. The electrons in cyber - ized conflict have to be interpreted and acted upon by physical forces (including agency by physical human beings). As one might say, intelligence (alone) sinks no ship; only men and machines can sink ships! That said, there is no doubt that if friendly cyber action can infiltrate and misinform the electronic informa - tion on which advisory weaponry and other machines depend, considerable warfighting advantage could be gained. I do not intend to join Clausewitz in his dis - dain for intelligence, but I will argue that in strategic affairs, intelligence usually is somewhat uncertain. 59 Detailed up-to-date intelligence literally is essential for successful cyber offense, but it can be healthily sobering to appreciate that the strategic rewards of intelligence often are considerably exaggerated. The basic reason is not hard to recognize. Strategic success is a complex endeavor that requires adequate perfor - mances by many necessary contributors at every level of conflict (from the political to the tactical). ¶ When thoroughly reliable intelligence on the en - emy is in short supply, which usually is the case, the strategist finds ways to compensate as best he or she can. The IT-led RMA of the past 2 decades was fueled in part by the prospect of a quality of military effec - tiveness that was believed to flow from “dominant battle space knowledge,” to deploy a familiar con - cept. 60 While there is much to be said in praise of this idea, it is not unreasonable to ask why it has been that our ever-improving battle space knowledge has been compatible with so troubled a course of events in the 2000s in Iraq and Afghanistan. What we might have misunderstood is not the value of knowledge, or of the information from which knowledge is quarried, or even the merit in the IT that passed information and knowledge around. Instead, we may well have failed to grasp and grip understanding of the whole context of war and strategy for which battle space knowledge unquestionably is vital. One must say “vital” rather than strictly essential, because relatively ignorant armies can and have fought and won despite their ig - norance. History requires only that one’s net strategic performance is superior to that of the enemy. One is not required to be deeply well informed about the en - emy. It is historically quite commonplace for armies to fight in a condition of more-than-marginal reciprocal and strategic cultural ignorance. Intelligence is king in electronic warfare, but such warfare is unlikely to be solely, or even close to solely, sovereign in war and its warfare, considered overall as they should be.¶ 4. Why the sky will not fall. More accurately, one should say that the sky will not fall because of hostile action against us in cyberspace unless we are improb - ably careless and foolish. David J. Betz and Tim Ste vens strike the right note when they conclude that “[i]f cyberspace is not quite the hoped-for Garden of Eden, it is also not quite the pestilential swamp of the imagination of the cyber-alarmists.” 61 Our understanding of cyber is high at the technical and tactical level, but re - mains distinctly rudimentary as one ascends through operations to the more rarified altitudes of strategy and policy. Nonetheless, our scientific, technological, and tactical knowledge and understanding clearly indicates that the sky is not falling and is unlikely to fall in the future as a result of hostile cyber action. This analysis has weighed the more technical and tactical literature on cyber and concludes, not simply on balance, that cyber alarmism has little basis save in the imagination of the alarmists. There is military and civil peril in the hostile use of cyber, which is why we must take cyber security seriously, even to the point of buying redundant capabilities for a range of command and control systems. 62 So seriously should we regard cyber danger that it is only prudent to as - sume that we will be the target for hostile cyber action in future conflicts, and that some of that action will promote disruption and uncertainty in the damage it will cause.¶ That granted, this analysis recommends strongly that the U.S. Army, and indeed the whole of the U.S. Government, should strive to comprehend cyber in context. Approached in isolation as a new technol - ogy, it is not unduly hard to be over impressed with its potential both for good and harm. But if we see networked computing as just the latest RMA in an episodic succession of revolutionary changes in the way information is packaged and communicated, the computer-led IT revolution is set where it belongs, in historical context. In modern strategic history, there has been only one truly game-changing basket of tech - nologies, those pertaining to the creation and deliv - ery of nuclear weapons. Everything else has altered the tools with which conflict has been supported and waged, but has not changed the game. The nuclear revolution alone raised still-unanswered questions about the viability of interstate armed conflict. How - ever, it would be accurate to claim that since 1945, methods have been found to pursue fairly traditional political ends in ways that accommodate nonuse of nuclear means, notwithstanding the permanent pres - ence of those means.¶ The light cast by general strategic theory reveals what requires revealing strategically about networked computers. Once one sheds some of the sheer wonder at the seeming miracle of cyber’s ubiquity, instanta - neity, and (near) anonymity, one realizes that cyber is just another operational domain, though certainly one very different from the others in its nonphysi - cality in direct agency. Having placed cyber where it belongs, as a domain of war, next it is essential to recognize that its nonphysicality compels that cyber should be treated as an enabler of joint action, rather than as an agent of military action capable of behav - ing independently for useful coercive strategic effect. There are stand-alone possibilities for cyber action, but they are not convincing as attractive options either for or in opposition to a great power, let alone a superpower. No matter how intriguing the scenario design for cyber war strictly or for cyber warfare, the logic of grand and military strategy and a common sense fueled by understanding of the course of strategic history, require one so to contextualize cyber war that its independence is seen as too close to absurd to merit much concern.

**No impact- conventional deterrence solves and systems are quickly repaired**

**The Economist ‘12**

<http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may> ETB

Few would argue against improving resilience, particularly of **critical** national **infrastructure** such as power grids, sewerage and transport systems. But such targets **are not as vulnerable as is** now often **suggested**. Cyber-attacks on physical assets are most likely to use what Mr Libicki calls “one-shot weapons” aimed at industrial control systems. Stuxnet was an example: it destroyed perhaps a tenth of the Iranian centrifuges at Natanz and delayed some uranium enrichment for a few months, but the vulnerabilities it exposed were soon repaired. Its limited and fleeting success will also have led Iran to take measures to hinder future attacks. If that is the best that two first-rate cyber-powers can do against a third-rate industrial power, notes Mr Libicki, it puts into perspective the more alarmist predictions of impending cyber-attacks on infrastructure in the West.¶ Moreover, anyone contemplating a cyber-attack on physical infrastructure has little idea how much actual damage it will cause, and if people will die. They cannot know if they are crossing an adversary’s red line and in doing so would trigger a violent “kinetic” response (involving real weapons). Whether or not America has effective cyber-weapons, it has more than enough conventional ones to make any potential aggressor think twice.

