# 1nc

### 1nc

#### Authority means “authorization” – topical affirmatives must remove the permission to act, not just regulate the President

**Hohfeld,** Yale Law,19**19** (Wesley, <http://www.hku.hk/philodep/courses/law/HohfeldRights.htm>)

Many examples of legal powers may readily be given. Thus, X, the owner of ordinary personal property "in a tangible object" has the power to extinguish his own legal interest (rights, powers, immunities, etc.) through that totality of operative facts known as abandonment; and-simultaneously and correlatively-to create in other persons privileges and powers relating to the abandoned object,-e. g., the power to acquire title to the latter by appropriating it. Similarly, X has the power to transfer his interest to Y, that is to extinguish his own interest and concomitantly create in Y a new and corresponding interest. So also X has the power to create contractual obligations of various kinds. Agency cases are likewise instructive. By the use of some metaphorical expression such as the Latin, qui facit per alium, facit per se\* the true nature of agency relations is only too frequently obscured. The creation of an agency relation involves, inter alia, the grant of legal powers to the so-called agent, and the creation of correlative liabilities in the principal. That is to say, one party, P, has the power to create agency powers in another party, A,-for example, the power to convey P's property, the power to impose (so called) contractual obligations on P, the power to discharge a debt owing to P, the power to "receive" title to property so that it shall vest in P, and so forth. In passing, it may be well to observe that the term "authority," so frequently used in agency cases, is very ambiguous and slippery in its connotation. Properly employed in the present connection, the word seems to be an abstract or qualitative term corresponding to the concrete "authorization," the latter consisting of a particular group of operative facts taking place between the principal and the agent. All too often, however, the term in question is so used as to blend and confuse these operative facts with the powers and privileges thereby created in the agent. A careful discrimination in these particulars would, it is submitted, go far toward clearing up certain problems in the law of agency.

#### Restriction on authority must reduce permission to act

**Lobel, 8** - Professor of Law, University of Pittsburgh Law School (Jules, “Conflicts Between the Commander in Chief and Congress: Concurrent Power over the Conduct of War” 392 OHIO STATE LAW JOURNAL [Vol. 69:391, <http://moritzlaw.osu.edu/students/groups/oslj/files/2012/04/69.3.lobel_.pdf>)

So  too, the congressional power to declare or authorize war has been long held to permit Congress to authorize and wage a limited war—“limited in place, in objects, and in time.” 63 When Congress places such restrictions on the President’s authority to wage war, it limits the President’s discretion to conduct battlefield operations. For example, Congress authorized President George H. W. Bush to attack Iraq in response to Iraq’s 1990 invasion of Kuwait, but it confined the President’s authority to the use of U.S. armed forces pursuant to U.N. Security Council resolutions directed to force Iraqi troops to leave Kuwait. That restriction would not have permitted the President to march into Baghdad after the Iraqi army had been decisively ejected from Kuwait, a limitation recognized by President Bush himself.64

#### Voting issue – they destroy predictable limits – express delegations are finite and predictable; executive claims of authority are unlimited. They make every possible regulation of the President topical

### 1nc

#### The President should issue an Executive Order establishing a presumptive legal framework for offensive cyber operations based on the covert action statute.

#### Solves case and sets a durable precedent—restraint is better than legislation

**Brecher 2012** – JD 2013, University of Michigan Law School (December, Aaron P., Michigan Law Review, “NOTE: Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations”, 111 Mich. L. Rev. 423, Lexis)

The executive might also issue the proposed order, even though it would limit her freedom in some ways, because of the possible benefits of constraining future administrations or preempting legislative intervention. n149 For example, in this context, an administration may choose to follow the finding and reporting requirements in order to convince Congress that legislative intervention is unnecessary for proper oversight. This is acceptable if the covert action regime is in fact adequate on its own. Moreover, if greater statutory control over cyberattacks is needed, the information shared with Congress may give Congress the tools and knowledge of the issue necessary to craft related legislation. n150 Additionally, while executive orders are hardly binding, the inertia following adoption of an order may help constrain future administrations, which may be more or less trustworthy than the current one. Creating a presumption through an executive order also establishes a stable legal framework for cyberattacks that allows law to follow policy in this new field, and permits decisionmakers to learn more about the nature of cyberoperations before passing detailed statutes that may result in unintended consequences.

A presumption in favor of the title 50 regime for cyberattacks is also desirable because it comports with the reality of an executive constrained by its own internal processes. Though energy, dispatch, and secrecy are among the key advantages the executive possesses over Congress, n151 the existence of a professional bureaucratic corps, including many lawyers, within the executive branch can foster necessary deliberation about important policy decisions. n152 For issues on which there is disagreement among executive agencies, such as a potential turf war between the military and intelligence communities over control of cyberattacks, advisory and adjudicatory bodies such as the Office of Legal Counsel can play a constructive role. n153 Even on an issue such as the best legal regime to govern cyberattacks, which is essentially [\*449] a policy choice, the friction between different competing agencies itself can serve a checking function. n154

### 1nc

#### Obama’s pressuring the GOP with a strong display of Presidential strength and staying on message – the GOP will blink

**Dovere, 10/1/13** (Edward, Politico, “Government shutdown: President Obama holds the line”

<http://www.politico.com/story/2013/10/government-shutdown-president-obama-holds-the-line-97646.html?hp=f3>)

