# 1NC

### 1

#### The executive branch of the United States should publish non-classified descriptions of the doctrine that governs cyber attacks.

#### Non binding transparency solves norm creation-restrictions will be manipulated by opponents to hamstring the US

**Metz, Army War College national security affairs professor, 2013**

(Steven, “Strategic Horizons: Transparency and American Security”, 6-26, <http://www.worldpoliticsreview.com/articles/13052/strategic-horizons-transparency-and-american-security>, ldg)

Two factors kept Americans from accepting government scrutiny as readily as during the Cold War. First, al-Qaida was not as dangerous as a Soviet Union armed with nuclear weapons, massive conventional forces and a global web of sympathizers and left-leaning organizations willing to give it a hand. Second was the coalescence of a transnational anti-authoritarian movement empowered by the intense connectivity of the Internet. Extremists in this movement believed that all information should be freed of government control and all government actions should be transparent to the public. While intellectually descended from the mistrust of government that inspired America's creators, transparency extremists did not understand what the Founding Fathers did: that if the virtue of government transparency and openness was pushed too far, it became a liability, potentially a dangerous one. In the latest twist, what had been a domestic American debate over transparency and openness is merging with global geopolitics. It is not a coincidence that the nations most interested in helping Snowden avoid arrest and sustain his access to the international media are precisely the ones, like China and Russia, that consider containment of the United States a core strategic objective. That repressive dictatorships should use the current U.S. debate over personal privacy and freedom against the United States borders on the absurd. For instance, the official news agency of North Korea—the most closed and repressive state on earth—wrote that Snowden’s disclosure of “such serious human rights abuses as massively gathering information by tapping phone messages and Internet usage of Americans . . . is clear evidence showing the true colors of the U.S. as a criminal state where human rights abuses are organized and legitimatized." While it is easy to dismiss North Korea's farcical rants, the involvement of China and Russia is both more important and more ominous. Being largely immune to domestic political criticism and having no qualms about invasive surveillance for the defense of their respective regimes, Beijing and Moscow are exploiting the extremist position on transparency and openness personified by Julian Assange and the other leaders of WikiLeaks, along with Manning and Snowden, as part of a broad, sophisticated and multifaceted strategy designed to weaken the United States. Just as the Soviets attempted to hijack legitimate organizations concerned with civil and labor rights during the Cold War—even though Soviet citizens had few rights of their own—the Russians and Chinese may increasingly try to use organizations focused on government openness and accountability both to hobble the ability of the U.S. government to collect security-related information and as a strategic distraction. However well-intentioned the transparency movement is, it risks becoming the tool of states with values antithetical to its own. As this issue unfolds in the coming years, it should be obvious that the extremist position—demanding that all government actions and programs should be public knowledge—is unrealistic. The Founding Fathers knew this and so too should 21st-century Americans. At the same time, simply trusting the government to collect and use information as it deems appropriate would be dangerous. The key is building a system that maximizes transparency and openness without giving a decisive advantage to America's enemies, whether pathological substate entities like al-Qaida or dictatorial states that are not quite enemies but certainly not friends.

### 2

#### Fast Track fight is on the top of the agenda-Strong push from Obama is key-Failure collapses global trade momentum

Good-Farm Policy-12/31/13

The FarmPolicy.com News Summary

HEADLINE: Farm Bill; Ag Economy; and, Biofuels- Tuesday

And with respect to trade, the Chicago Tribune editorial board[18] noted yesterday that, 'President Barack Obama wants the power to negotiate free-trade treaties on a fast track. With Trade Promotion Authority, he would have a good chance of clinching huge trade pacts now being hammered out with Europe and Asia. Yet Congress may not give him that authority — for all the wrong reasons.' The Tribune opinion item stated that, 'Within months the White House hopes to finish talks on a proposed Trans-Pacific Partnership with a group of Asia-Pacific nations. Talks with the European Union on the planned Transatlantic Trade and Investment Partnership are progressing too. Those deals would eliminate barriers and promote economic activity between the U.S. and key allies. The upside is huge: Billions of dollars in new business would be generated if these pacts come to pass. 'Yet given the special interests that oppose free trade, neither deal stands much of a chance in Congress without TPA. Consider farm tariffs, one of the most frustrating roadblocks to any free-trade pact with Europe or Asia. The agriculture lobby here and abroad has long succeeded in imposing some of the least competitive public policies of any industry. Although farm protectionism hurts the vast majority of the world's citizens, standing up to clout-heavy constituencies such as U.S. sugar magnates requires extraordinary political courage. TPA is essential for overcoming the inevitable fight against vested interests that are determined to advance themselves at the expense of the nation's good. 'Federal lawmakers and the president have to make their case with much more gusto than we have seen so far. Congress could OK a Trade Promotion Authority bill in the first few months of 2014. But that won't happen without leadership on Capitol Hill and, especially, from the White House. Now's the time.'

#### Congressional debate over the plan tanks agenda

Kriner, 10

(Douglas, Assistant professor of poly sci at Boston University, “After the

Rubicon: Congress, Presidents, and the Politics of Waging War”, University of Chicago Press, Dec

1, 2010)

While congressional support leaves the president’s reserve of political capital intact,¶ congressional criticism saps energy from other initiatives on the home front by forcing the¶ president to expend energy and effort defending his international agenda. Political capital¶ spent shoring up support for a president’s foreign policies is capital that is unavailable for his¶ future policy initiatives . Moreover, any weakening in the president’s political clout may have¶ immediate ramifications for his reelection prospects, as well as indirect consequences for congressional races.59¶ Indeed, Democratic efforts to tie congressional Republican incumbents to President George W. Bush and his war policies paid¶ immediate political dividends in the 2006 midterms, particularly in states, districts, and counties that had suffered the highest¶ casualty rates in the Iraq War. 60 In addition to boding ill for the president’s perceived political capital¶ and reputation, such partisan losses in Congress only further imperil his programmatic¶ agenda, both international and domestic. Scholars have long noted that President Lyndon¶ Johnson’s dream of a Great Society also perished in the rice paddies of Vietnam. Lacking the requisite¶ funds in a war-depleted treasury and the political capital needed to sustain his legislative vision, Johnson¶ gradually let his domestic goals slip away as he hunkered down in an effort first to win and¶ then to end the Vietnam War. In the same way, many of President Bush’s highest second-term¶ domestic proprieties, such as Social Security and immigration reform, failed perhaps in large part because¶ the administration had to expend so much energy and effort waging a rear-guard action¶ against congressional critics of the war in Iraq.61 When making their cost-benefit calculations,¶ presidents surely consider these wider political costs of congressional opposition to their¶ military policies. If congressional opposition in the military arena stands to derail other¶ elements of his agenda, all else being equal, the president will be more likely to judge the benefits¶ of military action insufficient to its costs than if Congress stood behind him in the¶ international arena.

#### Free trade prevents multiple scenarios for world war and WMD Terrorism

Panzner 2008

Michael, faculty at the New York Institute of Finance, 25-year veteran of the global stock, bond, and currency markets who has worked in New York and London for HSBC, Soros Funds, ABN Amro, Dresdner Bank, and JPMorgan Chase “Financial Armageddon: Protect Your Future from Economic Collapse,” pg. 136-138

Continuing calls for curbs on the flow of finance and trade will inspire the United States and other nations to spew forth protectionist legislation like the notorious Smoot-Hawley bill. Introduced at the start of the Great Depression, it triggered a series of tit-for-tat economic responses, which many commentators believe helped turn a serious economic downturn into a prolonged and devastating global disaster. But if history is any guide, those lessons will have been long forgotten during the next collapse. Eventually, fed by a mood of desperation and growing public anger, restrictions on trade, finance, investment, and immigration will almost certainly intensify. Authorities and ordinary citizens will likely scrutinize the cross-border movement of Americans and outsiders alike, and lawmakers may even call for a general crackdown on nonessential travel. Meanwhile, many nations will make transporting or sending funds to other countries exceedingly difficult. As desperate officials try to limit the fallout from decades of ill-conceived, corrupt, and reckless policies, they will introduce controls on foreign exchange. Foreign individuals and companies seeking to acquire certain American infrastructure assets, or trying to buy property and other assets on the cheap thanks to a rapidly depreciating dollar, will be stymied by limits on investment by noncitizens. Those efforts will cause spasms to ripple across economies and markets, disrupting global payment, settlement, and clearing mechanisms. All of this will, of course, continue to undermine business confidence and consumer spending. In a world of lockouts and lockdowns, any link that transmits systemic financial pressures across markets through arbitrage or portfolio-based risk management, or that allows diseases to be easily spread from one country to the next by tourists and wildlife, or that otherwise facilitates unwelcome exchanges of any kind will be viewed with suspicion and dealt with accordingly. The rise in isolationism and protectionism will bring about ever more heated arguments and dangerous confrontations over shared sources of oil, gas, and other key commodities as well as factors of production that must, out of necessity, be acquired from less-than-friendly nations. Whether involving raw materials used in strategic industries or basic necessities such as food, water, and energy, efforts to secure adequate supplies will take increasing precedence in a world where demand seems constantly out of kilter with supply. Disputes over the misuse, overuse, and pollution of the environment and natural resources will become more commonplace. Around the world, such tensions will give rise to full-scale military encounters, often with minimal provocation. In some instances, economic conditions will serve as a convenient pretext for conflicts that stem from cultural and religious differences. Alternatively, nations may look to divert attention away from domestic problems by channeling frustration and populist sentiment toward other countries and cultures. Enabled by cheap technology and the waning threat of American retribution, terrorist groups will likely boost the frequency and scale of their horrifying attacks, bringing the threat of random violence to a whole new level. Turbulent conditions will encourage aggressive saber rattling and interdictions by rogue nations running amok. Age-old clashes will also take on a new, more heated sense of urgency. China will likely assume an increasingly belligerent posture toward Taiwan, while Iran may embark on overt colonization of its neighbors in the Mideast. Israel, for its part, may look to draw a dwindling list of allies from around the world into a growing number of conflicts. Some observers, like John Mearsheimer, a political scientist at the University of Chicago, have even speculated that an “intense confrontation” between the United States and China is “inevitable” at some point. More than a few disputes will turn out to be almost wholly ideological. Growing cultural and religious differences will be transformed from wars of words to battles soaked in blood. Long-simmering resentments could also degenerate quickly, spurring the basest of human instincts and triggering genocidal acts. Terrorists employing biological or nuclear weapons will vie with conventional forces using jets, cruise missiles, and bunker-busting bombs to cause widespread destruction. Many will interpret stepped-up conflicts between Muslims and Western societies as the beginnings of a new world war.

### 3

#### A. Restrictions are prohibitions on action --- excludes conditions

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.

#### Plan isn’t a prohibition – doesn’t allow congress to say no to the president

#### B. Voting Issue---Precision—restrictions must be a distinct term for debate to occur

Heinze-Senior Lecturer Law, University of London-3

(Senior Lecturer in Law, University of London, Queen Mary. He has held fellowships from the Fulbright Foundation and the French and German governments. He teaches Legal Theory, Constitutional Law, Human Rights and Public International Law. JD Harvard) 2003 “The Logic of Liberal Rights A study in the formal analysis of legal discourse” http://mey.homelinux.org/companions/Eric%20Heinze/The%20Logic%20of%20Liberal%20Rights\_%20A%20Study%20in%20%20%28839%29/The%20Logic%20of%20Liberal%20Rights\_%20A%20Study%20in%20%20-%20Eric%20Heinze.pdf

Variety of ‘restrictions’

#### **The term ‘restriction’, defined so broadly, embraces any number of** familiar **concepts: ‘deprivation’, ‘denial’, ‘encroachment’, ‘incursion’, ‘infringement’, ‘interference’, ‘limitation’, ‘regulation’. Those terms commonly comport differences in meaning or nuance, and are not all interchangeable in standard legal usage**. For example, a ‘deprivation’ may be distinguished from a ‘limitation’ or ‘regulation’ in order to denote a full denial of a right (e.g. where private property is wholly appropriated by the state 16 Agents without compensation) as opposed to a partial constraint (e.g. where discrete restrictions are imposed on the use of property which nonetheless remains profitably usable). Similarly, **distinctions between acts and omissions can leave the blanket term ‘restriction’ sounding inapposite when applied to an omission: if a state is accused of not doing enough to give effect to a right, we would not colloquially refer to such inaction as a ‘restriction’**. Moreover, in a case of extreme abuse, such as extrajudicial killing or torture, **it might sound banal to speak merely of a ‘restriction’ on the corresponding right. However, the term ‘restriction’ will be used to include all of those circumstances**, in so far as they all comport a purpose or effect of extinguishing or diminishing the right-seeker’s enjoyment of an asserted right. (The only significant distinction which will be drawn will be between that concept of ‘restriction’ and the concept of ‘breach’ or ‘violation’. The terms ‘breach’ or ‘violation’ will be used to denote a judicial determination about the legality of the restriction.6) **Such an axiom may seem unwelcome, in so far as it obliterates subtleties which one would have thought to be useful in law**. It must be stressed that we are seeking to eliminate that variety of terms not for all purposes, but only for the very narrow purposes of a formal model, for which any distinctions among them are irrelevant.