### China

Sanger ev says the prob is that the US is conducting cy ops- no reason why consultation appeases the Chinese

#### No cyber war with China—interdependence checks

Austin and Gady 2012(Greg, professorial fellow at the EastWest Institute and senior visiting fellow in the department of War Studies at King’s College London, and Franz-Stefan, associate and foreign policy analyst at the EastWest Institute, "Cyber Detente Between the united States and China: Shaping the Agenda", http://www.ewi.info/system/files/detente.pdf)

That said, the two countries’ economies, though very different in many respects, are each highly dependent on a global Internet and shared communications platforms and hardware. While the Chinese economy is not as dependent on the Internet as the U.S., economy is, the difference between the two is fast shrinking. China’s export-driven economy and its trade in financial services make it as vulnerable to cyber attack as the United States. This interdependence—despite occasional outbursts of confrontational rhetoric coming from both Beijing and Washington— can be leveraged to promote stability in bilateral relations. In fact, this is already happening. We can think of this interdependency as a bal-ance of cyber power. If one accepts that both governments make rational calculations, than this new interconnectedness can be exploited to make conflict less likely. In today’s interconnected, digitalized world, the “opportunity cost” associated with embarking on a confrontational course will deter both parties from engaging in open hostile actions. This of course does not preclude cyber espionage, intellectual property theft, or even what some analysts have called the “long game,” i.e. the slow and gradual infiltration of strategically significant economic ICT systems by hackers on both sides.

#### No norm building – Russia and China won’t agree

Dawson ‘13

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

Conversely, some states, including Russia and China, have resisted these norms ¶ initiatives; citing cyberspace is a matter of national, their primary concern is regime ¶ control. Steven notes that in 2009 working through the Shanghai Cooperation ¶ Organization (SCO), alongside states such as Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan, Russia and China adopted an accord that defined “information war’” as the ¶ “dissemination of information harmful to social and political, social and economic ¶ systems, as well as spiritual, moral and cultural spheres of other States”.101 And in 2009, ¶ China, Russia, Tajikistan and Uzbekistan presented the UN general assembly with a new ¶ code of conduct for cyberspace, calling for international security. Framed in terms of ¶ “information security”, they proposed a variety reasonable measure of limiting the ¶ proliferation of cyber arsenals and prevention of cyber attack, but, notably, also proposed ¶ “information security’ included the need to protect against information dissemination that ¶ may endanger a states’ “political, economic and social stability, as well as their spiritual ¶ and cultural environment”.102 This incongruence between U.S. lead initiatives calling for norms of cooperation ¶ and non-liberal/non-democratic states, such as Russia and China, primarily focused on ¶ regime protection has created a major obstacle for broad adoption of norms in ¶ cyberspace. At a time where states are acting as the primary norm entrepreneurs, the ¶ inability to convince one another of divergent logics of appropriateness may prevent any ¶ broad recognition of common standards of behaviour in cyberspace. However, despite ¶ acute differences over governance issues, states do appear to recognize the need to ¶ prevent future limited-aims cyber attacks. It is possible, over time, states may settle on ¶ some agreed-upon norm able to address this going security concern. When, exactly what ¶ they will be, and how they will be enforced is the subject for further research.

#### No Taiwan war- any threats are just saber rattling and US deters

Vu Duc ‘13 "Khanh Vu Duc is a Vietnamese-Canadian lawyer who researches on Vietnamese politics, international relations and international law. He is a frequent contributor to Asia Sentinel and BBC Vietnamese Service, "Who's Bluffing Whom in the South China Sea?" www.asiasentinel.com/index.php?option=com\_content&task=view&id=5237&Itemid=171

Nevertheless, **it remains unlikely that any conflict** between China and Japan, Philippines, or Vietnam will **amount to more than saber rattling and harsh words.** Even a "small" police action against the Philippines or Vietnam over the Spratly Islands, however successful for China, would have severe consequences. Any Chinese use of force **would realize the fears of every state** in the region. Moreover, **Beijing's hope for a peaceful rise would be immediately set back, if not ruined**.

Presently, tensions are already running high; however, any clear displays of Chinese aggression would simply add fuel to the fire. Countries such as the Philippines and Vietnam would then be able to turn some of their neighbours—previously skeptical, if not cautious, about standing in opposition to China—and convince these states to protest openly. Any goodwill China possessed among some of these countries would evaporate as the Philippines and/or Vietnam make their case.

However, of all the scenarios of a conflict involving China, what can be certain is the potential for an immediate American intervention. While it is questionable that the US would directly intervene in any skirmish between nations, it is likely that Washington would use the conflict as an excuse for deploying a larger, if not more permanent, security force in Asia-Pacific. Although an increased American footprint would not be welcomed by all in the region, **the US would prove to be an appropriate balance against China.**

### Solvency

#### Oversight won’t restrict Presidential secrecy

Dycus 10

[“Congress’s Role in Cyber Warfare,” Stephen, Professor, Vermont Law School, Journal of National Security Law & Policy, http://jnslp.com/wp-content/uploads/2010/08/11\_Dycus.pdf]

Yet this legislation provides no guarantee that Congress will receive the information it needs to play a meaningful role in the development or execution of cyber warfare policy. It is not known, for example, precisely what it means for the intelligence committees to be “fully and currently” informed, what kinds of intelligence activities are regarded as “significant” enough to report, or who decides. 31 Other sections of the 1991 law call on all agencies involved in intelligence activities, not just the President, to keep the intelligence committees informed about those activities, but only “[t]o 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.” 32

#### Other agencies will still deploy OCOs

Sanger and Shanker 13

(David E. Sanger is chief Washington correspondent of The New York Times and Thom Shanker, Pentagon correspondent for The New York Times, 2/4/13, “Broad Powers Seen for Obama in Cyberstrikes”, http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?pagewanted=all&\_r=0, AB)

Cyberweaponry is the newest and perhaps most complex arms race under way. The Pentagon has created a new Cyber Command, and computer network warfare is one of the few parts of the military budget that is expected to grow. Officials said that the new cyberpolicies had been guided by a decade of evolution in counterterrorism policy, particularly on the division of authority between the military and the intelligence agencies in deploying cyberweapons. Officials spoke on condition of anonymity because they were not authorized to talk on the record.¶ Under current rules, the military can openly carry out counterterrorism missions in nations where the United States operates under the rules of war, like Afghanistan. But the intelligence agencies have the authority to carry out clandestine drone strikes and commando raids in places like Pakistan and Yemen, which are not declared war zones. The results have provoked wide protests.

#### The plan won’t compel any military reporting

Dycus 10

[“Congress’s Role in Cyber Warfare,” Stephen, Professor, Vermont Law School, Journal of National Security Law & Policy, http://jnslp.com/wp-content/uploads/2010/08/11\_Dycus.pdf]

The Defense Department is heavily engaged in preparations for cyber warfare, having recently announced the establishment of a new U.S. Cyber Command. 39 But congressional oversight of the work of this command could be hampered by the military’s reported practice of labeling its clandestine activities – those that are intended to be secret, but that can be publicly acknowledged if discovered or inadvertently revealed – as “operational preparation of the environment,” rather than intelligence activities, even though they may pose the same diplomatic and national security risks. 40 As thus characterized, these activities might not be reported to the intelligence committees. 41 Any oversight that occurred would be conducted instead by the House and Senate Armed Services Committees. 42 Such a division of responsibilities might create dangerous confusion. Congressional involvement also might be frustrated by the statutory exclusion of “traditional . . . military activities or routine support to such activities” from the definition of “covert action.” If secret military preparations for cyber war are regarded as “traditional military activities,” under the rationale outlined above they might escape both the presidential findings requirement for covert actions and any reporting to the intelligence committees.