President Barack Obama started September in an agonizing, extended display of how little sway he had in Congress. He ended the month with a display of resolve and strength that could redefine his presidency.¶ All it took was a government shutdown.¶ This was less a White House strategy than simply staying in the corner the House GOP had painted them into — to the White House’s surprise, Obama was forced to do what he so rarely has as president: he said no, and he didn’t stop saying no.¶ For two weeks ahead of Monday night’s deadline, Obama and aides rebuffed the efforts to kill Obamacare with the kind of firm, narrow sales pitch they struggled with in three years of trying to convince people the law should exist in the first place. There was no litany of doomsday scenarios that didn’t quite come true, like in the run-up to the fiscal cliff and the sequester. No leaked plans or musings in front of the cameras about Democratic priorities he might sacrifice to score a deal.¶ After five years of what’s often seen as Obama’s desperation to negotiate — to the fury of his liberal base and the frustration of party leaders who argue that he negotiates against himself. Even his signature health care law came with significant compromises in Congress.¶ Instead, over and over and over again, Obama delivered the simple line: Republicans want to repeal a law that was passed and upheld by the Supreme Court — to give people health insurance — or they’ll do something that everyone outside the GOP caucus meetings, including Wall Street bankers, seems to agree would be a ridiculous risk.¶ “If we lock these Americans out of affordable health care for one more year,” Obama said Monday afternoon as he listed examples of people who would enjoy better treatment under Obamacare, “if we sacrifice the health care of millions of Americans — then they’ll fund the government for a couple more months. Does anybody truly believe that we won’t have this fight again in a couple more months? Even at Christmas?”¶ The president and his advisers weren’t expecting this level of Republican melee, a White House official said. Only during Sen. Ted Cruz’s (R-Texas) 21-hour floor speech last week did the realization roll through the West Wing that they wouldn’t be negotiating because they couldn’t figure out anymore whom to negotiate with. And even then, they didn’t believe the shutdown was really going to happen until Saturday night, when the House voted again to strip Obamacare funding.¶ This wasn’t a credible position, Obama said again Monday afternoon, but rather, bowing to “extraneous and controversial demands” which are “all to save face after making some impossible promises to the extreme right wing of their political party.”¶ Obama and aides have said repeatedly that they’re not thinking about the shutdown in terms of political gain, but the situation’s is taking shape for them. Congress’s approval on dealing with the shutdown was at 10 percent even before the shutters started coming down on Monday according to a new CNN/ORC poll, with 69 percent of people saying the House Republicans are acting like “spoiled children.”¶ “The Republicans are making themselves so radioactive that the president and Democrats can win this debate in the court of public opinion” by waiting them out, said Jim Manley, a Democratic strategist and former aide to Senate Majority Leader Harry Reid who has previously been critical of Obama’s tactics.¶ Democratic pollster Stan Greenberg said the Obama White House learned from the 2011 debt ceiling standoff, when it demoralized fellow Democrats, deflated Obama’s approval ratings and got nothing substantive from the negotiations.¶ “They didn’t gain anything from that approach,” Greenberg said. “I think that there’s a lot they learned from what happened the last time they ran up against the debt ceiling.”¶ While the Republicans have been at war with each other, the White House has proceeded calmly — a breakthrough phone call with Iranian President Hassan Rouhani Friday that showed him getting things done (with the conveniently implied juxtaposition that Tehran is easier to negotiate with than the GOP conference), his regular golf game Saturday and a cordial meeting Monday with his old sparring partner Israeli Prime Minister Benjamin Netanyahu.¶ White House press secretary Jay Carney said Monday that the shutdown wasn’t really affecting much of anything.¶ “It’s busy, but it’s always busy here,” Carney said. “It’s busy for most of you covering this White House, any White House. We’re very much focused on making sure that the implementation of the Affordable Care Act continues.”¶ Obama called all four congressional leaders Monday evening — including Boehner, whose staff spent Friday needling reporters to point out that the president hadn’t called for a week. According to both the White House and Boehner’s office, the call was an exchange of well-worn talking points, and changed nothing.¶ Manley advised Obama to make sure people continue to see Boehner and the House Republicans as the problem and not rush into any more negotiations until public outrage forces them to bend.¶ “He may want to do a little outreach, but not until the House drives the country over the cliff,” Manley said Monday, before the shutdown. “Once the House has driven the country over the cliff and failed to fund the government, then it might be time to make a move.”¶ The White House believes Obama will take less than half the blame for a shutdown – with the rest heaped on congressional Republicans.¶ The divide is clear in a Gallup poll also out Monday: over 70 percent of self-identifying Republicans and Democrats each say their guys are the ones acting responsibly, while just 9 percent for both say the other side is.¶ If Obama is able to turn public opinion against Republicans, the GOP won’t be able to turn the blame back on Obama, Greenberg said. “Things only get worse once things begin to move in a particular direction,” he said. “They don’t suddenly start going the other way as people rethink this.”

#### OCO’s are extremely controversial and require significant political capital

Costigan and Perry 12 (Sean S. – Senior adviser for the Emerging Security Challenges Working Group. In 2010 he was a visiting fellow at the University of Calcutta's Institute of Foreign Policy Studies, and Jake, “Cyberspaces and Global Affairs”, 2012, pg 12, Google Books)

Much less is known about the U.S. military's offensive cyber capabilities which remain highly classified. A recent report in the New York Times reveals that there has been a "huge increase in the sophistication of American cyberwarfare" tactics (Sanger and Markoff 2009). The most exotic innovations under consideration would enable a Pentagon programmer to surreptitiously enter a computer server in Russia or China, for example, and destroy a “botnet” — a potentially destructive program that commandeers infected machines into a vast network that can be clandestinely controlled — before it could be unleashed in the United States. Or American intelligence agencies could activate malicious code that is secretly embedded on computer chips when they are manufactured, enabling the United States to take command of an enemy’s computers by remote control over the Internet. That, of course, is exactly the kind of attack officials fear could be launched on American targets, often through Chinese-made chips or computer servers. Issues like government-sanctioned hacking of foreign networks and pre-emptive cyber operations were so thorny that the Bush administration concluded they lacked "the credibility or the political capital to deal with the subject" (Sanger and Markoff 2009).