### 4

#### **Technical solutions to war powers are a** shell game which locks in exceptionalism; the US is in no danger. The violence they recreate is a blind spot in the western mind which is exactly why we must ask prior to debate about the plan what our national security interests are who is served by those goals

Williams 7 (Daniel, associate professor of law at Northeastern University School of Law. He received a J.D. from Harvard, “NORTHEASTERN UNIVERSITY SCHOOL OF LAW.” NORTHEASTERN PUBLIC LAW AND THEORY FACULTY WORKING PAPERS SERIES

NO. 16-2007. http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=970279)

This fearsome sort of legality is largely shielded from our view (that is, from the view of Americans---the ones wielding this legality) with the veil of democracy, knitted together with the thread of process jurisprudence. Within process jurisprudence, there is no inquiry into the fundamental question: allocation of power between the branches to accomplish . . . what? It is very easy to skip that question, and thus easy to slide into or accept circular argumentation.31 With the focus on the distribution of power, arguments about what to do in this so-called war on terror start off with assumptions about the nature of the problem (crudely expressed as violent Jihadists who hate our freedoms) and then appeal to those assumptions to justify certain actions that have come to constitute this “war.” The grip of this circularity, ironically enough, gains its strength from the ideology of legality, the very thing that the Court seeks to protect in this narrative drama, because that ideology fences out considerations of history, sociology, politics, and much else that makes up the human experience. What Judith Shklar observed over forty years ago captures the point here: the “legalism” mindset--which thoroughly infuses the process jurisprudence that characterizes the Hamdi analysis--produces the “urge to draw a clear line between law and nonlaw” which, in turn, leads to “the construction of ever more refined and rigid systems of formal definitions” and thus “serve[s] to isolate law completely from the social context within which it exists.” 32 The pretense behind the process jurisprudence--and here pretense is purpose--is the resilient belief that law can be, and ought to be, impervious to ideological considerations. And so, the avoidance of the “accomplish . . . what?” question is far from accidental; it is the quintessential act of legality itself.33 More than that, this “deliberate isolation of the legal system . . . is itself a refined political ideology, the expression of a preference” that masquerades as a form of judicial neutrality we find suitable in a democracy.34 If the Executive’s asserted prerogative to prosecute a war in a way that will assure victory is confronted with the prior question about what exactly we want to accomplish in that war--if, that is, we confront the question posed by Slavoj Zizek, noted at the outset of this article—then the idea of national security trumping “law” takes on an entirely different analytical hue. Professor Owen Fiss is probably right when he says that the Justices in Hamdi “searched for ways to honor the Constitution without compromising national interests.”35 But that is a distinctly unsatisfying observation if what we are concerned about is the identification of what exactly those “national interests” are.36 We may not feel unsatisfied because, in the context of Hamdi, it undoubtedly seems pointless to ask what we are trying to accomplish, since the answer strikes us as obvious. We are in a deadly struggle to stamp out the terrorist threat posed by Al Qaeda, and more generally, terrorism arising from a certain violent and nihilistic strain of Islamic fundamentalism. Our foreign policy is expressly fueled by the outlook that preemptive attacks is not merely an option, but is the option to be used. In the words of the Bush Administration’s 2002 National Security Strategy document, “In the world we have entered, the only path to safety is the path of action. And this nation will act.”37 O’Connor and the rest of the Court members implicitly understand our foreign policy and the goal to be pursued in these terms, which explains why the Hamdi opinion nowhere raises a question about what it is the so-called “war on terror” seeks to accomplish. After all, the stories we want to tell dictate the stories that we do tell. We want to tell ourselves stories about our own essential goodness and benevolence, our own fidelity to the rule of law; and that desire dictates the juridical story that ultimately gets told. Once one posits that our foreign policy is purely and always defensive, as well as benevolent in motivation,38 then whatever the juridical story—even one where the nation’s highest Court announces that the Executive has no blank check to prosecute a war on terror—the underlying reality inscribed upon the world’s inhabitants, the consequences real people must absorb somehow, is one where “the United States has established that its only limit on the world stage will be its military power.”39 As O’Connor sees it, the real problem here is that, given that the allocation-of-power issue is tied to the goal of eliminating the terrorist threat, we have to reckon with the probability that this allocation is not just an emergency provision, but one that will be cemented into our society, since the current emergency is likely to be, in all practicality, a permanent emergency. But to say we are in a struggle to stamp out a terrorist threat posed by Islamic fundamentalism, and to say that “the only path to safety is the path of action,” conceals--renders invisible, a postmodernist would likely put it--an even more fundamental, and more radical, question: the allocation of power that the Court is called upon to establish is in the service of eliminating a terrorist threat to accomplish . . . what? The standard answer is, our security, which most Americans would take to mean, to avert an attack on our homeland, and thus, as it was with Lincoln, to preserve the Union. And so, we accept as obvious that our dilemma is finding the right security-liberty balance. The problem with that standard answer is two-fold. First, it glosses over the fact that we face no true existential threat, no enemy that genuinely threatens to seize control over our state apparatus and foist upon us a form of government to which we would not consent. That fact alone distinguishes our current war on terrorism from Lincoln’s quest to preserve the Union against secession.40 Second, this we-must-protect-the-Homeland answer is far too convenient as a conversation stopper. When the Bush Administration=’ National Security Strategy document avers that “the only path to safety is the path of action,” we ought to ask what global arrangements are contemplated through that “path of action.” When that document announces that “this nation will act,” it surely cannot suffice to say that the goal is merely eliminating a threat to attain security. All empires and empire-seeking nations engage in aggression under the rubric of self-defense and the deployment of noble-aims rhetoric. These justifications carry no genuine meaning but are devices of the powerful and the privileged, with the acquiescence and often encouragement by a frightened populace, to quell unsettling questions from dissenters within the society.41 Stop and think for a moment, how is it that the nation with the most formidable military might--the beneficiary of the hugest imbalance in military power ever in world history--is also the nation that professes to be the most imperiled by threats throughout the world, often threatened by impoverished peasant societies (Vietnam, Nicaragua, El Salvador, Chile, Granada, etc.)?42 An empire must always cast itself as vulnerable to attack and as constantly being under attack in order to justify its own military aggression. This is most acutely true when the empire is a democracy that must garner the consent of the populace, which explains why so much of governmental rhetoric concerning global affairs is alarmist in tone. The point is that quandaries over constitutional interpretation--ought we be prudential, or are other techniques more closely tied to the text the only legitimate mode of constitutional adjudication--may very well mask what may be the most urgent issue of all, which concerns what exactly this nation’s true identity is at this moment in world history, what it is that we are pursuing. Whereas Sanford Levinson has courageously argued that “too many people >venerate= the Constitution and use it as a kind of moral compass,”43 which leads to a certain blindness, I raise for consideration an idea that Hamdi suppresses, through its narrative techniques, which is that too many people “venerate” this nation without any genuine consideration of the particular way we have, since World War II, manifested ourselves as a nation. I join Levinson’s suspicion that our Constitution is venerated as an idea, as an abstraction, without much thought given to its particulars. It is important to be open to the possibility that the same is true with regard to our nation--the possibility that we venerate the idea of America (undoubtedly worth venerating), but remain (willfully?) ignorant of the particulars of our actual responsibility for the health of the planet and its inhabitants.44 To openly consider such issues is not anti-American--an utterly absurd locution--for to suggest that it is amounts to a denial that U.S. actions (as opposed to rhetoric that leeches off of the promise and ideal of “America”) can be measured by some yardstick of propriety that applies to all nations.45 The very idea of a “yardstick of propriety” requires a prior acceptance of two ideas: one, that we are part of something larger, that we are properly accountable to others and to that larger circumstance; and two, that it is not a betrayal or traitorous for a people within a nation to look within itself.46 Issacharoff and Pildes, the most prominent process theorists, observe that process jurisprudence may be inadequate to address the risk that we “might succumb to wartime hysteria.”47 I would broaden that observation so as to be open to the possibility that the risk goes beyond just wartime hysteria, that our desire for security and military victory, rooted in our repudiation of a genuine universal yardstick of propriety that we willingly apply to ourselves (often called American exceptionalism48)--which means that security and military victory are not ipso facto the same thing--could easily slide us into sanctioning a form of sovereignty that is dangerously outmoded and far out of proportion to what circumstances warrant. Process jurisprudence supposedly has the merit of putting the balance of security and liberty into the hands of the democratic institutions of our government. But what it cannot bring into the field of vision--and what is absolutely banished from view in Hamdi--is the possibility that the democratic institutions themselves, and perhaps even the democratic culture generally, the public sphere of that culture, have been corrupted so severely as to reduce process jurisprudence to a shell game.49 More specifically, the formal processes of governmentality responding to crisis is judicially monitored, but the mythos of our national identity, particularly the idea that every international crisis boils down to the unquestioned fact that the United States at least endeavors to act solely in self defense and to promote some benevolent goal that the entire world ought to stand behind, is manufactured and thus some hegemonic pursuit in this global “war on terror” remains not just juridically ignored, but muted and marginalized in much of our public discussions about it.50 Under process jurisprudence, it is the wording of a piece of legislation, not the decoding of the slogan national security, that ultimately matters. And under process jurisprudence, fundamental decisions have already been made--fundamental decisions concerning the nature of our global ambitions and the way we will pursue them--before the judiciary can confront the so-called security-liberty balance, which means that the analytical deck has been stacked by the time the justiciable question---that is, what we regard as the justiciable question---is posed. Stacking the analytical deck in this way reduces the Court members to the role of technicians in the service of whatever pursuit the sovereign happens to choose.51 This is why it is worth asking what many might regard as a naive, if not tendentious, question: is it true that in the case of Hamdi and other post-9/11 cases, the judiciary’s quandary over allocation of power is actually in the service of genuine security, meaning physical safety of the populace? Does the seemingly obvious answer that we seek only to protect the safety of our communities against naked violence blind us to a deeper ailment within our culture? Is it possible that the allocation of power, at bottom, is rooted in a dark side of our Enlightenment heritage, an impulse within Legality that threatens us in a way similar to the Thanatos drive Freud identified as creating civilization’s discontent?52 Perhaps Hamdi itself, as a cultural document, signals yet another capitulation to the impulse to embrace a form of means-ends rationality that supports the Enlightenment drive to control and subdue.53 Perhaps what Hamdi shows is that 9/11 has not really triggered a need to recalibrate the security-liberty balance, but has actually unleashed that which has already filtered into and corrupted our culture—Enlightenment’s dark side, as the Frankfurt School understood it54’’and is thus one among many cultural documents that ought to tell us we are not averting a new dark age, but are already in it, or at least, to borrow a phrase from Wendell Berry, that we are “leapfrogging into the dark.” 55 It is impossible, without the benefit of historical distance, to answer these questions with what amounts to comforting certitude. But they are worth confronting, since the fate of so many people depends on it, given our unrivaled ability and frightening willingness to use military force. Our culture’s inability to ask such questions in any meaningful way, as opposed to marginalizing those who plead for them to be confronted, is somewhat reminiscent of how early Enlightenment culture treated scientific endeavors. “Science,” during the rise of Enlightenment culture, rebuffed the why question, banished it as a remnant of medieval darkness, because the why-ness of a certain scientific pursuit suggested that certain domains of knowledge were bad, off-limits, taboo. The whole cultural mindset of the Enlightenment was to jettison precisely such a suggestion. That cultural mindset produced a faith all its own, that all scientific pursuits, and by extension all human quests for knowledge, will in the end promote human flourishing. It has taken the devastation of our planet to reveal the folly of that faith, a blind-spot in the Western mind. It may turn out, as a sort of silver lining on a dark cloud, that the terrorism arising from Islamic jihadists may do something similar.