#### The President would ignore the plan

Dycus 10

Stephen Dycus—1AC Author—10, Professor, Vermont Law School, 8/11/10, “Congress’s Role in Cyber Warfare,” <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>

Congress’s active role in the development and implementation of cyber warfare policy is no guarantee of national security. The policy might be flawed in various ways. There is also a risk that whatever policy is adopted will not be properly executed or that its execution will have unintended results. The policy might be misunderstood or might not provide clear or appropriate guidance in the urgent circumstances facing its interpreter. The person charged with implementing the policy might make a mistake – for example, by interpreting a potential enemy’s electronic espionage as an attack. Available cyber weaponry might not work as planned. Or a purely defensive move by U.S. operators might be construed by another nation as offensive, and provoke an attack. Nor can the clearest policy, statutory or executive, guarantee compliance by an Executive determined to ignore it.71 The rules might be construed by the President in a way that reduces the importance of Congress’s role. Or they might be challenged in court.

#### Congress will CHOOSE to ignore the statutory limit – other obligations

Miller 13

Vice President for New Initiatives and Distinguished Scholar at the Wilson Center

Aaron, Interviewing Marvin Kalb – Emeritus Professor @ Harvard, “They’re the Deciders,” http://www.foreignpolicy.com/articles/2013/05/31/president\_congress\_war\_power\_marvin\_kalb\_interview?utm\_source=feedly

FP: If Congress had to approve America's wars, would it make any difference?¶ MK: Not really -- not unless Congress set certain conditions for prosecuting the war, such as a time frame or a cost ceiling. Congress has approved of wars in the form of an approving resolution -- the invasion of Iraq in 2003, for example; but the president has the ultimate responsibility for setting policy for the war, conducting the war, and finding a way out of the war.¶ FP: Why has Congress acquiesced so much of the time?¶ MK: Because Congress does not want the responsibility for the costs of a war, measured in bodybags and budget shortfalls. Politicians are so encumbered these days by fundraising obligations, by party pressures and challenges, by the everyday responsibilities of the job that they are relieved to play a subordinate role to the executive in questions of war and peace.

# 2NC

## K

### AT Perm - Do Both

#### 3 – Religitizming - The aff’s legal approach only serves to normalize the state of exception – by creating a legal framework for the deployment of offensive cyberoperations, the affirmative legitimizes their ‘legal’ military use

Gregory 11. Derek Gregory, professor of geography at the University of British Columbia, “The Everywhere War,” he Geographical Journal, Vol. 177, No. 3, September 2011, pg. 246

The question is a good one, but it needs to be directed outwards as well as inwards. For the United States is also developing an offensive capacity in cyberspace, and the mission of CYBERCOM includes the requirement ‘to prepare to, and when directed conduct, full-spectrum military cyberspace opera- tions in order to enable actions in all domains’. This is a programmatic statement, and there are difficult con- ceptual, technical and operational issues to be resolved. The concept of the ‘cyber kill-chain’ has already made its appearance: software engineers at Lockheed Martin have identified seven phases or ‘border-crossings’ in cyberspace through which all advanced persistent intrusions must pass so that, con- versely, blocking an attack at any one of them (dislo- cating any link in the kill-chain) makes it possible ‘to turn asymmetric battle to the defender’s advantage’ (Croom 2011; Holcomb and Shrewsbury 2011). The issues involved are also ethical and legal. Debate has been joined about what constitutes an armed attack in cyberspace and how this might be legally codified (Dipert 2010; Nakashima 2010), and most of all about how to incorporate the protection of civilians into the conduct of cyber warfare. In the ‘borderless realm of cyberspace’ Hughes (2010, 536) notes that the boundary between military and civilian assets – and hence military and civilian targets – becomes blurred, which places still more pressure on the already stressed laws of armed conflict that impose a vital distinction between the two (Kelsey 2008). Pre- paring for offensive operations includes developing a pre-emptive precision-strike capacity, and this is – precisely – why Stuxnet is so suggestive and why Shakarian (2011) sees it as inaugurating ‘a revolution in military affairs in the virtual realm’. Far from ‘carpet bombing’ cyberspace, Gross (2011) describes Stuxnet as a ‘self-directed stealth drone’ that, like the Predator and the Reaper, is ‘the new face of twenty- first century warfare’. Cyber wars will be secret affairs, he predicts, waged by technicians ‘none of whom would ever have to look an enemy in the eye. For people whose lives are connected to the targets, the results could be as catastrophic as a bombing raid but would be even more disorienting. People would suffer, but [they] would never be certain whom to blame.’

Contrapuntal geographies

I have argued elsewhere that the American way of war has changed since 9/11, though not uniquely because of it (Gregory 2010), and there are crucial continuities as well as differences between the Bush and Obama administrations: ‘The man who many considered the peace candidate in the last election was transformed into the war president’ (Carter 2011, 4). This requires a careful telling, and I do not mean to reduce the three studies I have sketched here to a single interpretative narrative. Yet there are connections between them as well as contradictions, and I have indicated some of these en route. Others have noted them too. Pakistan’s President has remarked that the war in Afghanistan has grave consequences for his country ‘just as the Mexican drug war on US borders makes a difference to American society’, and one scholar has suggested that the United States draws legal authority to conduct military operations across the border from Afghanistan (including the killing of bin Laden, codenamed ‘Geronimo’) from its history of extra-territorial opera- tions against non-state actors in Mexico in the 1870s and 1880s (including the capture of the real Geronimo) (Margolies 2011). Whatever one makes of this, one of the most persistent threads connecting all three cases is the question of legality, which runs like a red ribbon throughout the prosecution of late modern war. On one side, commentators claim that new wars in the global South are ‘non-political’, intrinsically predatory criminal enterprises, that cartels are morphing into insurgencies, and that the origins of cyber warfare lie in the dark networks of cyber crime; on the other side, the United States places a premium on the rule and role of law in its new counterinsurgency doctrine, accentuates the involvement of legal advisers in targeting decisions by the USAF and the CIA, and even as it refuses to confirm its UAV strikes in Pakistan provides arguments for their legality.

The invocation of legality works to marginalise ethics and politics by making available a seemingly neutral, objective language: disagreement and debate then become purely technical issues that involve matters of opinion, certainly, but not values. The appeal to legality – and to the quasi-judicial process it invokes – thus helps to authorise a widespread and widening militarisation of our world. While I think it is both premature and excessive to see this as a transformation from governmentality to ‘militariality’ (Marzec 2009), I do believe that Foucault’s (2003) injunction – ‘Society must be defended’ – has been transformed into an unconditional imperative since 9/11 and that this involves an intensifying triangulation of the planet by legality, security and war. We might remember that biopolitics, one of the central projects of late modern war, requires a legal armature to authorise its interven- tions, and that necropolitics is not always outside the law. This triangulation has become such a common- place and provides such an established base-line for contemporary politics that I am reminded of an inter- view with Zizek soon after 9/11 – which for him marked the last war of the twentieth century – when he predicted that the ‘new wars’ of the twenty-first century would be distinguished by a radical uncertainty: ‘it will not even be clear whether it is a war or not’ (Deich- mann et al. 2002).