#### It consumes his capital, undermines Democratic unity and prevents passing the debt ceiling

**Lillis, 9/7/13** (Mike, The Hill, “Fears of wounding Obama weigh heavily on Democrats ahead of vote”

Read more: http://thehill.com/homenews/house/320829-fears-of-wounding-obama-weigh-heavily-on-democrats#ixzz2gWiT9H8u

The prospect of wounding President Obama is weighing heavily on Democratic lawmakers as they decide their votes on Syria.¶ Obama needs all the political capital he can muster heading into bruising battles with the GOP over fiscal spending and the debt ceiling.¶ Democrats want Obama to use his popularity to reverse automatic spending cuts already in effect and pay for new economic stimulus measures through higher taxes on the wealthy and on multinational companies.¶ But if the request for authorization for Syria military strikes is rebuffed, some fear it could limit Obama's power in those high-stakes fights. ¶ That has left Democrats with an agonizing decision: vote "no" on Syria and possibly encourage more chemical attacks while weakening their president, or vote "yes" and risk another war in the Middle East.¶ “I’m sure a lot of people are focused on the political ramifications,” a House Democratic aide said.¶ Rep. Jim Moran (D-Va.), a veteran appropriator, said the failure of the Syria resolution would diminish Obama's leverage in the fiscal battles.¶ "It doesn't help him," Moran said Friday by phone. "We need a maximally strong president to get us through this fiscal thicket. These are going to be very difficult votes."

#### That causes default and will destroy the U.S. and global economy

**Davidson, 9/10/13** – co-founder of NPR’s Planet Money (Adam, “Our Debt to Society” New York Times, <http://www.nytimes.com/2013/09/15/magazine/our-debt-to-society.html?pagewanted=all>)

If the debt ceiling isn’t lifted again this fall, some serious financial decisions will have to be made. Perhaps the government can skimp on its foreign aid or furlough all of NASA, but eventually the big-ticket items, like Social Security and Medicare, will have to be cut. At some point, the government won’t be able to pay interest on its bonds and will enter what’s known as sovereign default, the ultimate national financial disaster achieved by countries like Zimbabwe, Ecuador and Argentina (and now Greece). In the case of the United States, though, it won’t be an isolated national crisis. If the American government can’t stand behind the dollar, the world’s benchmark currency, then the global financial system will very likely enter a new era in which there is much less trade and much less economic growth. It would be, by most accounts, the largest self-imposed financial disaster in history.¶ Nearly everyone involved predicts that someone will blink before this disaster occurs. Yet a small number of House Republicans (one political analyst told me it’s no more than 20) appear willing to see what happens if the debt ceiling isn’t raised — at least for a bit. This could be used as leverage to force Democrats to drastically cut government spending and eliminate President Obama’s signature health-care-reform plan. In fact, Representative Tom Price, a Georgia Republican, told me that the whole problem could be avoided if the president agreed to drastically cut spending and lower taxes. Still, it is hard to put this act of game theory into historic context. Plenty of countries — and some cities, like Detroit — have defaulted on their financial obligations, but only because their governments ran out of money to pay their bills. No wealthy country has ever voluntarily decided — in the middle of an economic recovery, no less — to default. And there’s certainly no record of that happening to the country that controls the global reserve currency.¶ Like many, I assumed a self-imposed U.S. debt crisis might unfold like most involuntary ones. If the debt ceiling isn’t raised by X-Day, I figured, the world’s investors would begin to see America as an unstable investment and rush to sell their Treasury bonds. The U.S. government, desperate to hold on to investment, would then raise interest rates far higher, hurtling up rates on credit cards, student loans, mortgages and corporate borrowing — which would effectively put a clamp on all trade and spending. The U.S. economy would collapse far worse than anything we’ve seen in the past several years.

### 1nc

#### Congressional restrictions cause adversaries to doubt the credibility of our threats --- causes crisis escalation

Matthew Waxman 8/25/13, Professor of Law @ Columbia and Adjunct Senior Fellow for Law and Foreign Policy @ CFR, “The Constitutional Power to Threaten War,” Forthcoming in Yale Law Journal, vol. 123, August 25, 2013, SSRN

A claim previously advanced from a presidentialist perspective is that stronger legislative checks on war powers is harmful to coercive and deterrent strategies, because it establishes easily-visible impediments to the President’s authority to follow through on threats. This was a common policy argument during the War Powers Resolution debates in the early 1970s. Eugene Rostow, an advocate inside and outside the government for executive primacy, remarked during consideration of legislative drafts that any serious restrictions on presidential use of force would mean in practice that “no President could make a credible threat to use force as an instrument of deterrent diplomacy, even to head off explosive confrontations.”178 He continued:¶ In the tense and cautious diplomacy of our present relations with the Soviet Union, as they have developed over the last twenty-five years, the authority of the President to set clear and silent limits in advance is perhaps the most important of all the powers in our constitutional armory to prevent confrontations that could carry nuclear implications. … [I]t is the diplomatic power the President needs most under the circumstance of modern life—the power to make a credible threat to use force in order to prevent a confrontation which might escalate.179