#### **Vote negative; daring to imagine a political alternative to fear is key to change the technical legalistic frame that creates the conditions for violence**

Ben-Asher 10 (NOA BEN-ASHER is a Assistant Professor of Law, Pace Law School, “Legalism and Decisionism in Crisis ,” http://moritzlaw.osu.edu/lawjournal/issues/volume71/number4/ben-asher.pdf)

“I am grateful for your hospitality and the hospitality of the people of Egypt”—thus begins President Obama’s address to the Muslim world in Cairo in June of 2009.300 Throughout this speech the President reaches out to Islam with rhetoric of gratitude, hospitality, and peace. He urges Muslims and non-Muslims to “have the courage to make a new beginning, keeping in mind what has been written.”301 And what has been written? Obama then quotes the Talmud—“The whole of the Torah is for the purpose of promoting peace”—302 and the New Testament—“Blessed are the peacemakers, for they shall be called sons of God.”303 Interestingly, though, he first quotes a passage from the Koran that, by contrast, does not mention peace: “O mankind! We have created you male and female and we have made you into nations and tribes so that you may know one another.” 304 Here, mankind has been divided into nations not for war or peace or prosperity or progress, but for one purpose: “so that you may know one another.” Knowledge of the other person and nation is the sole purpose of the separation of mankind into nations—says the Koran text that closes Obama’s speech. This was our definition of hospitality: conscious listening to the other, welcoming the face of the other, and occupying a relation of deference to the other. Perhaps Obama’s concluding words may help us understand what deference to the other might mean in this context—“It’s a faith in other people, and it’s what brought me here today.”305 This rhetoric of friendship, hospitality, and responsibility towards Islam is different from the strictly legalistic rhetoric of religious liberty pursued elsewhere by the President and by others. Such rhetoric is important, especially in times of hostilities, because it dares to imagine a political and legal alternative to fear, vulnerability, and enmity. Vice President Dick Cheney declared shortly after September 11, 2001, that we should consider the current period not an emergency at all, but “the new normalcy.”306 Necessity, enmity, and catastrophe have indeed become the normal politics shared by many Legalists and Decisionists in emergency powers debates. Legalist and Decisionist disagreements often turn on the balance of powers and the proper role of law in the “war on terror.” Should the primary tools for fighting terror be norms or decisions? Legalists have argued for the former and Decisionists for the latter. Legalists have argued that the rule of law must survive at all times. Decisionists have insisted that the key to the nation’s survival is a strong, decisive executive branch that is sometimes unbound by legal norms. But despite these disagreements, many versions of Decisionism and Legalism have conceded that the state of emergency has indeed become “the new normalcy.” This Article argues that we should develop an alternative vision of the human and the state as they exist in times of crisis.

### Preemption

#### Low risk of cyberwar-too hard to take down multiple targets and keep them down. Only 3 percent of attacks are actually scary.

**Cavelty, Center for Security Studies, 2012**

(Myriam Dunn, “The Militarisation of Cyber Security as a Source of Global Tension”, 10-22, <http://isn.ch/Digital-Library/Articles/Special-Feature/Detail/?lng=en&id=153888&tabid=1453350669&contextid774=153888&contextid775=153903>, ldg)

However, in the entire history of computer networks, there are no examples of cyber attacks that resulted in actual physical violence against persons (nobody has ever died from a cyber incident), and only very few had a substantial effect on property (Stuxnet being the most prominent). So far, cyber attacks have not caused serious long-term disruptions. They are risks that can be dealt with by individual entities using standard information security measures, and their overall costs remain low in comparison to other risk categories such as financial risks. These facts tend to be almost completely disregarded in policy circles. There are several reasons why the threat is overrated. First, as combating cyber threats has become a highly politicised issue, official statements about the level of threat must also be seen in the context of competition for resources and influence between various bureaucratic entities. This is usually done by stating an urgent need for action and describing the overall threat as big and rising. Second, psychological research has shown that risk perception, including the perception of experts, is highly dependent on intuition and emotions. Cyber risks, especially in their more extreme form, fit the risk profile of so-called ‘dread risks’, which are perceived as catastrophic, fatal, un- known, and basically uncontrollable. There is a propensity to be disproportionally afraid of these risks despite their low probability, which translates into pressure for regulatory action of all sorts and the willingness to bear high costs of uncertain benefit Third, the media distorts the threat perception even further. There is no hard data for the assumption that the level of cyber risks is actually rising– beyond the perception of impact and fear. Some IT security companies have recently warned against over-emphasising sophisticated attacks just because we hear more about them. In 2010, only about 3 per cent of all incidents were considered so sophisticated that they were impossible to stop. The vast majority of attackers go after low-hanging fruit, which are small to medium sized enterprises with bad defences. These types of incidents tend to remain under the radar of the media and even law enforcement. Cyber war remains unlikely Since the potentially devastating effects of cyber attacks are so scary, the temptation is very high not only to think about worst-case scenarios, but also to give them a lot of (often too much) weight despite their very low probability. However, most experts agree that strategic cyber war remains highly unlikely in the foreseeable future, mainly due to the uncertain results such a war would bring, the lack of motivation on the part of the possible combatants, and their shared inability to defend against counterattacks. Indeed, it is hard to see how cyber attacks could ever become truly effective for military purposes: It is exceptionally difficult to take down multiple, specific targets and keep them down over time. The key difficulty is proper reconnaissance and targeting, as well as the need to deal with a variety of diverse systems and be ready for countermoves from your adversary. Furthermore, nobody can be truly interested in allowing the unfettered proliferation and use of cyber war tools, least of all the countries with the offensive lead in this domain. Quite to the contrary, strong arguments can be made that the world’s big powers have an overall strategic interest in developing and accepting internationally agreed norms on cyber war, and in creating agreements that might pertain to the development, distribution, and deployment of cyber weapons or to their use (though the effectiveness of such norms must remain doubtful). The most obvious reason is that the countries that are currently openly discussing the use of cyber war tools are precisely the ones that are the most vulnerable to cyber warfare attacks due to their high dependency on information infrastructure. The features of the emerging information environment make it extremely unlikely that any but the most limited and tactically oriented instances of computer attacks could be contained. More likely, computer attacks could ‘blow back’ through the interdependencies that are such an essential feature of the environment. Even relatively harmless viruses and worms would cause considerable random disruption to businesses, governments, and consumers. This risk would most likely weigh much heavier than the uncertain benefits to be gained from cyber war activities. Certainly, thinking about (and planning for) worst-case scenarios is a legitimate task of the national security apparatus. Also, it seems almost inevitable that until cyber war is proven to be ineffective or forbidden, states and non-state actors who have the ability to develop cyber weapons will try to do so, because they appear cost-effective, more stealthy, and less risky than other forms of armed conflict. However, cyber war should not receive too much attention at the expense of more plausible and possible cyber problems. Using too many resources for high- impact, low-probability events – and therefore having less resources for the low to middle impact and high probability events – does not make sense, neither politically, nor strategically and certainly not when applying a cost-benefit logic.

#### Flex is key in cyberspace-no margin for error

**Cilluffo, George Washington University Homeland Security Policy Institute director, 2013**

(Frank, “A Blueprint for Cyber Deterrence: Building Stability through Strength”, 5-6, <http://defense-update.com/20130506_a-blueprint-for-cyber-deterrence-building-stability-through-strength.html>, ldg)

It is sometimes said that the best defense is a good offense. According to open source reports, the United States is developing rules of engagement regarding cyber attacks, and the Defense Department is seeking to bolster its arsenal of cyber weapons (though a cyber attack may engender a cyber or kinetic response). As former Vice Chairman of the Joint Chiefs of Staff General James E. Cartwright has observed, efforts and investments of the type just described would help recalibrate the defense to offense ratio – which until relatively recently stood at 90 percent to 10 percent in favor of defense – and would strengthen and build credence in the US ability to deter effectively adverse action in the cyber domain. However, the US cyber security community, like its allied counterparts, remains a work in progress. In the US in particular, the community still has a long way to go before it reaches the level of skill and maturity now displayed by the US counterterrorism community. The synchronization of Titles 10 and 50 of the United States Code, harmonizing military and intelligence functions, has been a major post-9/11 breakthrough that signiﬁcantly enhanced the US overall counterterrorism posture. The US can leverage this achievement by tailoring and applying the concept to the cyber context, bearing in mind the (yet-to-be-met) twin challenges of codifying rules of engagement and pursuing a more proactive stance. To move forward smartly in the cyber domain, the United States and its allies must demonstrate leadership and possess vision, together with a sound plan of action. For too long, incidents have driven strategy – in effect, tactics masquerading as strategy. While the United States possesses some unique capabilities, these capabilities will not be used to fullest advantage unless and until there is a broader strategic framework in which to embed them. Building on the conceptual framework set out above, certain key tenets emerge that can serve as a foundation for developing and enacting an effective cyber deterrence strategy, capacity, and posture. Those tenets, the beginnings of a blueprint for cyber deterrence, are as follows: Calibrate to meet the mission. Capability supports credibility in this context. To the extent that investments and efforts may reﬂect a defense to offense ratio that suggests an imbalance that could negatively impact on homeland/national security, the existing calibration should be considered carefully and adjusted as necessary. As a prerequisite to imposing consequences, calibration (or recalibration) goes hand in hand with the political will to act, when called upon, to impose sanctions. Start and build from a position of strength. To deter or dissuade successfully requires the capacity to convince potential adversaries that the costs of hostile action will exceed the perceived beneﬁts. Developing and signaling the existence of a ﬁrst strike capability is therefore fundamental. Put the accent on speed, surprise, and maneuverability. Nanoseconds can make a difference in cyberspace. Response in close to real time should therefore be the goal. While there should be no doubt about the principle that any breach of red lines will incur consequences, there is value in maintaining a measure of ambiguity about the precise nature of those consequences, so as to keep the object looking constantly over its shoulder. Flexibility plus clarity may seem a non sequitur, but in fact is strategically prudent here.

#### Opponents have no incentive for restraint-only in a world of threating US capabilities can reciprocal agreements happen.

**Goldsmith, Harvard law professor, 2013**

(Jack, “Cybersecurity Treaties A Skeptical View”, <http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf>, ldg)One response to this argument is that even with these clashes of interests, there are still opportunities for agreement to secure the basic infrastructure of the Internet on which all nations depend and from which they all benefit. For example, C&K propose to ban cyber attacks on banks.12 The United States does not attack banks and thus would lose nothing from promising not to do so. And perhaps other nations also have no interest in attacking (as opposed to stealing from) banks, because all nations would lose a lot if the international banking system went down. So perhaps nations’ interests align in the protection of certain discrete infrastructures. And perhaps this natural conversion of interests could be concretized and strengthened by an international agreement. Even here, though, the supposed alliance of interests is misleading. Set aside the significant verification problems, and just focus on China’s interests. China is committed to the deployment of malicious agents inside our critical infrastructure (including banking systems) to make up for its relative weakness in traditional military capabilities in the event of a hot war.13 Combining this consideration with its relatively powerful control over its own critical infrastructures, China might think itself relatively better off, vis a vis the United States, by not giving up cyber threats against civilian infrastructures, including banking. Similarly, Iran or North Korea might want to maintain the threat of shutting down our electricity grid—even if doing so heightened the vulnerability of its own grid. These points become even stronger when one considers that our adversaries might think, based on credible public sources, that the United States is deeply self-constrained in its use of cyber weapons by its interpretation of the laws of war, the Title 10 v. 50 debate, and other legal factors. Because the threat of U.S. cyber attack is already weak, at least short of a hot war, our adversaries might think they gain relatively little from a cybersecurity agreement to refrain from using offensive weapons. This consideration is probably only heightened by the United States’ sudden and seemingly panicked rush of interest in international treaties. The general point here is that even if every nation would to some degree benefit from protection of interconnected computer and communication infrastructures, those potential benefits by themselves do not necessarily imply that there is space for cooperative agreement. The distributional consequences of any such agreement may be such that some nations will be willing to risk the threats to infrastructures from non-cooperation because the threats fall asymmetrically on their adversaries. This relative-gains problem is a frequent hurdle to arms control and security agreements.14 It is also a frequent hurdle to international agreements about the regulation of telecommunications technology that relates to national security.15 It has special salience in the cybsersecurity context, because the United States, as explained above, is asymmetrically vulnerable to cyber attack. The fundamental clash of interests will also matter in a different way. Assume for the moment that every nation in the world would benefit from a ban on certain forms of cyber attack and that every nation can perfectly monitor every other’s compliance with a cybersecurity treaty. It does not follow that nations will cooperate. An important prerequisite to cooperation is that nations must agree on what counts as cooperation. For example, if two nations agree simply to not engage in “hostile activity,” or to reduce their nuclear arsenals to a “reasonable level,” without further definitional clarity, then even with perfect verification, they will have a hard time cooperating around these norms. The reason is that “hostile activity” and “reasonable levels” are vague terms subject to many different interpretations. If what is banned is unclear, misinterpretations and disagreements will invariably occur, even if each side knows precisely what the other is doing. These misinterpretations and disagreements, in turn, are significant hurdles to the trust and perceptions of mutual compliance that are essential to mutually constrained cooperation. To avoid this problem, arms-control treaties use very precise technological definitions about which weapons are banned and what can be done with certain weapons.