#### Double bind is stupid - we must choose between universalization of values or recognition of enmity

Moreiras 04

[Director of European Studies at Duke, Alberto, “A God without Sovereignty. Political Jouissance. The Passive Decision”, CR: The New Centennial Review 4.3, p. 79-80, Project MUSE]

The friend/enemy division is peculiar at the highest level, at the level of the order of the political. This peculiarity ultimately destroys the under- standing of the political as based on and circumscribed by the friend/enemy division. The idea of **an order of the political presupposes that the enemies of the order as such**—that is, the enemy configuration that can overthrow a given order, or even the very idea of an order of the political—**are generated from the inside**: enemies of the order are not properly external enemies. This is so **because the order of the political**, as a principle of division, as division itself, **always already** regulates, and thus **subsumes, its** externality: **externality is produced by the order** as such, and it is a function of the order. Or rather: a principle of division can have no externality. Beyond the order, there can be enemies, if attacked, but they are not necessarily enemies of the order: they are simply ignorant of it. At the highest level of the political, at the highest level of the friend/ enemy division, there where the very existence of a given order of the political is at stake, the order itself secretes its own enmity. Enmity does not precede the order: it is in every case produced by the order. **The friend/enemy division is** therefore a division that is **subordinate to the primary ordering division**, produced from itself. The friend/enemy division is therefore not supreme: **a nomic antithesis generates it**, **and** thus **stands above** it. The order of the political rules over politics. The political ontology implied inthe notion ofan order of the political deconstructs the **political** ontology ciphered in the friend/enemy division, and vice versa. They are mutually incompatible**. Either the friend/enemy division is supreme**, for a determination of the political, **or the order of the political is** supreme**. Both** of them **cannot simultaneously be supreme. The gap between them is** strictly **untheorizable.** If the friend/enemy division obtains independently of all the other antitheses as politically primary, then there is no order of the political. If there is an order of the political, the order produces its own political divisions.

### AT IR

#### The K qualitatively outweighs – we control the biggest internal link to macro-level violence - only our evidence is comparative about the scope and quality of violence in what our authors describe as “war”.

Prozorov 2K6

[Sergei, collegium fellow at the Helsinki Collegium for Advanced Studies, University of Helsinki, Professor of International Relations in the Department of International Relations, Faculty of Politics and Social Sciences, Petrozavodsk State University, Russia, 2006, “Liberal Enmity: The Figure of the Foe in the Political Ontology of Liberalism,” Millennium: Journal of International Studies, Vol. 35, No. 1, p. 75-99]

Schmitt makes a distinction between hostis and inimicus to stress the specificity of the relationship of a properly political enmity. The concept of inimicus belongs to the realm of the private and concerns various forms of moral, aesthetic or economic resentment, revulsion or hate that are connoted by the archaic English word ‘foe’, whose return into everyday circulation was taken by Schmitt as an example of the collapse of the political into the moral.31 In contrast, the concept of hostis is limited to the public realm and concerns the existential threat posed to the form of life of the community either from the inside or from the outside. In simple terms, the enemy (hostis) is what we confront, fight and seek to defeat in the public realm, to which it also belongs, while the foe (inimicus) is what we despise and seek either to transform into a more acceptable life-form or to annihilate. Contrary to Zizek’s attribution of the ‘ultra-politics of the foe’ to Schmitt, he persistently emphasised that the enemy conceptually need not and normatively should not be reduced to the foe: ‘The enemy in the political sense need not be hated personally.’32 In Schmitt’s argument, during the twentieth century such a reduction entailed the destruction of the symbolic framework of managing enmity on the basis of equality and the consequent absolutisation of enmity, i.e. the actualisation of the ‘most extreme possibility’: [Presently] the war is considered to constitute the absolute last war of humanity. Such a war is necessarily unusually intense and inhuman because, by transcending the limits of the political framework, it simultaneously degrades the enemy into moral and other categories and is forced to make of him a monster that must not only be defeated but also utterly destroyed. In other words, he is an enemy who no longer must be compelled to retreat into his borders only.33 Thus, it appears impossible to equate Schmitt’s notion of enmity with the friend–foe politics that was the object of his criticism. The very anti- essentialism, which Zizek’s reading recovers in Schmitt, brings into play a plurality of possible modalities of enmity. To argue, as Schmitt certainly does, that enmity is an ontological presupposition of any meaningful political relation, is certainly not to valorise any specific construction of the friend–enemy distinction. What is at stake is the need to distinguish clearly between what we have termed the transcendental function of the friend–enemy distinction (and in this aspect, Zizek’s own work on politics, particularly his recent ‘Leninist’ turn,34 remains resolutely Schmittian) and the empirical plurality of historical modalities of enmity. Schmitt’s philosophical achievement arguably consists in his affirmation of the irreducibility of the former function and the perils of its disavowal, an achievement that is not tarnished by a plausible criticism of his historical excursus on the Jus Publicum Europaeum as marked by a conservative nostalgia for a system that, after all, combined the sovereign equality of European powers with the manifestly asymmetric structure of colonial domination. At the same time, the objective of this article is not merely to correct manifold misreadings in the exegesis of a ‘properly Schmittian’ conception of enmity. Instead, we shall rely on Schmitt’s political realism and more contemporary philosophical orientations in deconstructing the present, actually existing ultra-politics of the foe, which has acquired a particular urgency in the current ascendancy of American neoconservative exceptionalism but is by no means reducible to it. Against the facile assumption of the unbridgeable gulf between the politics of the Bush administration and the remainder of the transatlantic community, we shall rather posit the ‘ultra-politics of the foe’ as the definitive feature of the transformation of the relation of enmity in Western politics in the twentieth century. Moreover, as our analysis below will demonstrate, the emergence of this ultra-politics is a direct effect of the universalisation of the liberal disposition rather than a resurgence of an ‘archaic’ form of political realism. What we observe presently is not a temporary ‘barbarian’ deviation from the progressive teleology of liberalism, but the fulfilment of Schmitt’s prophecy that liberalism produces its own form of barbarism.

#### The 1AC’s denial of enmity results in extinction

Schmitt ’63

(Carl. The Theory of the Partisan: A Commentary/Remark on the Theory of the Political. Trans. A. C. Goodson. East Lansing, MI: Michigan State University Press, 2004. 67.)