#### Effective cyberdeterrence key to future Chinese cyber aggression

Schmitt 13 (Gary, co-directs the Marilyn War Center for Security Studies at the American Enterprise Institute, “How to meet the threat from China's army of cyber guerrillas” June 06, 2013, Fox News)

When President Obama meets woth Chinese President Xi Jinping Friday and Saturday in Southern California, a major topic of conversation between the two will be Chinese cyber-attacks and cyber-espionage against American commercial and government targets. ¶ According to U.S. counterintelligence officials, billions upon billions of dollars worth of information has been “lifted” out of American computers and servers in recent years. ¶ In fact, only last week, newspapers were reporting that an internal Defense Department review had concluded that China had used cyber attacks to gather data on more than three dozen key U.S. military programs, including the country’s most advanced missile defense systems, naval warships and even the F-35 Joint Strike Fighter—the stealthy, fifth-generation jet **that will be the backbone of the American military’s ability to sustain air superiority in the decades ahead.**¶As one might expect, the Chinese government has denied any complicity in these attacks. And it is doubtful, given how successful Chinese efforts have been, that even “blunt” talk by the president to the new Chinese leader, will have much effect on Chinese practices.¶ The reality is, the Chinese government is engaged in a form of warfare—new to be sure in its technological aspects but not new in the sense that cyber attacks harm our relative military strength and damage the property (intellectual and proprietary) of citizens and companies alike.¶ So far, the American government’s response has largely been defensive, either talking to the Chinese about establishing new, agreed-upon “rules of road” for cyberspace or working assiduously to perfect new security walls to protect government and key private sector computer systems. ¶ Although neither effort should be abandoned, they are no more likely to work than, say, before World War II, the Kellogg-Briand Pact could outlaw war and the Maginot Line could protect France from an invading Germany.¶ This last point is especially important. When it comes to cyberspace, according to Cyber Command head and director of the National Security Agency, General Keith Alexander, those on the offensive side of the computer screen–that is, those hacking into or compromising computer systems–have the advantage over those on the defensive side who are trying to keep systems secure. Walls have always been breached and codes broken.¶ Moreover, attempts to beef up security are complicated by the fact that our own cyber warriors are undoubtedly reluctant to provide those charged with protecting systems here at home with the latest in their own capabilities. ¶ In addition to increasing the chance such information might leak by expanding the number of persons in the know, efforts to use that information to plug our own vulnerabilities can inadvertently alert a potential adversary on the very backdoors American would want to save for using in a future crisis or conflict.¶ All of which leads to the conclusion that to stem the tide of harmful cyber attacks by the Chinese (or, for that matter, Iran, Russia or North Korea), **there has to be a cyber response on America’s part that** deters continued cyber aggression**.** ¶Reprisals that are proportionate, in self-defense and designed to stop others from such behavior falls well within the bounds of international law as traditionally understood.¶ Nor is it the case that such reprisals should be limited to responding to government-on-government cyber attacks. The U.S. government has always understood that it has an affirmative duty to protect the lives and property of its citizens from foreign aggression and, in times both past and current, this has meant using American military might. ¶ That need not be the case here, however. Indeed, one advantage of the cyber realm is the wide variety of options it offers up for reprisal that can inflict economic harm without causing loss of life or limb.¶ The good news is that the U.S. government has been gradually beefing up its offensive cyber capabilities. ¶ Indeed, a little over a month ago in open testimony before the House Armed Services Committee, Gen. Alexander said that he created thirteen new teams that would go on the offensive if the nation were hit by a major cyber attack. And new reports coming out of the Pentagon indicate that the Joint Chiefs would like to empower geographic combatant commanders to counter cyber attacks with offensive cyber operations of their own.¶ These are necessary steps if we hope to create a deterrent to Chinese cyber aggression; however, they are not sufficient. ¶ The threat posed by China’s army of cyber “guerrillas” is constant, is directed at both the U.S. government and the private sector, and ranges from the annoying to the deadly serious. ¶ **A truly adequate response would require meeting the Chinese challenge on all these fronts**. And **no amount of summitry between the American and Chinese leaders** is likely to **substitute for the cold, hard fact that, when it comes to Chinese misbehavior,** upping the cost to Beijing is a necessary first step **to reclaiming the peaceful potential of the newest of the “great commons,” cyberspace.**

#### China will use cyber to take Taiwan

Hjortdal 11 (Magnus Hjortdal is a researcher asso ciated with CHINA-SEC, Centre for Military Studies at the University of Copenhagen. He ho lds an M.Sc. in Political Science from the University of Copenhagen and is owner of MH International Relations, which advise s private and public institutions, “China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence” Journal of Strategic Security , 4 (2): 1-24)