#### Secrecy means Congress would be ineffective

**Dycus, Vermont law professor, 2010**

(Stephen, “Congress’s Role in Cyber Warfare”, 8-11, <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>, ldg)

The National Security Act of 1947 23 showed Congress’s determination to exert some control over this nation’s intelligence apparatus. That determination was strengthened after the disclosure of widespread intelligence abuses by the CIA and other agencies.24 In 1991, in response to the Iran-Contra Affair, Congress adopted a measure directing the President to keep the congressional intelligence committees “fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity.”25 The term “intelligence activity” expressly includes “covert actions,”26 which additionally require a written finding by the President that they are “necessary to support identifiable foreign policy objectives of the United States and [are] important to the national security of the United States.”27 Intelligence activities are also understood to include “all activities that elements of the Intelligence Community are authorized to conduct pursuant to [Executive Order No. 12,333],” the executive charter for such activities.28 The “intelligence community” includes the Office of the Director of National Intelligence, CIA, NSA, other Defense Department intelligence components, and other federal intelligence elements,29 which are authorized to engage in, inter alia, intelligence collection and analysis and “activities to protect against international terrorism . . . and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents.”30 This broad mandate certainly encompasses many U.S. efforts to defend against cyber attack and to employ cyber weapons offensively. By this definition, most preparations for and conduct of cyber warfare should be reported to the intelligence committees as “intelligence activities.” It is significant that the reporting requirement in the 1991 law is not limited to agencies within the intelligence community. 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 The “due regard for” language might be invoked to keep Congress in the dark. Under the 1991 law, “covert actions,” those with respect to which “it is intended that the role of the United States Government will not be apparent or acknowledged publicly,”33 need only be reported to a small group of legislators known as the “Gang of Eight,”34 and then only in a “timely fashion,” a term not defined by statute.35 Characterization of U.S. planning and execution of electronic warfare as “covert” could enable reporting to the smaller group, making it more difficult for Congress to play a significant role.36 Moreover, any reporting might be delayed indefinitely.37

### China

#### Offensive doctrine critical to prevent US-China war and solve IP theft

Blumenthal 2/28/13 (Dan, the director of Asian Studies at the American Enterprise Institute, where he focuses on East Asian security issues and Sino-American relations. Mr. Blumenthal has both served in and advised the U.S. government on China issues for over a decade. From 2001 to 2004, he served as senior director for China, Taiwan, and Mongolia at the Department of Defense. Additionally, he served as a commissioner on the congressionally-mandated U.S.-China Economic and Security Review Commission since 2006-2012, and held the position of vice chairman in 2007. He has also served on the Academic Advisory Board of the congressional U.S.-China Working Group. J.D., Duke Law School M.A., School of Advanced International Studies, Johns Hopkins University B.A., Washington University Chinese language studies, Capital Normal University “How to Win a Cyberwar with China” <http://www.foreignpolicy.com/articles/2013/02/28/how_to_win_a_cyberwar_with_china>)

The Internet is now a battlefield. China is not only militarizing cyberspace -- it is also deploying its cyberwarriors against the United States and other countries to conduct corporate espionage, hack think tanks, and engage in retaliatory harassment of news organizations. These attacks are another dimension of the ongoing strategic competition between the United States and China -- a competition playing out in the waters of the East and South China seas, in Iran and Syria, across the Taiwan Strait, and in outer space. With a number of recent high-profile attacks in cyberspace traced to the Chinese government, the cybercompetition seems particularly pressing. It is time for Washington to develop a clear, concerted strategy to deter cyberwar, theft of intellectual property, espionage, and digital harassment. Simply put, the United States must make China pay for conducting these activities, in addition to defending cybernetworks and critical infrastructure such as power stations and cell towers. The U.S. government needs to go on the offensive and enact a set of diplomatic, security, and legal measures designed to impose serious costs on China for its flagrant violations of the law and to deter a conflict in the cybersphere. Fashioning an adequate response to this challenge requires understanding that China places clear value on the cyber military capability. During the wars of the last two decades, China was terrified by the U.S. military's joint, highly networked capabilities. The People's Liberation Army (PLA) began paying attention to the role of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) assets in the conduct of war. But the PLA also concluded that the seeds of weakness were planted within this new way of war that allowed the United States to find, fix, and kill targets quickly and precisely -- an overdependence on information networks. Consider what might happen in a broader U.S.-China conflict. The PLA could conduct major efforts to disable critical U.S. military information systems (it already demonstrates these capabilities for purposes of deterrence). Even more ominously, PLA cyberwarriors could turn their attention to strategic attacks on critical infrastructure in America. This may be a highly risky option, but the PLA may view cyber-escalation as justified if, for example, the United States struck military targets on Chinese soil. China is, of course, using attacks in cyberspace to achieve other strategic goals as well, from stealing trade secrets to advance its wish for a more innovative economy to harassing organizations and individuals who criticize its officials or policies. Barack Obama's administration has begun to fight back. On Feb. 20, the White House announced enhanced efforts to fight the theft of American trade secrets through several initiatives: building a program of cooperative diplomacy with like-minded nations to press leaders of "countries of concern," enhancing domestic investigation and prosecution of theft, promoting intelligence sharing, and improving current legislation that would enable these initiatives. These largely defensive measures are important but should be paired with more initiatives that start to play offense. Offensive measures may be gaining some steam. The U.S. Justice Department, in creating the National Security Cyber Specialists' Network (NSCS) last year, recognizes the need for such an approach. The NSCS -- consisting of almost 100 prosecutors from U.S. attorneys' offices working in partnership with cyber-experts from the Justice Department's National Security Division and the Criminal Division's Computer Crime and Intellectual Property Section -- is tasked with "exploring investigations and prosecutions as viable options for deterrence and disruption" of cyberattacks, including indictments of governments or individuals working on the government's behalf. It's a good first step, but Congress could also consider passing laws forbidding individuals and entities from doing business in the United States if there is clear evidence of involvement in cyberattacks. Congress could also create a cyberattack exception to the Foreign Sovereign Immunities Act, which currently precludes civil suits against a foreign government or entity acting on its behalf in the cyber-realm. There is precedent: In the case of terrorism, Congress enacted an exception to immunity for states and their agents that sponsor terrorism, allowing individuals to sue them. Enterprising companies and intelligence personnel are already able to trace attacks with an increasing degree of accuracy. For example, the U.S. security company Mandiant traced numerous incidents going back several years to the Shanghai-based Unit 61398 of the PLA, which was first identified publicly by the Project 2049 Institute, a Virginia-based think tank. Scholars Jeremy and Ariel Rabkin have identified another way to initiate nongovernmental legal action: rekindling the 19th-century legal practice of issuing "letters of marque" -- the act of commissioning privateers to attack enemy ships on behalf of the state -- to selectively and cautiously legitimize retaliation by private U.S. actors against hacking and cyber-espionage. This would allow the U.S. government to effectively employ its own cybermilitia. Creating new laws or using current ones would force the Chinese government and the entities that support its cyberstrategy to consider the reputational and financial costs of their actions. Of course, if the United States retaliates by committing similar acts of harassment and hacking, it risks Chinese legal action. But America has a key advantage in that its legal system is respected and trusted; China's is not. Diplomatic action should bolster these efforts. The Obama administration's suggestions for pressuring China and other countries are a good start, but U.S. diplomacy must be tougher. In presenting Chinese leaders with overwhelming evidence of cyber-misdeeds (but without giving away too many details), Washington should communicate how it could respond. To control escalation, the administration should explain what it views as proportionate reprisals to different kinds of attacks. (For instance, an attack on critical infrastructure that led to deaths would merit a different response than harassment of the New York Times.) As the administration's report suggests, the United States is not the only victim and should engage in cooperative diplomacy. The United States should set up a center for cyberdefense that would bring together the best minds from allied countries to develop countermeasures and conduct offensive activities. One such center could be Taiwan, as its understanding of Chinese language, culture, business networks, and political landscape make it invaluable in the fight against cyberattacks. Of course, centers could be placed elsewhere and still utilize Taiwan's knowledge, but even the threat of placing a cyberdefense center just across the strait would be very embarrassing for China's leaders, as Taiwan is viewed as a renegade province. The point is not to be gratuitously provocative, but rather to demonstrate that the United States options that China would not favor. The U.S. military's cyber-efforts presumably already include it own probes, penetrations, and demonstrations of capability. While the leaks claiming the U.S. government's involvement in the Stuxnet operation -- the computer worm that disabled centrifuges in the Iranian nuclear program -- may have damaged U.S. national security, at least China knows that Washington is quite capable of carrying out strategic cyberattacks. To enhance deterrence, the U.S. government needs to demonstrate these sorts of capabilities more regularly, perhaps through cyber-exercises modeled after military exercises. For example, the U.S. military could set up an allied public training exercise in which it conducted cyberattacks against a "Country X" to disable its military infrastructure such as radars, satellites, and computer-based command-and-control systems. To use the tools at America's disposal in the fight for cybersecurity will require a high degree of interagency coordination, a much-maligned process. But Washington has made all the levers of power work together previously. The successful use of unified legal, law enforcement, financial, intelligence, and military deterrence against the Kim regime of North Korea during a short period of George W. Bush's administration met the strategic goals of imposing serious costs on a dangerous government. China is not North Korea -- it is far more responsible and less totalitarian. But America must target those acting irresponsibly in cyberspace. By taking the offensive, the United States can start to impose, rather than simply incur, costs in this element of strategic competition with China. Sitting by idly, however, presents a much greater likelihood that China's dangerous cyberstrategy could spark a wider conflict.

#### OCOs solves North Korean brinkmanship-speed is key to coercive leverage

**Libicki, RAND senior management scientist, 2013**

(Martin, “Brandishing Cyberattack Capabilities”, [http://www.rand.org/pub s/research\_reports/RR175.html](http://www.rand.org/pub%20s/research_reports/RR175.html), ldg)