This means concretely that the supra-conventional weapon supposes¶ the supra-conventional man. It presupposes him not merely as a postulate¶ of some remote future; it intimates his existence as an already existent reality. The ultimate danger lies then not so much in the living presence of the¶ means of destruction and a premeditated meanness in man. It consists in¶ the inevitability of a moral compulsion. Men who turn these means against¶ others see themselves obliged/forced to annihilate their victims and¶ objects, even morally. They have to consider the other side as entirely criminal and inhuman, as totally worthless. Otherwise they are themselves¶ criminal and inhuman. The logic of value and its obverse, worthlessness,¶ unfolds its annihilating consequence, compelling ever new, ever deeper discriminations, criminalizations, and devaluations to the point of annihilating all of unworthy life [lebensunwerten Lebens]. In a world in which the partners push each other in this way into the¶ abyss of total devaluation before they annihilate one another physically,¶ new kinds of absolute enmity must come into being. Enmity will be so terrifying that one perhaps mustn’t even speak any longer of the enemy or of¶ enmity, and both words will have to be outlawed and damned fully before¶ the work of annihilation can begin. Annihilation thus becomes entirely¶ abstract and entirely absolute. It is no longer directed [96] against an¶ enemy, but serves only another, ostensibly objective attainment of highest¶ values, for which no price is too high to pay. It is the renunciation of real¶ enmity that opens the door for the work of annihilation of an absolute¶ enmity.

### AT Legal Restraints Work

#### That guarantees circumvention

Pollack, 13

MSU Guggenheim Fellow and professor of history emeritus [Norman, "Drones, Israel, and the Eclipse of Democracy," Counterpunch, 2-5-13, www.counterpunch.org/2013/02/05/drones-israel-and-the-eclipse-of-democracy/

Bisharat first addresses the transmogrification of international law by Israel’s military lawyers. We might call this damage control, were it not more serious. When the Palestinians first sought to join the I.C.C., and then, to receive the UN’s conferral of nonmember status on them, Israel raised fierce opposition. Why? He writes: “Israel’s frantic opposition to the elevation of Palestine’s status at the United Nations was motivated precisely by the fear that it would soon lead to I.C.C. jurisdiction over Palestinian claims of war crimes. Israeli leaders are unnerved for good reason. The I.C.C. could prosecute major international crimes committed on Palestinian soil anytime after the court’s founding on July 1, 2002.” In response to the threat, we see the deliberate reshaping of the law: Since 2000, “the Israel Defense Forces, guided by its military lawyers, have attempted to **remake the laws** of war by consciously violating them and then **creating new legal concepts to provide juridical cover** for their misdeeds.” (Italics, mine) In other words, habituate the law to the existence of atrocities; in the US‘s case, targeted assassination, repeated often enough, seems permissible, indeed clever and wise, as pressure is steadily applied to the laws of war. Even then, “collateral damage” is seen as unintentional, regrettable, but hardly prosecutable, and in the current atmosphere of complicity and desensitization, never a war crime. (**Obama is hardly a novice at** this game of **stretching the law to suit the convenience of**, shall we say, the **national interest**? In order to ensure the distortion in counting civilian casualties, which would bring the number down, as Brennan with a straight face claimed, was “zero,” the Big Lie if ever there was one, placing him in distinguished European company, Obama **redefined the meaning** of “combatant” status to be any male of military age throughout the area (which we) declared a combat zone, which noticeably led to a higher incidence of sadism, because it allowed for “second strikes” on funerals—the assumption that anyone attending must be a terrorist—and first responders, those who went to the aid of the wounded and dying, themselves also certainly terrorists because of their rescue attempts.) These guys play hardball, perhaps no more than in using—by report—the proverbial baseball cards to designate who would be next on the kill list. But funerals and first responders—verified by accredited witnesses–seems overly much, and not a murmur from an adoring public.

#### Their framing of emergencies guarantee the limitation fails

Vermeule 6

Adrian Vermeule, Professor of Law, Harvard Law School, 2006, “THE EMERGENCY CONSTITUTION IN THE POSTSEPTEMBER¶ 11 WORLD ORDER: SELF‐DEFEATING PROPOSALS: ACKERMAN ON EMERGENCY POWERS,” Fordham Law¶ Review, Nov., pp. LN.

A statute could, in principle, perform such constitutional functions by aligning the various parties' expectations about the¶ future, which then provide a basis for objecting to usurpations or interference when the emergency occurs. However,¶ history shows that statutory limitations are weak during emergencies. The War Powers Resolution , which limited the¶ circumstances under which the President could use military force and imposed various reporting requirements when the¶ President did use force, has been ignored. As I mentioned above, the National Emergencies Act similarly imposed¶ restrictions and reporting requirements on the President's power to declare emergencies, and the International Emergency¶ Economic Powers Act limited the President's power to impose economic sanctions during emergencies. None of these¶ statutes has had much of an impact on the behavior of executives. n61 Finally, after 9/11 the President undertook a¶ program of domestic warrantless surveillance, one that in the view of many commentators clearly violates the Foreign¶ Intelligence Surveillance Act. n62 Public opinion, however, is divided about the program's legality. n63 As of this writing,¶ there seems little prospect that Congress will retaliate; the most likely outcome is some sort of legislative ratification of the¶ program, which means that the President will have effectively annulled the Foreign Intelligence Surveillance Act as well as¶ the other framework statutes governing executive action in emergencies.”

## Solvency

### 2NC Congressional Oversight

#### Impossible to overcome executive information monopoly

Berman 10

Assistant professor @ Brooklyn Law School, Emily, “Executive Privilege Disputes between Congress and the President: A Legislative Proposal” *Albany Government Law Review*, Vol. 3, No. 741, 2010 [http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2112154] //mtc