China's military strategy mentions cyber capabilities as an area that the People's Liberation Army (PLA) should invest in and use on a large scale. 13 The U.S. Secretary of Defense, Robert Gates, has also declared that China's development in the cyber area increasingly concerns him, 14 and that there has been a decade-long trend of cyber attacks emanating from China. 15¶ Virtually **all digital and electronic military systems can be attacked via cyberspace**. Therefore, it is essential for a state to develop capabilities in this area if it wishes to challenge the present American hegemony. The interesting question then is whether China is developing capabilities in cyberspace in order to deter the United States. 16¶ China's military strategists describe cyber capabilities as a powerful asymmetric opportunity in a deterrence strategy. 19 Analysts consider that an "important theme in Chinese writings on computer-network operations (CNO) is the use of computer-network attack (CNA) as the **spearpoint** of deterrence." 20 CNA increases the enemy's costs to become too great to engage in warfare in the first place, which Chinese analysts judge to be essential for deterrence. 21 This could, for example, leave China with the potential ability to deter the Unit ed States from intervening in a scenario concerning Taiwan. CNO is viewed as a focal point for the People's Liberation Army, but it is not clear how the actual capacity functions or precisely what condit ions it works under. 22¶ If a state with superpower potential (here China) is to create an opportunity to ascend militarily and politically in the international system, it would require an asymmetric deterrence capability such as that described here. 23¶ It is said that the "most significant computer network attack is characterized as a pre-emption weapon to be used under the rubric of the rising Chinese strategy of [...] gaining mastery before the enemy has struck." 24 Therefore, China, like other states seeking a similar capacity, has recruited massively within the hacker milieu inside China. 25 Increasing resources in the PLA are being allocated to develop assets in relation to cyberspace. 26 The improvements are visible: The PLA has established " information warfare " capabilities, 27 with a special focus on cyber warfare that, according to their doctrine, can be used in peacetime. 28 Strategists from the PLA advocate the use of virus and hacker attacks that can paralyze and surp rise its enemies. 29

#### That goes nuclear

**Glaser 11**, Professor of Political Science and International Affairs – George Washington University,

(Charles, “Will China’s Rise Lead to War?” *Foreign Affairs* Vol. 9 Iss. 2, March/April)

THE PROSPECTS for avoiding intense military competition and war may be good, but growth in China's power may nevertheless require some changes in U.S. foreign policy that Washington will find disagreeable--particularly regarding Taiwan. Although it lost control of Taiwan during the Chinese Civil War more than six decades ago, China still considers Taiwan to be part of its homeland, and unification remains a key political goal for Beijing. China has made clear that it will use force if Taiwan declares independence, and much of China's conventional military buildup has been dedicated to increasing its ability to coerce Taiwan and reducing the United States' ability to intervene. Because China places such high value on Taiwan and because the United States and China--whatever they might formally agree to--have such different attitudes regarding the legitimacy of the status quo, the issue poses special dangers and challenges for the U.S.-Chinese relationship, placing it in a different category than Japan or South Korea. A crisis over Taiwan could fairly easily escalate to nuclear war, because each step along the way might well seem rational to the actors involved. Current U.S. policy is designed to reduce the probability that Taiwan will declare independence and to make clear that the United States will not come to Taiwan's aid if it does. Nevertheless, the United States would find itself under pressure to protect Taiwan against any sort of attack, no matter how it originated. Given the different interests and perceptions of the various parties and the limited control Washington has over Taipei's behavior, a crisis could unfold in which the United States found itself following events rather than leading them. Such dangers have been around for decades, but ongoing improvements in China's military capabilities may make Beijing more willing to escalate a Taiwan crisis. In addition to its improved conventional capabilities, China is modernizing its nuclear forces to increase their ability to survive and retaliate following a large-scale U.S. attack. Standard deterrence theory holds that Washington's current ability to destroy most or all of China's nuclear force enhances its bargaining position. China's nuclear modernization might remove that check on Chinese action, leading Beijing to behave more boldly in future crises than it has in past ones. A U.S. attempt to preserve its ability to defend Taiwan, meanwhile, could fuel a conventional and nuclear arms race. Enhancements to U.S. offensive targeting capabilities and strategic ballistic missile defenses might be interpreted by China as a signal of malign U.S. motives, leading to further Chinese military efforts and a general poisoning of U.S.-Chinese relations.

### 1nc

#### the aff allows the government to deploy victimhood of 9/11 to wage wars and erases agency

**Faulkner, ‘8** professor at the University of New South Wales (Joanne Faulkner, Spring/Autumn 2008, “The Innocence of Victimhood Versus the “Innocence of Becoming”: Nietzsche, 9/11, and the “Falling Man,”” The Journal of Nietzsche Studies, Iss. 35/36)//CC