Our inquiry is therefore more humble. Could a U.S. threat that it might interfere with a rogue state’s nuclear weapon delivery help shape a nuclear confrontation? For this question, assume a rogue nuclear power with a handful of weapons capable of hitting nearby countries (but generally incapable of hitting the continental United States). The United States has a robust cyberattack capability (in general terms), from which the rogue state’s nuclear arsenal is not provably immune. Although the United States enjoys escalation dominance, the rogue state is far more willing to go to the nuclear brink than the United States is. The rogue state (thinks it) has more at stake (i.e., regime survival). Furthermore, it may act in ways that are irrational by Western perspectives. We first model a two-state confrontation, then later introduce a friendly state on whose behalf the United States has intervened. The United States enters this scenario facing the choice of acting when doing so risks the rogue state releasing a nuclear weapon. Whether the threat is explicit or implicit is secondary. The usual calculus applies. The rogue state is better off if its threat leads the United States to stop. The United States is better off ignoring the threat and going ahead with what it would have done in the absence of the threat if the threat can be nullified but cannot know that it will be for certain. The rogue state understands that if it does use nuclear weapons, it could face great retaliation.1 If the United States acts (successfully) in the face of warning and if the rogue state does not use nuclear weapons, the United States achieves its objectives and wins the overall confrontation.2 If the United States flinches, the rogue state wins. If the rogue state uses its nuclear weapons and if, as is likely, the United States responds likewise, the rogue state loses greatly, but the United States is also far worse off.3 Two-Party Confrontations In a confrontation in which disaster would result from both sides carrying out their threats, each must ask: Are such threats credible? If one side thinks the other will yield, it pays to stand firm. If it thinks, however, that the other is implacable, it may have no good choice but to yield itself. The projection of implacability is beneficial, but the reality of implacability is frequently suicidal. Note that the basis for the implacability can also be entirely subjective, which is to say, unfounded on the facts of the matter. If one party is convinced that it will never pay a high price for being implacable, communicates as much, and acts as if it were so, the other cannot take any comfort from the fact that the first has no technical basis for the belief. The only consideration is whether the first party actually believes as much, is willing to act accordingly, and can ignore the logic that whispers that no one can possibly be completely confident on the basis of iffy information. To one party, the willingness to act on the basis of the impossible seems like cheating. To use an analogy, imagine a game of “chicken” in which the driver of one of the two oncoming cars throws the steering wheel out the window. This cheat forces the opponent to choose between a certain crash or veering away (and thus losing). However, when the consequences of a crash are far greater than the benefits of winning, this strategy is irrational if there is a nontrivial likelihood that the other side will be intent on punishing cheaters at the cost of all other values. In the analogy, the second driver might rather crash than lose to a cheater.4 But in general, a strategy of implacability, can, if credible, do well, as long as the other side is not equally implacable. So, the United States creates the belief (whether by saying so, hinting, or letting others draw their own conclusion) that the rogue state cannot carry out its nuclear threat. That is, the United States acts as though a flaw somewhere in the nuclear command-and-control cycle, probably an induced flaw, prevents immediate nuclear use. A lesser case is that the command and control is less certain, the weapon is weaker, and/or the delivery system is far less accurate than feared.5 Although permanently disabling a nuclear command-and-control system is quite a stretch for cyberwar, it is less fantastic to imagine that the United States could delay a weapon’s use. A temporary advantage, though, may still give the United States time to cross the red line and thereby attain a fait accompli. So posturing, the United States prepares to cross the red line, while communicating its confidence that the rogue state will not retaliate. This confidence stems from a combination of its own nuclear deterrence capability plus its ability to confound the rogue state’s nuclear capability: The rogue nuclear state probably will not decide to retaliate, and if it did decide to, probably cannot retaliate. The combination, in this case, is what reduces the odds of a nuclear response to a sufficiently low level, if the rogue state is at all rational. Even if it later assures itself and others that its nuclear capacity is intact, but the United States has already acted, the onus then falls on the rogue nuclear state to respond to what could well be a done deal. If the rogue state understands the logic before brandishing its own nuclear weapons, it may choose not to ratchet up tensions in advance of the U.S. crossing red lines.

#### Global nuclear war

**Hayes and Green, Victoria University AND Executive Director of the Nautilus Institute, 2010**

 [Peter, Victoria University, and Michael, Executive Director of the Nautilus Institute, “-“The Path Not Taken, the Way Still Open: Denuclearizing the Korean Peninsula and Northeast Asia”]jap

The consequences of failing to address the proliferation threat posed by the North Korea developments, and related political and economic issues, are serious, not only for the Northeast Asian region but for the whole international community. At worst, there is the possibility of nuclear attack1, whether by intention, miscalculation, or merely accident, leading to the resumption of Korean War hostilities. On the Korean Peninsula itself, key population centres are well within short or medium range missiles. The whole of Japan is likely to come within North Korean missile range. Pyongyang has a population of over 2 million, Seoul (close to the North Korean border) 11 million, and Tokyo over 20 million. Even a limited nuclear exchange would result in a holocaust of unprecedented proportions. But the catastrophe within the region would not be the only outcome. New research indicates that even a limited nuclear war in the region would rearrange our global climate far more quickly than global warming. Westberg draws attention to new studies modelling the effects of even a limited nuclear exchange involving approximately 100 Hiroshima-sized 15 kt bombs2 (by comparison it should be noted that the United States currently deploys warheads in the range 100 to 477 kt, that is, individual warheads equivalent in yield to a range of 6 to 32 Hiroshimas).The studies indicate that the soot from the fires produced would lead to a decrease in global temperature by 1.25 degrees Celsius for a period of 6-8 years.3 In Westberg’s view: That is not global winter, but the nuclear darkness will cause a deeper drop in temperature than at any time during the last 1000 years. The temperature over the continents would decrease substantially more than the global average. A decrease in rainfall over the continents would also follow...The period of nuclear darkness will cause much greater decrease in grain production than 5% and it will continue for many years...hundreds of millions of people will die from hunger...To make matters even worse, such amounts of smoke injected into the stratosphere would cause a huge reduction in the Earth’s protective ozone.4 These, of course, are not the only consequences. Reactors might also be targeted, causing further mayhem and downwind radiation effects, superimposed on a smoking, radiating ruin left by nuclear next-use. Millions of refugees would flee the affected regions. The direct impacts, and the follow-on impacts on the global economy via ecological and food insecurity, could make the present global financial crisis pale by comparison.

#### OCO’s deescalate the East China Sea

**Drogen, Surfview Capital founder and CIO, 2013**

(Leigh, “Why Cyber Weapons Will Make The World Even Safer”, 3-4, <http://www.leighdrogen.com/why-cyber-weapons-will-make-the-world-even-safer/>, ldg)

Scene: China has just exchanged fire with Japan over the East China Sea Islands. The US Navy is in theatre and has as promised under its security umbrella treaty with Japan vows to protect the sovereignty of Japanese territory. In response China has threatened to hold US infrastructure (power, water, transportation) hostage and gives the US 48 hours to exit the theatre. The US immediately responds with a similar threat to cripple Chinese infrastructure via cyber attacks unless China relinquishes cyber attacks within 48 hours. Now you can bet your last dollar that the US has been holding war games designed to simulate exactly this scenario. And while we don’t know how they’ve played out, we can make some pretty informed assumptions based on the corollary of nuclear war theory. The ability for foreign agents to hijack critical infrastructure and cripple it within a short period of time is now to the point where we, and our potential adversaries, could face damage many magnitudes higher than a nuclear strike, not in lives lost, but economic, social, and political damage. Cyber warfare has reached a level where we can say that there is mutually assured destruction of critical infrastructure in a war between the US and China. Which is exactly why I’m ready to say that cyber warfare will make the world an even safer place. There is no argument against the claim that nuclear weapons have massively decreased overall warfare across the world since World War II. During that time we haven’t seen a war between two nuclear states. But the more important development, as Tom Friedman loves to point out, we haven’t seen a major conflict between two countries with a McDonalds. Now, look past the frivolity of that statement through to the bigger point, lives lost is no longer the major determinant of why countries decide to forgo war, it is now primarily an economic and social decision. The cost in treasure and political capital that it takes to go to war as a developed economy with another state is massive. The US has had a huge hand in this no doubt playing the world’s policeman since World War II. Police are not very effective at hunting down transgressors, their job is primarily prevention, a job that the US has pretty much perfected at this point. China will not follow through on its cyber war threat because the cost in economic, social, and political damage to the regime from a crippling US cyber attack would be far too much to handle versus the benefit from its move on the islands. What do you think middle and upper class urban Chinese citizens would do if China risked everything they’ve worked so hard to build over the past 25 years for the islands? They risk nothing less than the regime being toppled. They are already walking on thin ice under the unwritten deal they’ve made, continued economic development for the regime’s position in power. Cyber war has reached the level of mutually assured destruction as the damage caused will lead to popular revolt. It certainly would here in the US. The flip side to this argument, as it is made with nuclear weapons, is that non state actors are not tied to the same consequences and therefor are much more dangerous. I would agree, and in the case of cyber war they it’s even scarier as their capability to inflict damage is far greater (this was the theme of Skyfall), it’s hard to obtain and deliver a nuclear weapon. That said, I believe cyber weapons will add to global security as they become more pervasive.

# 2NC

## Topicality

### Their card

**Doesn’t say RESTRICTION ANYWHERE WHICH IS GAME OVER**

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

devices are more readily available and more easily effectuated than controls imposed by statute. And some observers have attributed substantial influence to nonstatutory controls in regulatory as well as other matters.3 It is impossible, in a limited space, to provide a comprehensive and exhaustive listing of congressional actions that override, have the effect of overturning, or prevent the promulgation of administrative rules. Consequently, this report concentrates upon the more direct statutory devices, although it also encompasses committee reports accompanying bills, the one nonstatutory instrument that is frequently most authoritatively connected with the final legislative product. The statutory mechanisms surveyed here cross a wide spectrum of possible congressional action: 1. single-purpose provisions to overturn or preempt a specific rule; 2. alterations in program authority that remove jurisdiction from an agency; 3. agency authorization and appropriation limitations; 4. inter-agency consultation requirements; and 5. congressional prior notification provisions

#### Their ev only defines "statutory," not "restrictions on authority" - that kills predictability

J.A.D. Haneman 59, justice of the Superior Court of New Jersey, Appellate Division. “Russell S. Bertrand et al. v. Donald T. Jones et al.,” 58 NJ Super. 273; 156 A.2d 161; 1959 N.J. Super, Lexis

 HN4 In ascertaining the meaning of the word "restrictions" as here employed, it must be considered in context with the entire clause in which it appears. It is to be noted that the exception concerns restrictions "which have been complied with." Plainly, this connotes a representation of compliance by the vendor with any restrictions upon the permitted uses of the subject property. The conclusion that "restrictions" refer solely to a limitation of the manner in which the vendor may [\*\*\*14] use his own lands is strengthened by the further provision found in said clause that the conveyance is "subject to the effect, [\*\*167] if any, of municipal zoning laws." Municipal zoning laws affect the use of property.¶ HN5 A familiar maxim to aid in the construction of contracts is noscitur a sociis. Simply stated, this means that a word is known from its associates. Words of general and specific import take color from each other when associated together, and thus the word of general significance is modified by its associates of restricted sense. 3 Corbin on Contracts, § 552, p. 110; cf. Ford Motor Co. v. New Jersey Department of Labor and Industry, 5 N.J. 494 (1950). The [\*284] word "restrictions," therefore, should be construed as being used in the same limited fashion as "zoning."

## K

### 2NC – OV

#### The use of their cyber war metaphor turns the case – institutionalizes power in the hands of military organizations at the expense of civilians and breeds complacency. The alternative allows a holistic form of policy planning which solves the entire aff.

Wallace 13 (Ian Wallace is a visiting fellow in cybersecurity at Brookings’ Center on 21st Century Security and Intelligence in Washington, DC, “Why The U.S. Is Not In A Cyber War,” http://www.thedailybeast.com/articles/2013/03/10/why-the-u-s-is-not-in-a-cyber-war.html)