2. Congress’s Inability to Overcome the Executive’s Monopoly on Information Creates Bias in Favor of Under-Disclosure¶ The second problem with the current system is that Congress’s tools are insufficient to overcome the Executive’s information monopoly. The fact that the Executive has exclusive control over information, which includes the related power to leak information selectively, provides the Executive with a structural advantage in information disputes that Congress’s tools are inadequate to overcome.¶ Consider first the central importance of the executive branch’s monopoly on information.75 With minor exceptions, Congress relies on the Executive for its information lifeblood. By definition, executive privilege conflicts can arise only when Congress has requested information from the Executive.76 As a consequence, inaction is response to an information request – i.e., when congress is unable to compel disclosure – necessarily confers victory on the Executive. The default result is nondisclosure. ¶ Next consider the related problem of selective disclosure by the Executive. As a consequence, inaction in response to an information request—i.e., when Congress is unable to compel disclosure—necessarily confers victory on the Executive. The default result is nondisclosure. 77 Selective release of information designed to cast the President or his policies in a favorable light while simultaneously withholding any damaging information or counterarguments manipulates public opinion, spinning any dispute over further disclosure in the Executive’s favor. A recent stark example is President Bush’s decision to declassify select portions of the National Intelligence Estimate on Iraq to provide support for going to war in 2003.78 This selective disclosure was designed to alter public perception and to bolster support for President Bush’s preferred policy. Though evidence later revealed that the Bush Administration had failed to disclose the full story, Congress could not contemporaneously rebut these selective disclosures. The Executive’s control over information thus provides a tool to perpetuate its monopoly by use of partial information to manipulate public opinion and stave off effective congressional inquiry.¶ Proponents of the current system assume that Congress can overcome these structural biases in favor of executive secrecy. To be sure, Congress does possess several political tools theoretically useful for obtaining information from the Executive: the power to investigate by committee; to appropriate (or withhold) funds; to withhold confirmation of appointed officials; to bring law suits; and, in extreme cases, to impeach.79 While all of these tools may be applied to attempt to compel the Executive to disclose information,80¶ First, all extract a significant toll in political capital, sometimes more than Congress possesses. each is problematic, either because it is ineffective or counterproductive.¶ First, all extract a significant toll in political capital, sometimes more than Congress possesses. Second, to exercise its powers, Congress must overcome the significant challenges to collective action that plague all legislative decision making. Given the drastic nature of some of Congress’s tools, those challenges prove insurmountable in all but the most extreme cases. ¶ Third, the disclosure or nondisclosure of some information can dramatically change the very political environment upon which the current system relies to resolve disputes. When Congress most needs information—because it possesses only hints of wrongdoing, error, or waste within the executive branch—is precisely when it lacks both political capital and incentive to compel disclosure. Yet if additional information reveals malfeasance, public support for Congress’s active pursuit of an investigation becomes considerably more intense. Until that information becomes public, Congress may lack sufficient support to maintain the political will necessary to pursue the issue. 84\\

## Preemption

# 1NR

## China

**US restraint does nothing --- norm setting is utopian**

James **Lewis 12**, Director of the Technology and Public Policy Program at the Center for Strategic and International Studies, “Benefits Are Great, and the Risks Exist Anyway,” Oct 17, NYT, http://www.nytimes.com/roomfordebate/2012/06/04/do-cyberattacks-on-iran-make-us-vulnerable-12/benefits-are-great-and-the-risks-exist-anyway

**Nor do cyberattacks against Iran increase the risk of damaging cyberattacks against the U**nited **S**tates. It is true that we are defenseless; efforts to make us safer are hamstrung by self-interest, ideology and the gridlock of American politics. But **we are no more vulnerable today than we were the day before the news. If someone decides to attack us, they may cite Iran as precedent, but it will only be to justify a decision they had already made.**¶ We could ask whether the United States creates more problems for itself when it makes public a new weapon while potential opponents keep it secret. **Four other countries can launch sophisticated and damaging cyber attacks** -- **including China and Russia** -- **and plan to use them in warfare**. Another **30 nations are acquiring cyber weapons**, including Iran and North Korea.¶ **There is a very old argument** for disarmament **that holds that if the U**nited **S**tates **were to renounce some weapons** -- usually nuclear weapons -- **the world would be a better place. This** **utopianism** **has a revered place in American political thinking, but when humans invent weapons they rarely give them up, especially useful weapons whose components are easy to acquire.** **Cyberattack is now part of warfare**, no different from any other weapon. The publicity around Stuxnet may complicate U.S. efforts to get international rules for the use of cyberattack, but the White House decided that tampering with Iran’s nuclear program was more important than possible risk to slow-moving negotiations.

**Cyber security frame undermines international coop - turns case**

**Friedman ‘11**

[Allan A. Friedman is ¶ research director of ¶ the Center for ¶ Technology Innovation ¶ at Brookings. He is ¶ also a fellow in ¶ Governance Studies.¶ <http://www.brookings.edu/~/media/research/files/papers/2011/7/21%20cybersecurity%20friedman/0721_cybersecurity_friedman.pdf> ETB]

**Disambiguating the nature of cybersecurity risk is key to building frameworks for**¶ **policies to address the real issues we face.** Framing the issue as a national security ¶ problem does have some advantages, of course. **National security solutions** come ¶ with national security budgets. On the other hand, they also **come** **with** other ¶ baggage of the national security apparatus: **large centralized bureaucracies, poor** ¶ **tradeoffs against economic benefits and civil liberties, and less consideration for** ¶ **the** (much larger) **civil side of cyberspace.** Moreover, cyberspace is not an ¶ American territory, and we **will require the cooperation and engagement of our** ¶ **allies and the broader international community to establish norms of acceptable** ¶ **behavior and jurisdictional authority. Other nations would be less likely to follow** ¶ **our lead if initiatives are framed as a question of American national security.**

### Link

**Turns the case -- Apocalyptic cyber rhetoric causes serial policy failure, resulting in MORE cyber insecurity.**

**Dunlap ‘13**

[Charles J. Dunlap, Jr. Major General, USAF (Ret.), Executive Director, Center on Law, Ethics, and National Security, Duke University School of Law. The Intersection of Law and Ethics in Cyberwar: Some Reflections. ETB]

The rule mentions **candor**. Again, this not something simply for attorneys, but¶ **is a fundamental ethical virtue for all defense professionals**.50 Among other ¶ things**, it is an important trait to keep in mind when assessing the potential** ¶ **threat that cyber represents. Misstating or**, worse, **deliberately** ¶ **misrepresenting the threat, can lead to poor allocations of resources and other** ¶ **errors in judgment.** Opinions about the scope and nature of the threat differ ¶ widely; in a PBS Newshour interview in the spring of 2012 Terry Benzel of the¶ Information Research Institute insists that “all of us in [the cyber] community, ¶ we talk about cyber-Pearl Harbor. And it's not if. It's when.”51 Likewise, a ¶ “leading European cybersecurity expert says international action is needed to ¶ prevent a catastrophic cyberwar and cyberterrorism.”52¶ Not all agree, however. In April of 2012 Rear Admiral Samuel Cox, director of ¶ intelligence at the U.S. Cyber Command, was reported as having “played down ¶ the prospect that an enemy of the U.S. could disable the nation's electric power ¶ grid or shut down the Internet, saying those systems are designed to withstand ¶ severe cyberattacks.”53 More stinging is a February 2012 Wired, article in ¶ which researchers Jerry Brito and Tate Watkins debunk much of the histrionic ¶ talk about the threat of cyberwar.54 According to Brito and Watkins, “**evidence** ¶ **to sustain such dire warnings [about cyberwar] is conspicuously absent;**.”55¶ Consistent with Brito and Watkins’ conclusions is a 2011 report by the ¶ Organization for Economic Cooperation and Development.56 While asserting ¶ that governments “need to make detailed preparations to withstand and ¶ recover from a wide range of unwanted cyber events, both accidental and ¶ deliberate,”57 the authors of that study nevertheless conclude “that very **few** ¶ single **cyber-related events have the capacity to cause a global shock**.”58¶ Writing in Foreign Policy analyst Thomas Rid contends that **cyberwar is “still** ¶ **more hype than hazard.”**59¶ All of this raises concerns because Brito and Watkins say that “[i]n many ¶ respects, **rhetoric about cyber catastrophe resemble the threat inflation we saw** ¶ **in the run-up to the Iraq War.**”60 They also point out that **“[c**]**ybersecurity is a** ¶ **big and booming industry” and** that “**Washington teems with people who have a** ¶ **vested interest in conflating and inflating threats to our digital security**.”61¶ Although they stop short of actually accusing anyone of pushing cyberwar fears ¶ for personal gain, **they** do **call for a “stop” in the “apocalyptic rhetoric” and** ¶ **insist that “alarmist scenarios dominating policy discourse may be good for the** ¶ **cybersecurity-industrial complex, but they aren’t doing real security any** ¶ **favors.”**62¶ The scope and immediacy of the threat is rightly debated, yet all might agree ¶ that, in any case, **deliberately overstating** (or understating**) the threat, even for** ¶ **the well-intentioned reasons of advocacy, can raise questions of ethics and** ¶ **professionalism**. As Brito and Watkins suggest, in **considering the run-up to** ¶ **the war with Iraq in 2003 it is clear what can happen when a threat is** ¶ **misconstrued,** which may be why they entitle their polemic “Cyberwar Is the ¶ New Yellowcake.” In short, candor – and tempered rhetoric if appropriate – are ¶ critical qualities for cyberwarriors. President **Obama’s** **measured language** ¶ **which urges people to take the cyber threat “seriously” and to make planning** ¶ **for it a “priority,” represents a responsible approach that highlights the dangers** ¶ **without falling victim to counterproductive and misleading hyping**.6