It would seem that there is very little about the events of the September 11, 2001, that has not already been said or imagined. Our understanding of these events, and especially the attacks on the Twin Towers, has been overdetermined by the seemingly endless repetition of (by now) iconic images: of planes perforating the clear, tranquil surface of those seemingly impenetrable buildings and thus opening a rupture in the Western consciousness, the reparation of which is not yet in sight. Other images also populate the post-9/11 memory: images of disbelief, of grief, and of bravery—especially with respect to the members of the New York Fire Department, who rose to the occasion of providing a sense of American resilience and fortitude, thus representing a possible future after the catastrophe. These images played a major role in enabling certain mainstream media groups in the United States to reconstruct a narrative concerning their particular place in the world and with respect to each other: a narrative about national character and identity, hope, fear, and desire. The images drawn on to illustrate this narrative were therefore of critical importance; what was needed was a strong and coherent picture of innocence: the innocence of those killed in the attacks, to be sure, but also of the American people more generally—who, after a brief period of tending to their wounds, would need to collect themselves and return to the everyday commerce of existence, secure in the belief that evil is radically external to their “way of life” and that their government will ultimately protect them.1 Such a narrative, however, also served to exclude images that could not support the specific requirements of its coherence: equivocal images that jar against our [End Page 67] sense of propriety, certainly now after the effects of repetition have etched within us a certain understanding of the experience of 9/11. But also, interestingly, just after the attacks and before the grooves of this understanding had been consolidated, spontaneous and diffuse acts of censorship regulated the kinds of experiences, fears, and decisions that the victims of the attacks could enact. This article addresses one such image, which proved to be disruptive of the limits of identity asserted immediately following 9/11: Richard Drew’s “Falling Man,” depicting an unknown victim of the attacks in midflight from the North Tower of the World Trade Center. This image complicates the very culturally specific notion of innocence that was invoked during the reconstruction of national identity following the terrorist attacks against America. In particular, it will be argued that the “falling man” compromised the vision of an innocence that solicits protection precisely because it is outside the sphere of action. The image represents a decision—a wild and hopeless decision but a decision nonetheless—that, from the perspective of a claim to innocence, conceived as passive and guiltless, is difficult to comprehend or acknowledge as a “proper” comportment of an innocent. The falling man reveals and embodies a traumatic horror, difficult to encounter: the horror of choosing the means of one’s own particular death in the face of a less certain but more protracted demise at the hands of another. This article argues for a reconsideration of “innocence” that might emphasize agency and creativity above morality and victimhood and in so doing hopes to promote an understanding of those who found themselves preferring to jump than to burn on that fateful morning. Conceptual development along these lines will also affect the concept of agency in accordance with Nietzsche’s critique of morality and metaphysics. The broader project to which this essay contributes is concerned with the manner in which the application of innocence to a group can serve to erode their political agency: governments thus soothe our civic conscience while also establishing a mandate of protection in relation to their citizens. The events of 9/11 precipitated a shift from innocence to victimhood and, finally, to a loss of civil liberties for populations across the “West,” not only in the United States. It is therefore imperative to disrupt this equation of innocence with helplessness and to restore agency to the victims of terrorism and citizens alike. In response to antidemocratic policies enacted by governments after 9/11, much political theory has orbited about the constellation of Giorgio Agamben and Carl Schmitt, with Nietzsche lurking in the background as a conceptual precursor to Schmitt’s friend/enemy motif (Z:1 “Of the Friend”).2 We have therefore latterly seen an emphasis placed on the sovereign decision of the executive, the state of exception, and this in turn enlarges the sense that citizens of democracies are politically disempowered. In this context, the falling man is emblematic of the manner in which we might rework the concept of agency [End Page 68] to empower victims and those whose range of choices is limited. This kind of move is necessary, I contend, if the sense of hopelessness and futility that increasingly accompanies political subjectivity in Western democracies might be alleviated and a space for civil creativity might be opened. The essay will proceed by providing an account of the juridical or moral (Judeo-Christian) understanding of innocence and interrogating its conceptual relation to agency and belongingness to the political community. An alternative account of innocence—drawn from an interpretation of Nietzsche’s concept of the “innocence of becoming”—is then considered, through which the memory of the falling man might perhaps be redeemed. The article’s primary question thus concerns how this latter account might assist us in a revaluation of the falling man as innocent and of the “innocent” as capable of moral decision making and political participation.

#### the only way to achieve meaningful existence is to accept that violence and chaos are inevitable.

**Scott—90** (Charles E., professor of Philosophy at Pennsylvania State University, “The Question of Ethics: Nietzsche, Foucault, Heidegger,” Ed. John Sallis, p. 173-174)

One pathogenic aspect of our Western ethos that we have followed is the ascetic ideal. It is characterized by many types of refusal and denial regarding the manner in which human life occurs, and on Nietzsche's account the ascetic ideal reinforces this denial with a habitual insistence on the continuous presence of meaning in all dimensions of life and being. In our ascetic withdrawal from life we join forces with hopelessness, suffering, death, and helplessness by giving them meaning, in our appropriation of them, that far exceeds their occurrence and that subordinates them within a scheme of meaning and hope. The rule governing the ascetic ideal is found in its incorporation and blind expression of the hopelessness and meaninglessness that it is designed to overcome. This incorporation of what it is constitutes the ideal's nihilism for Nietzsche: the affirmations within the ascetic ideal project their opposites and produce a spiral of unwitting and inevitable violence in the spirituality that they create. The denial of life within the boundaries of the ascetic ideal continuously reestablishes the power of the ideal. But when this movement is broken by a self-overcoming like that in Nietzsche's genealogy of the ascetic ideal, the rule of the ascetic ideal is interrupted and a possibility is opened for life-affirmations that do not suppress the most fearful occurrences involved in being alive. The joyousness of life without the illusion of continuous meaning, the joyousness that Nietzsche found in early Greek culture, was lost, according to his reading, in the course of the increasing cultural dominance of those whose nerve has failed before the disheartening flow of life. The ascetic ideal expresses this failure in its insistence on meaning and in its persistent manufacture of hope out of illusions bred of the failure. Heidegger is perhaps at his most non-Nietzschean point when in his Rector's address he turns to the Greek division between the everyday and the question of being. This is an ironic moment in Heidegger's thought: he traces the origins of his own move to separate the future of the German university from the German Volkstum, (that is, from dominant popular culture) to the emergence of the separation of thought from everyday life in Greek culture. But this move is not associated with the joyousness that Nietzsche uses as his reference in delimiting the ascetic ideal. According to Nietzsche's genealogy we have lost an earthly affirmation of life in the midst of the specific suffering of everyday existence. Nietzsche countenances fully the brutality, the fateful shattering of hope, the disappointments that break people's lives, the individual and social tragedies. The debilitation of minds and bodies is juxtaposed to people's savoring food and drink, enjoying sexual pleasure. It is juxtaposed to friendship, the energy of ambition, the struggle between competitors, the mixture of desperation and exhilaration in efforts of accomplishment. Nietzsche's move is toward affirmation in the midst of chaotic living when he speaks of what is lost in the blind and self-deceived chaos of asceticism that is ordered by the illusion of continuous meaning. In this affirmation one has an awareness, presumably a full awareness, of the otherness to human interest that radically distresses us. People's attention is delimited by it. Rather than escape or turn away from it, people are delimited by it in their relations with things. Rather than appropriate the suffering of life in ascetic self-denial, human beings stand over against its otherness, its unthinkableness, its density. They need not attempt to embody it in forms that seem to shape it to human and thinkable dimensions. They live in the inappropriable, meaningless dark vacuity, with it and other to it, out of it and in it. They are angel and animal, Nietzsche said. Not to be lost, not to be redeemed, not to be overcome, it is juxtaposed to a will to live, an affirmation with, and not in spite of, the chaos.