For several weeks, it has been difficult to open a newspaper or watch a Sunday talk show without hearing about the advent of “cyber war.” The media has been filled with an avalanche of cyber threat-related stories: the hacking of leading newspapers, evidence of Chinese government involvement in intellectual property theft, and now, further distributed denial of service attacks against U.S. banks. All these events present real and serious national security challenges. But cyber-espionage, cyber-crime and the malicious disruption of critical infrastructure are not the same as war, and the distinction is important. The idea that America is in the middle of a “cyber war” isn't just lazy and wrong. It's dangerous. The war analogy implies the requirement for military response to cyber intrusions. America genuinely needs effective civilian government cyber defense organizations with strong relationships with the private sector and the active engagement of an informed general public. Creating and even promoting the fear of “cyber war” makes that more difficult. Here’s why: First, while the U.S fights its wars using the highly-trained professional within the U.S. Armed Forces, defending against cyber threats does not necessary require military expertise or prowess. True, most private individuals and corporations lack the knowledge and training needed to fight off attacks from elite Chinese, Iranian and Russian cyber “warriors.” As a result, there is and will continue to be a pressing need for highly qualified information security experts to help defend the larger U.S. cyber landscape. Nonetheless, there are relatively simple ways to make it more difficult for the bad guys without escalating to a “war” standing. In 2011, the Australian Defence Signals Directorate (their equivalent of the U.S. National Security Agency) showed that by taking just four key measures--“whitelisting” (i.e., allowing only authorized software to run on a computer or network), very rapid patching of applications and of operating system vulnerabilities, and restricting the number of people with administrator access to a system--85 percent of targeted intrusions can be prevented. These might appear more like prophylactic public health measures than warfare--and that’s the point. The United States does not need to declare “war” and call up the military to fend off cyber threats. Second, people expect wars to end and when they drag on, often succumb to war fatigue. People want to believe that victory is achievable. Cyber security, however, is a mission without end. As a result, using the language of war may only serve to frustrate and mislead the public. The fight against cyber attacks will never achieve a definitive, all-encompassing, long-term victory. As more and different devices are connected to the Internet, the threat will continually evolve. While technological countermeasures will surely improve, cyber attacks will remain a very attractive means through which to coerce, defraud, and potentially even harm us as our lives grow ever more dependent on the Internet. The problem with ‘war’ terminology is that it may breed frustration and contempt, and eventually complacency and cynicism. The growing use of sensational terms like “electronic Pearl Harbor”--which in particular evokes a horrific event that ended the lives of 2402 sailors, airmen, and civilians--becomes as much a part of the problem as the solution. Better analogies (and public policy) are needed to ensure that the public comes to ‘own’ this cyber security challenge as part of their daily lives. The third problem with the war analogy is that it legitimizes expedients, especially institutional ones. This goes to the core of the ongoing cyber legislation debate. An important point of difference between the advocates and opponents of the failed Senate Cybersecurity Act of 2012 was about the role that the National Security Agency (NSA) should play in information exchange with industry. And while the recently relaunched House Intelligence Committee’s Cyber Intelligence Sharing and Protection Act CISPA is carefully worded to acknowledge the centrality of the Department of Homeland Security to its information-sharing process, concerns still remain. Internet advocacy groups like the Center for Democracy and Technology have argued that its provisions could weaken Homeland Security’s role in favor of more engagement between the private sector and the National Security Agency. Whether that is true or not--and CISPA advocates deny it--there are still those in Congress who see “giving the problem” to the Department of Defense as part of the answer. Now is not the time for expedients, however well intentioned. The NSA certainly has a key role to play; when dealing with overseas threats, it would be self-defeating not to utilize the capabilities of the world’s most impressive signals intelligence organization. Privacy concerns need to be balanced against the potential for extreme privacy loss when your data is spread across the web by cyber criminals or exfiltrated by foreign intelligence operatives. It is also unrealistic, both financially and practically, to create a parallel organization within the Department of Homeland Security. That is why President Obama’s recent Executive Order sensibly includes measures to widen the pool of organizations that can benefit from what the NSA knows. However, none of that means additional responsibility for America’s cybersecurity efforts should be put into military hands. What is required is a more effective DHS, not a more customer-focused NSA. The quicker the country builds up the civilian institutional capacity it needs for long-term cyber security, the better. It would be unfortunate indeed if the specter of “cyber war” gave succor to those who favor further boosting the Pentagon’s and the Intelligence Community’s responsibilities at the expense (in practice, if not in theory) of a non-military security agency such as DHS. This is would be particularly true if the short-term effect was a continued block on the passage of much-needed cyber legislation. However, this is not just a Congressional problem. The Obama administration has also internalized the lessons from the last decade: in a time of “war,” it is relatively easy to get funding for the military to take on and complete a mission as opposed to building new civilian capacity to handle the job. Just as it was with nation building in Iraq, so it is with cyber defense. The reported plan to establish national mission forces under the military’s U.S. Cyber Command (which is tasked with protecting critical infrastructure) is an understandable bureaucratic response to a perceived need to “defend the nation.” The problem comes if nothing more happens. The challenge then becomes ensuring that the necessary cyber defense architecture and robust civilian government support shifts over to the private sector. That will be difficult enough; the banging of war-drums will make it even harder to accomplish. Not that the Defense Department and U.S. military should stay out of the cyber security business--quite the opposite. The fourth and final reason why we should be cautious in talking about cyber warfare is the risk that such imprecision leaves us ill-prepared to deal with the cyber elements of war when we do have to confront them. Director of the NSA and Commander of U.S. Cyber Command General Keith Alexander not only has to continue to supply U.S. leaders with top quality strategic intelligence, he must also ensure the United States is prepared to exploit cyber opportunities when the country does go to war. At the same time, General Alexander will need to ensure that U.S. forces’ extraordinary technological capabilities retain their edge in the face of the cyber attacks that will very likely target them whenever they next go into the field. While General Alexander and his organizations will remain major contributors to any government effort to fend off serious national threats, we should also be mindful of the opportunity cost of making the NSA and the Cyber Command the “super Geek Squad” for the private sector and the nation more generally. These organizations must stay focused on their primary missions--defending U.S. national security. Rejecting the application of the war metaphor to cybersecurity should not diminish the current challenges faced by governments, the public, and cyber security professionals. However, when a real cyber war is declared, it will be messy and dangerous, and we need to be prepared, especially on the home front. That planning is best done deliberately, dispassionately and holistically. Declaring “war” too early will undermine our efforts and likelihood of success.

#### Focus on cyber weapons ignores underlying political conflict

Schwartz and Derber 1990

William A., Boston Nuclear Study Group, and Charles, BNSG and professor of political economy and sociology at Boston College, online: http://ark.cdlib.org/ark:/13030/ft1n39n7wg/

For many years, a striking consensus has reigned: the nuclear arms race between the superpowers is the main source of danger. The arms race is "the central concern of the closing years of the century," the cause célèbre of our time. A U.S. senator says that "the very survival of our planet, the survival of the human race, is at stake," a common view.[[1](http://texts.cdlib.org/dynaxml/servlet/BookView?source=eschol/4916/4916.xml&style=eschol/xsl/dynaxml/BookView?source=eschol/4916/4916.xml&style=eschol/xsl/dynaxml/dynaxml.xsl&doc.view=0&chunk.id=nsd0e180&toc.id=endnotes&toc.depth=1&query=0&anch%20)] **The right, the center, and the left disagree**, of course, **about how the U**nited **S**tates **should run the arms race. The right urges us to build weapons** like the MX missile, the Stealth bomber, and "Star Wars"; **the center, to sign arms control treaties** like INF and START with the Soviet Union; **and the left, to stop and then reverse the arms race** through a test ban, a "freeze," and huge reductions in nuclear arsenals. **But all focus on the** hardware, the **weapons themselves**. Most of the nuclear debate concerns which weapons should be deployed and which destroyed. But short of near-total nuclear disarmament, we believe that **no change in the arms race can in fact make a profound difference**. MX, Star Wars, INF, a freeze, or even a 90 percent reduction in nuclear arsenals cannot reliably change the horror of a nuclear war. They cannot much affect the risk that the nuclear states will plunge us into that horror. They cannot make the world much safer or more dangerous than it already is. The nuclear danger is real—even more ominous, as we will show, than most people appreciate. But **the fixation on weapons has obscured the real menace: the political conflict** and violence raging around the world **that could** one day burn out of control and **set off a nuclear cataclysm. As the world debates** largely **irrelevant** missiles and **arms control treaties, the superpowers are fanning the flames of** conflict and **war from Afghanistan to Nicaragua**, Lebanon to Cambodia. Forty years of history reveal that such conflicts can suddenly veer out of control and even erupt into open superpower confrontation. Yet in a time of unprecedented public concern about nuclear war, **few—even in the peace movement—protest the nuclear hazards of their governments' foreign intrigues and interventions. Those** of us **concerned with the nuclear threat have** long **been like the** apocryphal **drunk who searches for his lost keys** hour after hour **under a lamppost—because it's light there. The giant weapons systems are** seductive, **the obvious place to look for answers to the nuclear peril.** The light there is good. **But there is little to be found. If we want the keys to a safer world, we must turn the light to the real conflicts** and battlefields where the superpowers and their clients confront each other every day, **often hidden from public view**, **and where they periodically collide in terrifying crises that threaten to provoke worldwide catastrophe**.

### 2NC – Epistemology

#### **Questioning the affirmatives ontology is a prior question to the advantages; the form of social relations their advocacy embodies rests on faulty epistemology and makes extinction inevitable---vote negative as a form of noncooperation with their political economy**

Willson 13 (Brain, is a Ph.D New College San Fransisco, Humanities, JD, American University, “Developing Nonviolent Bioregional Revolutionary Strategies,” http://www.brianwillson.com/developing-nonviolent-bioregional-revolutionary-strategies/)

I. Industrial civilization is on a collision course with life itself. Facilitating its collapse is a deserved and welcomed correction, long overdue. Collapse is inevitable whether we seek to facilitate it or not. Nonetheless, whatever we do, industrial civilization, based as it is on mining and burning finite and polluting fossil fuels, cannot last because it is destroying the ecosystem and the basis of local, cooperative life itself. It knows no limits in a physically finite world and thus is unsustainable. And the numbers of our human species on earth, which have proliferated from 1.6 billion in 1900 to 7 billion today, is the consequence of mindlessly eating oil – tractors, fertilizers, pesticides, herbicides – while destroying human culture in the process. Our food system itself is not sustainable. Dramatic die-off is part of the inevitable correction in the very near future, whether we like it or not. Human and political culture has become totally subservient to a near religion of economics and market forces. Technologies are never neutral, with some being seriously detrimental. Technologies come with an intrinsic character representing the purposes and values of the prevailing political economy that births it. The Industrialism process itself is traumatic. It is likely that only when we experience an apprenticeship in nature can we be trusted with machines, especially when they capital intensive & complicated. The nation-state, intertwined more than ever with corporate industrialism, will always come to its aid and rescue. Withdrawal of popular support enables new imagination and energy for re-creating local human food sufficient communities conforming with bioregional limits. II. The United States of America is irredeemable and unreformable, a Pretend Society. The USA as a nation state, as a recent culture, is irredeemable, unreformable, an anti-democratic, vertical, over-sized imperial unmanageable monster, sustained by the obedience and cooperation, even if reluctant, of the vast majority of its non-autonomous population. Virtually all of us are complicit in this imperial plunder even as many of us are increasingly repulsed by it and speak out against it. Lofty rhetoric has conditioned us to believe in our national exceptionalism, despite it being dramatically at odds with the empirically revealed pattern of our plundering cultural behavior totally dependent upon outsourcing the pain and suffering elsewhere. We cling to living a life based on the social myth of US America being committed to justice for all, even as we increasingly know this has always served as a cover for the social secret that the US is committed to prosperity for a minority thru expansion at ANY cost. Our Eurocentric origins have been built on an extraordinary and forceful but rationalized dispossession of hundreds of Indigenous nations (a genocide) assuring acquisition of free land, murdering millions with total impunity. This still unaddressed crime against humanity assured that our eyes themselves are the wool. Our addiction to the comfort and convenience brought to us by centuries of forceful theft of land, labor, and resources is very difficult to break, as with any addiction. However, our survival, and healing, requires a commitment to recovery of our humanity, ceasing our obedience to the national state. This is the (r)evolution begging us. Original wool is in our eyes: Eurocentric values were established with the invasion by Columbus: Cruelty never before seen, nor heard of, nor read of – Bartolome de las Casas describing the behavior of the Spaniards inflicted on the Indigenous of the West Indies in the 1500s. In fact the Indigenous had no vocabulary words to describe the behavior inflicted on them (A Short Account of the Destruction of the Indies, 1552). Eurocentric racism (hatred driven by fear) and arrogant religious ethnocentrism (self-righteous superiority) have never been honestly addressed or overcome. Thus, our foundational values and behaviors, if not radically transformed from arrogance to caring, will prove fatal to our modern species. Wool has remained uncleansed from our eyes: I personally discovered the continued vigorous U.S. application of the “Columbus Enterprise” in Viet Nam, discovering that Viet Nam was no aberration after learning of more than 500 previous US military interventions beginning in the late 1790s. Our business is killing, and business is good was a slogan painted on the front of a 9th Infantry Division helicopter in Viet Nam’s Mekong Delta in 1969. We, not the Indigenous, were and remain the savages. The US has been built on three genocides: violent and arrogant dispossession of hundreds of Indigenous nations in North America (Genocide #1), and in Africa (Genocide #2), stealing land and labor, respectively, with total impunity, murdering and maiming millions, amounting to genocide. It is morally unsustainable, now ecologically, politically, economically, and socially unsustainable as well. Further, in the 20th Century, the Republic of the US intervened several hundred times in well over a hundred nations stealing resources and labor, while imposing US-friendly markets, killing millions, impoverishing perhaps billions (Genocide #3). Since 1798, the US military forces have militarily intervened over 560 times in dozens of nations, nearly 400 of which have occurred since World War II. And since WWII, the US has bombed 28 countries, while covertly intervening thousands of times in the majority of nations on the earth. It is not helpful to continue believing in the social myth that the USA is a society committed to justice for all , in fact a convenient mask (since our origins) of our social secret being a society committed to prosperity for a few through expansion at ANY cost. (See William Appleman Williams). Always possessing oligarchic tendencies, it is now an outright corrupt corporatocracy owned lock stock and barrel by big money made obscenely rich from war making with our consent, even if reluctant. The Cold War and its nuclear and conventional arms race with the exaggerated “red menace”, was an insidious cover for a war preserving the Haves from the Have-Nots, in effect, ironically preserving a western, consumptive way of life that itself is killing us. Pretty amazing! Our way of life has produced so much carbon in the water, soil, and atmosphere, that it may in the end be equivalent to having caused nuclear winter. The war OF wholesale terror on retail terror has replaced the “red menace” as the rhetorical justification for the continued imperial plunder of the earth and the riches it brings to the military-industrial-intelligence-congressional-executive-information complex. Our cooperation with and addiction to the American Way Of Life provides the political energy that guarantees continuation of U.S. polices of imperial plunder. III. The American Way Of Life (AWOL), and the Western Way of Life in general, is the most dangerous force that exists on the earth. Our insatiable consumption patterns on a finite earth, enabled by but a one-century blip in burning energy efficient liquid fossil fuels, have made virtually all of us addicted to our way of life as we have been conditioned to be in denial about the egregious consequences outsourced outside our view or feeling fields. Of course, this trend began 2 centuries earlier with the advent of the industrial revolution. With 4.6% of the world’s population, we consume anywhere from 25% to nearly half the world’s resources. This kind of theft can only occur by force or its threat, justifying it with noble sounding rhetoric, over and over and over. Our insatiable individual and collective human demands for energy inputs originating from outside our bioregions, furnish the political-economic profit motives for the energy extractors, which in turn own the political process obsessed with preserving “national (in)security”, e.g., maintaining a very class-based life of affluence and comfort for a minority of the world’s people. This, in turn, requires a huge military to assure control of resources for our use, protecting corporate plunder, and to eliminate perceived threats from competing political agendas. The U.S. War department’s policy of “full spectrum dominance” is intended to control the world’s seas, airspaces, land bases, outer spaces, our “inner” mental spaces, and cyberspaces. Resources everywhere are constantly needed to supply our delusional modern life demands on a finite planet as the system seeks to dumb us down ever more. Thus, we are terribly complicit in the current severe dilemmas coming to a head due to (1) climate instability largely caused by mindless human activities; (2) from our dependence upon national currencies; and (3) dependence upon rapidly depleting finite resources. We have become addicts in a classical sense. Recovery requires a deep psychological, spiritual, and physical commitment to break our addiction to materialism, as we embark on a radical healing journey, individually and collectively, where less and local becomes a mantra, as does sharing and caring, I call it the Neolithic or Indigenous model. Sharing and caring replace individualism and competition. Therefore, A Radical Prescription Understanding these facts requires a radical paradigmatic shift in our thinking and behavior, equivalent to an evolutionary shift in our epistemology where our knowledge/thinking framework shifts: arrogant separateness from and domination over nature (ending a post-Ice Age 10,000 year cycle of thought structure among moderns) morphs to integration with nature, i.e., an eco-consciousness felt deeply in the viscera, more powerful than a cognitive idea. Thus, we re-discover ancient, archetypal Indigenous thought patterns. It requires creative disobedience to and strategic noncooperation with the prevailing political economy, while re-constructing locally reliant communities patterned on instructive models of historic Indigenous and Neolithic villages.