**The modern liberal state utilizes the threat of nuclear weapons to justify invasion in the interim to prevent catastrophe. Their representations are more likely to lead to preemption than passivity.**

**Massumi 07** (Brian, Communication Department of the Université de Montréal , “Potential Politics and the Primacy of Preemption”)

Fear is always a good reason to go politically conditional. **Fear** **is the palpable action in the present of a threatening future cause**. It acts just as palpably whether the threat is determinate or not. It weakens your resolve, creates stress, lowers consumer confidence, and may ultimately lead to individual and/or economic paralysis. **To avoid the paralysis**, which would make yourself even more of a target and carry the fear to even higher level, **you must simply act**. In Bush administration parlance, you "go kinetic."6 You leap into action on a level with the potential that frightens you. You do that, once again, by inciting the potential to take an actual shape you can respond to. You trigger a production of what you fear. **You turn the** objectively **indeterminate cause into an actual effect so you can actually deal with it in some way.** Any time you feel the need to act, then all you have to do is actuate a fear. The production of the effect follows as smoothly as a reflex. This affective dynamic is still very much in place, independent of Rumsfeld's individual fate. It will remain in place as long as fear and remains politically actuatable. **The logic of preemption operates on this** affective **plane**, in this proliferative or ontogenetic way: in a way that contributes to the reflex production of the specific being of the threat. **You're afraid Iraq is a breeding ground for terrorists? It could have been.** If it could have been, it would have been. **So go ahead, make it one**. "Bring 'em on," the President said, following Hollywood-trained reflex. He knew it in his "guts." He couldn't have gone wrong. His reflex was right. **Because "now we can all agree" that Iraq is in actual fact a breeding ground for "terrrorists". That just goes to prove that the potential was always there.** Before, there was doubt in some quarters that Saddam had to be removed from power. Some agreed he had to go, some didn't. Now we can all agree. It was right to remove him because doing so made Iraq become what it always could have been. And that's the truth. Truth, in this new world order, is by nature retroactive. Fact grows conditionally in the affective soil of an indeterminately present futurity. It becomes objective as that present reflexively plays out, as a effect of the preemptive action taken. The reality-based community wastes time studying empirical reality, the Bushites said: "we create it." And because of that, "we" the preemptors will always be right. We always will have been right to preempt, because we have objectively produced a recursive truth-effect for your judicious study. And while you are looking back studying the truth of it, we will have acted with reflex speed again, effecting a new reality. 7 We will always have had no choice but to prosecute the "war on terror," ever more vigilantly and ever more intensely on every potential front. We, preemptors, are the producers of your world. Get used to it. The War in Iraq is a success to the extent that it made the productivity of the preemptive "war on terror" a self-perpetuating movement. Even if the US were to withdraw from Iraq tomorrow, the war would have to continue on other fronts no matter who controls Congress or who is in the White House. It would have to continue in Afghanistan, for example, where the assymetrical tactics perfected in Iraq are now being applied to renew the conflict there. Or in Iran, which also always could have/would have been a terrorist breeding ground. Or it could morph and move to the Mexican-US border, itself morphed into a distributed frontline proliferating throughout the territory in the moving form of "illegal immigration". **On the indefinite Homeland Security front of** a protieform **war, who knows what threats may be spinelessly incubating** where, abetted by those who lack the "backbone" to go kinetic. **Preemption** is like deterrence in that it **combines a proprietary epistemology with a unique ontology in such a way as to make present a future cause that sets a self-perpetuating movement into operation**. Its differences from deterrence hinge on its taking objectively indeterminate or potential threat as its self-constitutive cause rather than fully formed and specified threat. It situates itself on the ground of ontogenetic potential. There, rather than deterring the feared effect, it actualizes the potential in a shape to which it hopes it can respond. It assumes a proliferation of potential threats, and mirrors that capacity in its own operation. It becomes proliferative. It assumes the objective imbalance of a far-from-equilibrium state as a permanent condition. Rather than trying to right the imbalance, it seizes it as an opportunity for itself. Preemption also sets a race in motion. But this is a race run on the edge of chaos. It is a race of movement-flushing, detection, perception, and affective actuation, run in irreparably chaotic or quasi-chaotic conditions. The race of preemption has any number of laps, each ending in the actual effecting of a threat. Each actualization of a threat triggers the next lap, as a continuation of the first in the same direction, or in another way in a different field. Deterrence revolved around an objective cause. Preemption revolves around a proliferative effect. Both are operative logics. The operative logic of deterrence, however, remained causal even as it displaced its cause's effect. **Preemption** is an effective operative logic rather than a causal operative logic. Since its ground is potential, there is no actual cause for it to organize itself around. It **compensates for the absence of an actual cause by producing an actual effect in its place**. This it makes the motor of its movement: it converts an absent or virtual cause really, directly into a taking-actual-effect. It does this affectively. It uses affect to effectively trigger a virtual causality.8 Preemption is when the futurity of unspecified threat is affectively held in the present in a perpetual state of potential emergence(y) so that a movement of actualization may be triggered that is not only self-propelling but also effectively, indefinitely, ontologically productive, because it works from a virtual cause whose potential no single actualization exhausts. Preemption's operational parameters mean that is never univocal. It operates in the element of vagueness and objective uncertainty. Due to its proliferative nature, it cannot be monolithic. Its logic cannot close in around its self-causing as the logic deterrence does. It includes an essential openness in its productive logic.9 It incites its adversary to take emergent form. It then strives to become as proteiform as its ever-emergent adversary can be. It is as shape-shifting as it is self-driving. It infiltrates across boundaries, sweeping up existing formations in its own transversal movement. Faced with gravity-bound formations too inertial for it to sweep up and carry off with its own operative logic, it contents itself with opening windows of opportunity to pass through. This is the case with the domestic legal and juridical structure in the US. It can't sweep that away. But it can build into that structure escape holes for itself. These take the form of formal provisions vastly expanding the power of the executive, in the person of the president in his role as commander-in-chief, to declare states of exception which suspend the normal legal course in order to enable a continued flow of preemptive action.10 **Preemption stands for conflict unlimited: the potential for peace amended to become a perpetual state of undeclared war.** This is the "permanent state of emergency" so presciently described by Walter Benjamin. In current Bush administration parlance, it has come to be called "Long War" replacing the Cold War: a preemptive war with an in-built tendency to be never-ending. Deterrence produced asymmetrical conflict as a by-product. The MADly balanced East-West bipolarity spun off a North-South sub-polarity. This was less a polarity than an axis of imbalance. The "South" was neither a second Western First nor another Eastern Second. It was an anomalous Third. In this chaotic " Third World ," local conflicts prefiguring the present "imbalance of terror" proliferated. The phrase "the war on terror" was in fact first popularized by Richard Nixon in 1972 in response to the attack at the Munich Olympics when the Israeli-Palestinian conflict spectacularly overspilled northward. Asymmetrical conflicts, however, were perceivable by the reigning logic of deterrence only as a reflection of itself. The dynamic of deterrence were overlaid upon them. Their heterogeneity was overcoded by the familiar US-Soviet duality. Globally such conflicts figured only as opportunities to reproduce the worldwide balance of terror on a reduced scale. The strategy of "containment" adopted toward them was for the two sides in the dominant dyad to operate in each local theater through proxies in such a way that their influence, on the whole, balanced out. "I decided," Nixon said after Munich , "that we must maintain a balance."11 He did not, as Bush did after 9-11, decide to skew things by going unilaterally "kinetic." The rhetoric of the "war on terror" fell into abeyance during the remainder of the 1970s, as Southern asymmetries tended to be overcoded as global rebalancings, and going kinetic was "contained" to the status of local anomaly.