#### choose death in the face of inevitability – your ballot allows you to reclaim agency

**Faulkner, ‘8** professor at the University of New South Wales (Joanne Faulkner, Spring/Autumn 2008, “The Innocence of Victimhood Versus the “Innocence of Becoming”: Nietzsche, 9/11, and the “Falling Man,”” The Journal of Nietzsche Studies, Iss. 35/36)//CC

Most significantly, for the purposes of this essay, we can perhaps see now how for Nietzsche agency is compatible with innocence. Indeed, innocence—regarded as what is unsullied by moral thinking—is integral to the skillful exercise of agency. Understood in these terms, innocence is neither a precious ideal to be protected from the forces of chance nor a moralistic instrument for the meting of punishment to those who threaten society. Rather, innocence is conceived as a style of existence that becomes active by claiming to itself what chance throws up before it. Innocence would here suggest a resistance to passivity and victimhood and a choice to take part in the inevitability of the moment—even if this agency ultimately extinguishes the subject through which it is performed. Perhaps at this point, then, we might attempt a return to the acts of the 9/11 jumpers, who in the light of the above can be understood as agents of their own demise but in a manner that nonetheless does not compromise their innocence.

The visions of falling bodies from the Twin Towers do not sit well with orthodox imagery surrounding 9/11 because they invoke an uncomfortable ambiguity with respect to their victim status. In their final moments of animation and on the precipice of death, these bodies occupy a middle space between life and death that renders us uncomfortable in our own mortality. But they also mark a cleavage between innocence and guilt: their decision to seize the opportunity to escape confinement within their smoky “tombs” signals a confusing complicity with the terrorists who had perpetrated the attacks. In the terms that Nietzsche (and Spinoza) set out above, the jumpers took an active part in the causes that led to their deaths—causes that originate in a terrorist plot against America. And in the eyes of some, this exposed them as irresolute, and even disloyal, in the face of what later emerged to be a monumental national threat.

In theological terms also—and keeping in mind the religious frame through which many in the United States view global politics—Drew’s photograph, especially, resonates with a near-godly defiance of death: the subject’s fall can be read as the taking of a liberty against God, who claims a privilege with respect to determining who lives or dies. The image may thus evoke to the viewing public humanity’s primal scene and the original sin that it demonstrates: the [End Page 80] taking of the fruit of knowledge that marks a new beginning for humanity. Even the photograph’s title would seem to suggest a proximity to the guilt through which humanity is engendered, by means of its irreparable separation from innocence. Likewise, its subject is separated from the other victims of the attacks who (more appropriately) awaited divine sanction on their lives and have thus continued to be redeemed (drawn back into the community’s fold) by means of the various ceremonies and purification rites since performed at Ground Zero. The resigned posture of the subject of “The Falling Man” surely gives the viewer pause: it looks like a suicide attempt, and the suicide cannot be connected to a redemptive innocence. Yet, according to Nietzsche’s refiguring of agency, the decision to die can be reconciled with innocence: and moreover, innocence comes to be the very condition of an agency—as opposed to (fictitious) free will—an agency that, rather, refuses the moralizing economy of guilt and punishment.

The decision to jump hundreds of meters to one’s death from a burning building might seem a limited, and somewhat undesirable, instance of agency. Clearly, it is a choice these people would not have made on any other morning and in any other circumstance. In the light of Nietzsche’s account of agency as conditioned by context and circumstance, however, it is possible to count the jumpers among the innocents lost to 9/11—and to do so in full recognition of their specific choice to take their lives into their own hands. In the context of Nietzsche’s innocence of becoming, we may understand innocence as a suspension of moral judgment rather than as prior to (and separate from) social existence. Nietzschean innocence emerges from within existence and gives rise to an agency that responds to the chance necessities life occasions. Likewise, the innocence of becoming is not grounded in opposition to guilt but, rather, undercuts the understanding of social relations in terms of guilt and debt. For this reason, Nietzsche’s innocence of becoming furnishes the jumpers’ decision with a sense that would be otherwise unavailable, at least within the narrow parameters according to which moral action and worth are conventionally adjudged.