### 2NC – Link Debate

#### Discussing cyber in terms of war leads to militaristic problem/solution schemes

Lawson 11 (Sean Lawson, Assistant Professor in the Department of Communication at the University of Utah. His Ph.D. is from the Department of Science and Technology Studies at Rensselaer Polytechnic Institute. “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>)

The language that we use to frame problems opens up some avenues for response while closing off others. In cyber-doom scenarios, cybersecurity is framed primarily in terms of “war” and, with the use of terms like “cyber-9/11” and “cyber-Katrina,” in terms of large-scale “disaster.” This war/disaster framing can lead to a militarist, command and control mindset that is ultimately counter-productive. A war framing implies the need for military solutions to cybersecurity challenges, even though most of what gets lumped under the term “cyberwar” are really acts of crime, espionage, or political protest, and even though it is not at all clear that a military response is either appropriate or effective (Lewis, 2010). Nonetheless, the establishment of the military’s U.S. Cyber Command (USCYBERCOM) has been the most significant U.S. response yet to perceived cyber-threats. Such a response is fraught with danger. First, the very existence of USCYBERCOM, which has both an offensive and defensive mission, could undermine the U.S. policy of promoting a free and open Internet worldwide by encouraging greater Internet censorship and filtering, as well as more rapid militarization of cyberspace (Cavelty, 2007: 143). For example, some have already called for USCYBERCOM to launch strikes on WikiLeaks, which leaked hundreds of thousands of classified U.S. documents about the wars in Iraq and Afghanistan (McCullagh, 2010b; Whitton, 2010; Thiessen, 2010). Such a response would only serve to create a “say-do gap” (Mullen, 2009) that potential adversaries could use to justify their own development and use of offensive cyber weapons and efforts to thwart whatever possibility there is for international cooperation on cybersecurity. Second, there is the danger of “blow back.” In a highly interconnected world, there is no guarantee that an offensive cyberattack launched by the United States against another country would not result in serious collateral damage to noncombatants or even end up causing harm to the United States (Cavelty, 2007: 143). Such “blow back” may have occurred in a recent case where the United States military took down a Jihadist discussion forum, causing collateral damage to noncombatant computers and websites, as well as undermining an ongoing U.S. intelligence gathering operation (Nakashima, 2010). Third, there is the risk of conflict escalation from cyberattack to physical attack. If the United States launched a cyberattack against a state or non-state actor lacking the capability to respond in kind, that actor might chose to respond with physical attacks (Clarke, 2009). There have even been calls for the United States to respond with conventional military force to cyberattacks that amounted to little more than vandalism (Zetter, 2009; Dunn, 2010). Finally, a 2009 review of U.S. military strategy documents, combined with statements from officials, further adds to the confusion and potential for escalation by indicating that nuclear response remains on the table as a possible U.S. response to cyberattack (Markoff & Shanker, 2009; Owens et al., 2009).

#### Reject this disaster framing—it only diverts resources and attention from more pressing issues

Lawson 11 (Sean Lawson, Assistant Professor in the Department of Communication at the University of Utah. His Ph.D. is from the Department of Science and Technology Studies at Rensselaer Polytechnic Institute. “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>)

Next, a disaster framing portends cybersecurity planning dominated by the same “command and control [C2] model” rooted in flawed assumptions of inevitable “panic” and “social collapse” that has increasingly dominated official U.S. disaster planning (Quarantelli, 2008: 897). The result has been ever more centralized, hierarchical, and bureaucratic disaster responses that increasingly rely upon the military to restore order and official control first and foremost (Quarantelli, 2008: 895–896; Alexander, 2006; Lakoff, 2006). The result can be a form of “government paternalism” in which officials panic about the possibility of panic and then take actions that exacerbate the situation by not only failing to provide victims with the help they need, but also preventing them from effectively helping themselves (Dynes, 2006; Clarke & Chess, 2009: 999–1001). This phenomenon was on display in the official response to Hurricane Katrina (Clarke & Chess, 2009: 1003–1004). In the realm of cybersecurity, there are already provisions for the military’s USCYBERCOM to provide assistance to the Department of Homeland Security in the event of a domestic cyber emergency (Ackerman, 2010). Reminiscent of self-imposed blackouts during WWII, Senator Joseph Lieberman’s proposal for a so-called “Internet kill switch,” which would give the president the authority to cut U.S. Internet connections to the rest of the world in the event of a large-scale cyberattack, 5 is the ultimate expression of the desire to regain control by developing the means to destroy that which we fear to lose. The war/disaster framing at the heart of cyber-doom scenarios and much of contemporary U.S. cybersecurity discourse risks focusing policy on the narrowest and least likely portion of the overall cybersecurity challenge—i.e. acts of “cyberwar” leading to economic, social, or civilizational collapse—while potentially diverting attention and resources away from making preparations to prevent or mitigate the effects of more realistic but perhaps less dramatic scenarios. But, there are a number of principles that can guide the formulation and evaluation of cybersecurity policy that can help us to avoid these pitfalls.

### AT: Security Mobilizes Activism --- Securitization

#### ---Security mobilized activism is bad ---

#### (A.) Framing policies through a lens of fear causes paralysis, partying, praying or preparing, NOT the creation of preventative solutions.

Gross & Gilles 2012

Matthew Barrett, editor of the Glen Canyon Reader and media strategist who has worked for Howard Dean's 2004 presidential campaign and Jon Tester's successful campaign for U.S. Senate in Montana, Mel, writer and a former advocate for victims of domestic abuse, From “The Last Myth: What the Rise of Apocalyptic Thinking Tells Us About America,” How Apocalyptic Thinking Prevents Us from Taking Political Action, The Atlantic, http://www.theatlantic.com/politics/archive/2012/04/how-apocalyptic-thinking-prevents-us-from-taking-political-action/255758/

The deeper we entangle the challenges of the 21st century with apocalyptic fantasy, the more likely we are to paralyze ourselves with inaction -- or with the wrong course of action. We react to the idea of the apocalypse -- rather than to the underlying issues activating the apocalyptic storyline to begin with -- by either denying its reality ("global warming isn't real") or by despairing at its inevitability ("why bother recycling when the whole world is burning up?"). We react to apocalyptic threats by either partying (assuaging our apocalyptic anxiety through increased consumerism, reasoning that if it all may be gone tomorrow, we might as well enjoy it today), praying (in hopes that divine intervention or mere time will allow us to avoid confronting the challenges before us), or preparing (packing "bugout" packs for a quick escape or stocking up on gold, guns, and canned food, as though the transformative moment we anticipate will be but a brief interlude, a bad winter storm that might trap us indoors for a few days or weeks but that will eventually melt away). None of these responses avert, nor even mitigate, the very threats that have elicited our apocalyptic anxiety in the first place. Buying an electric car doesn't solve the problem of a culture dependent on endless growth in a finite world; building a bunker to defend against the zombie hordes doesn't solve the growing inequities between the rich and poor; praying for deliverance from the trials of history doesn't change that we must live in the times in which we were born. Indeed, neither partying, nor preparing, nor praying achieves what should be the natural goal when we perceive a threat on the horizon: we should not seek to ignore it, or simply brace for it, but to avert it.

#### (B.) Nationalist framing of security makes it impossible to correctly assess problems & solutions, inevitably sparking militarist intervention and war.

Massumi 2011

Brian, professor in the communication department at the University of Montreal, The half-life of disaster, http://www.guardian.co.uk/commentisfree/2011/apr/15/half-life-of-disaster

Collective response does, of course, go on. But it takes the privileged form of a growing state security apparatus. The anti-terrorism doctrine of the US explicitly includes emergency response to natural disaster in its purview. All suddenly striking, unforeseen events that defy human logic and thus seem to substract themselves from the political sphere in its everyday functioning are lumped together in the same category, and together fall under the jurisdiction of a security apparatus that is continually growing new arms and extending old ones, weaving itself into a complex, tentacular network. The network is designed to enable seamless relay from civilian emergency response to military response. Hurricane Katrina, for example, was used by the Bush administration to break down the historical prohibition against the domestic deployment of national military force in America. A US National Guard was recalled from Iraq for service in Louisiana. When the fires were ravaging Greece in the summer of 2009, the Greek government declared the senseless, unforeseen disaster a terrorist threat, because it could not be ruled out that it had been the result of terrorist-connected arson. The army was called in. Tendencies such as these blur the boundary between the policing of civil society and the military sphere, and between natural activity, criminal activity, and acts of war. The distinction between civil society and the state of exception that is war is operationally blurred by the exercise of a "full-spectrum force" that is every much as diffuse and protean as the "threat environment" it purportedly secures. Measures suspending civil and political rights are extended and multiplied, and increasingly applied preemptively. The right to peaceful dissent suffers (witness the preemptive military-style tactics mobilised against peaceful demonstrators who had broken no law in Copenhagen at the climate talks in 2009 and at the G20 meeting in Toronto in 2010). Collective action is further restrained as the state of exception becomes the norm. The threat environment becomes an open field for autocratic intervention and arbitrary exercises of power operating on a continuum with military force. True to form, the nuclear disaster unfolding at the Fukushima reactor as a consequence of the earthquake and tsunami became "an opportunity for this pacifist nation to rely on its military at a level unseen since world war two," as the Japanese Self-Defense Forces are mobilised for civilian duty. Crucially, these developments are no longer legitimated in terms of political reason or reason of state. The blurring of the boundaries between war and peace, and the full-spectrum potential militarisation it fosters, is legitimated affectively, through the media-driven affective conversion circuit just described. In that affective logic, against the all-encompassing background of low-level fear, the tentacularly extending security apparatus appears as "natural" and as fateful as the events it is designed to respond to or preempt.