### A2 Their Chit

**This is particularly true in the context of apocalyptic cyber war rhetoric**

**Stevens 2013** (Tim, Department of War Studies, King's College London; Centre for Science & Security Studies; International Centre for the Study of Radicalisation; "Apocalyptic Visions: Cyber War and the Politics of Time")

**Prophets who read and pronounce upon these apocalyptic signs**—the ‘Cassandras of cyber warfare’ (Rid, 2012: 6)—**do not**, like their religious counterparts, **restrict themselves to specific dates and times upon which terrible events will occur, so need not excuse themselves from incorrect predictions; consequently, they can never be wrong**. However, they do have in common talents as ‘masterful bricoleurs, skilfully recasting elements and themes within the constraints of their respective traditions and reconfiguring them to formulate new, meaningful endtimes scenarios’ (Wojcik, 1997: 148). **Specific vectors of ‘cyber insecurity’ may change, and timescales expand and contract, but the certainty in apocalypse remains unwavering**. ‘**Apocalyptic intensity’ is maintained and heightened further by making continued ‘imminent but indeterminate’ predictions, legitimising a constant state of readiness** in which adherents ‘feel themselves to be standing poised on the brink of time’ (Bromley, 1997: 36). In fact, it is always ‘only a matter of time’ before a ‘cyber-apocalypse’ occurs (Gable, 2010). **This uncertainty is shared with other forms of security, which thrive on a ‘denotative imprecision …. simultaneous appeal to the** hard and the vacuous, the **precise and the imprecise** …. vague generalities about everything and nothing’ (Walker, 1997: 63). This epistemic tension is partially resolved by reading the signs of cyber war as corroboration of a deterministic ‘script’ of the future (Robbins and Palmer, 1997: 5). **When events and scenarios converge, the narrative of cyber war gains explanatory power in its own right.** In periods of ‘thickened history’ like this, it becomes ever more difficult to comprehend these events—‘to see the wood for the trees’, as it were—and they become part of their own causal structure (Beissinger, 2002: 27). In this case, the impression is that if cyber war is not already occurring, it very soon will be.

### Weigh Case

**Empiricism is the standard for evaluating the 1AC risk assessment – the lack of a single** **historical example of wide-scale cyber warfare proves the 1AC impacts are colored too deeply by ideological fear of the unknown. The reality of cyber warfare is mundane and banal – attributing spectacle instigates cereal\* policy failure.**

\*captain crunch

**Lawson ‘11**

[Sean Lawson is an assistant professor in the Department of Communication at the University of Utah. His research focuses on the relationships among science, technology, and the development of military theory and discourse, in particular the intersections of national security and military thought with new media, information, and communication technologies. BEYOND CYBER-DOOM:

Cyberattack Scenarios and the Evidence of History. <http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf> ETB]

Seek Guidance from Empirical Research

**The formulation and evaluation of cybersecurity policy needs to be guided whenever** ¶ **possible by empirical research and rely less on hypothetical scenarios**. In **the case of early** ¶ **airpower theory, reliance upon unchallenged assumptions and hypothetical scenarios in the face** ¶ **of contradictory empirical evidence had disastrous results. By relying too heavily on** ¶ **hypothetical, cyber-doom scenarios, current cybersecurity planning is open to the same criticism** ¶ **that has been leveled against contemporary disaster planning, which is that it is “organized to** ¶ **deal with predicted vulnerabilities rather than to mobilize social capital to deal with actual** ¶ **threats**” (Dynes, 2006). Additionally, we should follow the recommendations of both James ¶ Lewis and Jeffrey Carr, who note **that while empirical research of a technical nature is crucial,** ¶ **the formulation and evaluation of cybersecurity policy requires knowledge of relevant “nontechnical” matters like the geopolitical, economic, legal, and other aspects of cybersecurity** (Carr, ¶ 2009; Lewis, 2009). One goal of this essay has been to demonstrate the value of research ¶ conducted in the humanities and social sciences, in particular the history of technology, military ¶ history, and disaster sociology, to the analysis of cyber-threats. Finally, **experts and policy**¶ **makers alike need to be critical and reflexive about cybersecurity claims, constantly asking if** ¶ **what they are saying or hearing is based on empirical evidence or merely the reflection of long- held anxieties about technology and recycled assumptions about infrastructural and social** ¶ **fragility**.¶