### Vtl

#### ---Security destroys value to life.

Der Derian 1998

James, professor of political science at Brown University, “The Value of Security: Hobbes, Marx, Nietzsche, and Baudrillard,” *On Security*, 1998, pgs. 7

The desire for security is manifested as a collective resentment of difference--that which is not us, not certain, not predictable. Complicit with a negative will to power is the fear-driven desire for protection from the unknown. Unlike the positive will to power, which produces an aesthetic affirmation of difference, the search for truth produces a truncated life which conforms to the rationally knowable, to the causally sustainable. In The Gay Science , Nietzsche asks of the reader: "Look, isn't our need for knowledge precisely this need for the familiar, the will to uncover everything strange, unusual, and questionable, something that no longer disturbs us? Is it not the instinct of fear that bids us to know? And is the jubilation of those who obtain knowledge not the jubilation over the restoration of a sense of security?"37¶ The fear of the unknown and the desire for certainty combine to produce a domesticated life, in which causality and rationality become the highest sign of a sovereign self, the surest protection against contingent forces. The fear of fate assures a belief that everything reasonable is true, and everything true, reasonable. In short, the security imperative produces, and is sustained by, the strategies of knowledge which seek to explain it. Nietzsche elucidates the nature of this generative relationship in The Twilight of the Idols :¶ The causal instinct is thus conditional upon, and excited by, the feeling of fear. The "why?" shall, if at all possible, not give the cause for its own sake so much as for a particular kind of cause --a cause that is comforting, liberating and relieving. . . . That which is new and strange and has not been experienced before, is excluded as a cause. Thus one not only searches for some kind of explanation, to serve as a cause, but for a particularly selected and preferred kind of explanation--that which most quickly and frequently abolished the feeling of the strange, new and hitherto unexperienced: the most habitual explanations.38

# 1NR

## Preemption

### No Cyber-War Impact

#### Their military planners empirically overstate risk.

**Healey, Atlantic Council Cyber Statecraft Initiative director, 2013**

(Jason, “No, Cyberwarfare Isn't as Dangerous as Nuclear War”, 3-20, <http://www.usnews.com/opinion/blogs/world-report/2013/03/20/cyber-attacks-not-yet-an-existential-threat-to-the-us>, ldg)

Eighty years ago, the generals of the U.S. Army Air Corps were sure that their bombers would easily topple other countries and cause their populations to panic, claims which did not stand up to reality. A study of the 25-year history of cyber conflict, by the Atlantic Council and Cyber Conflict Studies Association, has shown a similar dynamic where the impact of disruptive cyberattacks has been consistently overestimated. Rather than theorizing about future cyberwars or extrapolating from today's concerns, the history of cyberconflict that have actually been fought, shows that cyber incidents have so far tended to have effects that are either widespread but fleeting or persistent but narrowly focused. No attacks, so far, have been both widespread and persistent. There have been no authenticated cases of anyone dying from a cyber attack. Any widespread disruptions, even the 2007 disruption against Estonia, have been short-lived causing no significant GDP loss.

#### Zero impact to cyber arms race-consensus goes NEG

**Gray, Reading strategic studies professor, 2013**

(Colin, “Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling”, April, <http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1147.pdf>, ldg)

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.

### Flex Key

#### This turns the case – effective offense is the only way to have an effective defense

**Limnéll, NDU military science PhD, 2012**

(Jarno, “Offensive Cyber Capabilities Need to be Built and Exposed Because of Deterrence”, 10-9, <http://infosecisland.com/blogview/22534-Offensive-Cyber-Capabilities-Need-to-be-Built-and-Exposed-Because-of-Deterrence.html>, ldg)

First, if you want be a credible player both on the military battlefield and in world politics, you must have offensive capabilities, just as you must have defensive capabilities and the ability to be resilient. You simply cannot have a credible cyber defense without offensive abilities. Second, in order to achieve and raise your deterrence, you must possess offensive capabilities. The ability to act offensively includes a strong preventive message to others, provided they understand it and believe it. Offensive capabilities represent the key components of deterrence. Third, offensive thinking and building weaponry are vital in order to create a stronger and credible defense. With only “defensive thinking” you will not succeed. You have to understand how an attacker acts and you must try to find all possible vulnerabilities in your defense. You must also develop your defensive potential, by testing your current defense and training your forces. All this becomes much more efficient if you can test it with your own capabilities. Without the ability to act as an attacker, no country can build an effective and credible cyber defense.

### Solvency

#### The plan can’t solve – two warrants

#### A. Normsetting

#### Anonymity

**Goldsmith, Harvard law professor, 2013**

(Jack, “Cybersecurity Treaties A Skeptical View”, <http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf>, ldg)

James Lewis acknowledges that verification of compliance will not work, but he nonetheless thinks that cybersecurity treaties can promote cooperation. Even in the absence of compliance verification, he argues, “multilateral agreements could increase stability and reduce the risks of miscalculation or escalation by focusing on several specific areas: confidence-building and transparency measures, such as increased transparency in doctrine; creation of norms for responsible state behavior in cyberspace; and expansion of common understandings on the application of international law to cyber conflicts, or development of assurances on the use of cyberattacks.”26 The possibility of softer norms of this sort—whether embodied in a treaty or in a less formal document—is frequently mentioned, and the subject warrants a more extended discussion than I can here give it. My skepticism can be summarized as follows: in the absence of decent verification, we cannot be confident that transparency measures are in fact transparent, or that revealed doctrine is actual doctrine. Nor can norms get much purchase in a world without serious attribution and verification; anonymity is a norm destroyer.

## China//OCO Disad

### Overview

#### Lack of US cyber flexibility is the only scenario for Taiwan war – there are checks on every other threat now

**Rosecrance, Berkeley political science professor, 2010**

(Richard, “Delicately Poised: Are China and the US Heading for Conflict?” Global Asia 4.4, <http://www.globalasia.org/l.php?c=e251>, DOA: 10-2-12, ldg)

Finally, even on the question of Taiwan, which China believes is an indisputable part of its territory, it has adopted a policy of peaceful reunification. A country that handles territorial issues in such a manner is by no means expansionist. Third, China has relied on trade and investment for national welfare and prestige, instead of military conquest. And like the US, Japan and Germany, China has been very successful in this regard. In fact, so successful that it really sees no other option than to continue on this path to prosperity. Finally, after years of reforms, China increasingly finds itself sharing certain basic values with the US, such as a commitment to the free market, rule of law, human rights and democracy. Of course, there are still significant differences in terms of how China understands and practices these values. However, at a conceptual level, Beijing agrees that these are good values that it should strive to realize in practice. A Different World It is also important to note that certain changes in international relations since the end of World War II have made the peaceful rise of a great power more likely. To begin with, the emergence of nuclear weapons has drastically reduced the usefulness of war as a way to settle great power rivalry. By now, all great powers either have nuclear weapons or are under a nuclear umbrella. If the objective of great power rivalry is to enhance one’s interests or prestige, the sheer destructiveness of nuclear weapons means that these goals can no longer be achieved through military confrontation.

### Link Debate

#### Four links –

#### And you tank all cyber operations – even retaliatory operations are defined as offensive – prefer military statements

**Klobucher, SAP journalist, 2013**

(Derek, “U.S. Prepares Counterstrike Against Cyber-Attack”, 3-15, Forbes, <http://www.forbes.com/sites/sap/2013/03/15/u-s-prepares-counterstrike-against-cyber-attack/>, ldg)

In a departure for Alexander, the general not only discussed U.S. defense against cyber-attacks, but its offensive capacity, The New York Times reported Tuesday. Cyber Command will have 13 teams of digital warriors would counter-cyber-strike any nation to launch a major attack on American networks. “This team, this defend-the-nation team, is not a defensive team,” Alexander told the House Armed Services Committee. “This is an offensive team that the Defense Department would use to defend the nation if it were attacked in cyberspace.”

#### 3. Legal hurdles – limitations stem from other theaters-they won’t work for cyber and will hamper doctrine development.

**Kallberg, Cyber Security Research and Educational Center researcher, 2013**

(Jan, “Offensive Cyber: Superiority or Stuck in Legal Hurdles?”, 2-17, <http://works.bepress.com/cgi/viewcontent.cgi?article=1021&context=jan_kallberg>, ldg)

In recent years, offensive cyber operations have attracted significant interest from the non-Defense Department academic legal community, prompting numerous articles seeking to create a legal theory for cyber conflicts. Naturally, cyber operations should be used in an ethical way, but the hurdles generated by the legal community are staggering. At a time when the United States has already lost an estimated $4 trillion in intellectual property as a result of foreign cyber espionage, not to mention the loss of military advantage, focusing on what the United States cannot do in cyberspace only hinders efforts to defend the country from future cyber attack. The country is facing an enemy unrestrained by limitations, clearly visible in blatant cyber attacks on military networks, major banks and media outlets. Academics who question the legality of offensive counter cyber operations often have limited technical understanding of the unique characteristics of cyberspace. The theoretical framework for an emerging cyber law under development by the legal community uses analogies from international law, such as the laws of the high seas and international commercial air treaties. But these are highly inappropriate for the cyber domain. For example, the vast majority of these academic legal scholars would require the United States ensure that malicious software attack only combatant systems and legitimate military targets, and not affect any other systems. What these requirements ignore is the issue of control. Those digital bits easily can be copied and distributed, and targeting removed or redesigned. How can a coder control the duplication of the code? While code can be targeted to a specific military system, that is no guarantee it will be limited because of the dual use of information technology. There is no control of the code once it is released. The legal perception of cyber is based on an assumption that actors are either civilian or military, but there is no such clear distinction in the militarized and contested digital world. It is digital bits; in the same way that we cannot distinguish military air and civilian air. It is just air. In cyberspace, universities, municipal utilities, communication companies and other actors are a part of the war-fighting effort without clear boundaries to being civilian or military. If the U.S. became engaged in a cyber conflict with Hezbollah in southern Lebanon, an organization that is a mix of crude arms manufacturing, terrorism training and soup kitchens for the poor, there is no way to ensure that a counter cyber attack would not affect the soup kitchens. Second, to avoid the slightest collateral damage, the counter-attacker needs to be able to identify each computer in the counter-attacked network and verify its purpose. That requires full overview of the targeted system, maybe beyond even what the defending system administrators are aware of. The only way you can verify resources in another network is to pre-emptively gain access to their networks and gain targeting information. Third, international laws rely on territorial boundaries. The laws of the high sea are effective in international water. The national laws apply to territorial waters. But there is no territorial or international cyberspace as long as attribution is unsolved — and even with attribution solved, the answer to where, when and by whom is troublesome to answer. Applying laws of war that have origins in the 1800s, when massive armies fought on a field in broad daylight, in an abundance of object permanence, is not relevant to cyber when the contested space is changed, lost, created, reborn and redesigned in real time. Inferences about cyber operations made in published articles in the academic legal press are in many cases, to use a mild word, spurious. Retired Air Force Maj. Gen. Dale Meyerrose, former associate director of national intelligence, said in regard to offensive cyber operations, “Like everything else in cyber, our legal system is about 20 years behind.” The risk for the nation is tangible. The proposed legal hurdles evaporate the opportunity to successfully conduct offensive cyber as a soft policy option. The non-DoD academics’ legal theories on how to conduct cyberwar fail to recognize the human costs in the alternative: traditional kinetic warfare. The absence of relevant legal guidance creates confusion and undermines a coherent and systematic approach. Cyber can help the U.S. achieve political and military goals. These operations will require a legal framework based on the unique tenets of cyber to enable, not disable, American options and abilities.

#### 4. Notification – it kills effective cyber responses

**Dycus, Vermont law professor, 2010**

(Stephen, “Congress’s Role in Cyber Warfare”, 8-11, <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>, ldg)

Cyber weapons bear a striking resemblance to nuclear weapons in some important ways. An enemy’s cyber attack would, like a nuclear strike, probably come without a clear warning. There are as yet no reliable defenses against either a cyber attack or a nuclear attack. Collateral damage from a nuclear attack would almost certainly be very extensive and would linger for an extended period.48 The direct and indirect effects of a cyber attack, while different in kind and degree, still could be widespread and indiscriminate.49 In other ways, cyber weapons are critically different from their nuclear counterparts. For one thing, the time frame for response to a cyber attack might be much narrower. A nuclear weapon delivered by a land-based ICBM could take 30 minutes to reach its target. An electronic attack would arrive instantaneously, and leave no time to consult with or even inform anyone outside the executive branch before launching a counterstrike, if that were U.S. policy.