In the absence of an acknowledgment of the jumpers’ choice (and of the possibility of making a decision to die in one’s own way, where the choice to live is unavailable), we will continue to misunderstand their relationship to these events and thus to limit their political agency. In the context of the 9/11 attacks, the innocent—understood through the vista of Judeo-Christian moral tradition—has become an eternally aggrieved icon of national identity: a perennially threatened and victimized creature of ressentiment who “in order to exist first needs a hostile external world” (GM I:10).32 Although it is important to acknowledge the suffering of those affected, and this may indeed include the nation as a whole, what Nietzsche’s innocence of becoming reveals is that the relationship to one’s suffering is far from straightforward. If we subscribe too readily to the status of innocent-to-be-protected—thus recoiling from suffering and requiring that the [End Page 81] debts of enemies be paid in full—then we also deny the possibility of freedom opened by the affirmation of becoming. And such a predicament is all too well reflected in the erosion of civil liberties that is ongoing since the end of 2001 in the United States and elsewhere.

But were we to allow ourselves to imagine being trapped within those buildings and to contemplate the possibility that one might still make a choice, perhaps identification with the falling man might open the citizen to a new kind of agency in relation to government and nationhood. Remembering that the imagination furnishes us with knowledge of our situation—by means of the traces of interactions impressed upon memory—then we are able to develop a capacity for agency by using our imaginations to understand the decisions of those who have lived through what we have not. Through the rubric offered by the jumper’s predicament, we might then imagine a mode of resistance against attack, wherein strength is reappropriated from the enemy—even in death. Our reinterpretation of the falling man as innocent thus allows for a conception of freedom with respect to the chance events that constrain action. But moreover, it also allows us to develop a resistance to governments’ attempts to render us passive subjects by means of the moral mantle of innocence by which we are both idealized and contained. Such a modest and situated exercise of agency would involve attentiveness to the diffuse and unexpected opportunities that arise in one’s locality, to actively participate in the causes of change. For instance, one could organize a demonstration, write letters to political representatives and newspapers, meet with others who share one’s values, walk to work, or recycle.

Each of these activities, however humble or ambitious, contributes to the determination of life and prevents one being the mere passive object of external causes—disempowered and separated from agency. Such attunement to one’s situation, however, requires above all engaging one’s imagination: the site of ethical understanding—of what empowers the body and what the body should avoid. In this vein, we might reimagine the falling man as a figure of the active resistance that Nietzsche’s innocence of becoming teaches. And we can understand his final act of agency as such, without casting him out of the sanctum of human virtue. With respect to this reinterpretation of innocence, as a sensitivity to the specific opportunities that life grants, I will leave the last word to one who, mourning the loss of his wife, finds it within himself to understand her final decision: “Whether she jumped, I don’t know. I hoped that she had succumbed to the smoke but it doesn’t seem likely. In some ways it might just be the last element of control, that everything around you is happening and you can’t stop it, but this is something you can do. To be out of the smoke and the heat, to be out in the air … it must have felt like flying.”33 [End Page 82]

### 1nc

The United States Department of Defense, with executive agencies, should provide a substantial number of employment-based visas to computer security specialists who will provide service to the United States Cyber Command. The Department of Defense, with executive agencies, should announce that it will double the salary of any competing offer for any qualified applicant to the United States Cyber Command.

#### Counterplan solves effective cybersecurity

**Haddick**, 8/6/**2010** (Robert - editor of Small Wars Journal, Uncle Sam Wants You…Whoever You Are, Foreign Policy, p. http://www.foreignpolicy.com/articles/2010/08/06/this\_week\_at\_war\_uncle\_sam\_wants\_you\_whoever\_you\_are)

Writing in Small Wars Journal, Gregory Conti and Jen Easterly, both U.S. Army lieutenant colonels, discussed the problems the military faces recruiting "cyber warriors" into the newly created Cyber Command, which aims to "conduct full-spectrum military cyberspace operations in order to ... ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries." Yet Conti and Easterly note that Cyber Command will recruit from an already tiny pool of cybersavvy talent, a pool made even smaller by Cyber Command's requirement that its soldiers pass security clearances, polygraph examinations, and drug screening. Meanwhile, Cyber Command will have to compete with the likes of Google for talented techies who may not find military culture all that inviting. It should come as no surprise to eventually find Cyber Command mostly staffed by highly-paid civilian contractors rather than uniformed soldiers or career civil servants. Cyber Command's recruiting difficulties are a microcosm of the broader troubles the military, especially the Army, now faces. The all-volunteer military has been a success and should be retained. But evidence continues to mount that the Army has grown as big as it can under the all-volunteer system. If circumstances ever required a significantly larger Army, Army leaders and U.S. society would have to get used to an Army of much lower quality at the margin. Deploying such a force, especially into stability operations, would entail taking greater risks and paying higher costs. The recently released Quadrennial Defense Review (QDR) Independent Panel report called for an overhaul in the military's personnel system. The report concluded that compensation costs for the all-volunteer force have exploded and are no longer sustainable. Active-duty head count has declined from 2 million in 1991 to 1.37 million in 2009. Yet in spite of this 32 percent decline in head count, military personnel costs (in constant 2005 dollars) have grown from $122 billion in 1991 to $130 billion in 2009 ($60,939 per head in 1991 versus $94,533 per head in 2009, adjusted for inflation). Even with this vast expansion in soldier compensation, the Army has had to reduce enlistment standards to fill its ranks. According to the QDR Independent Panel, these reduced standards include raising the maximum enlistment age to 42; accepting more recruits without high school diplomas, with criminal records, and in Category IV (low mental aptitude) on the Armed Forces Qualification Test; and increasing the numbers of noncitizens serving. The overall population of the United States is growing, but the cohort qualified and willing to volunteer for military service is shrinking. (Seventy-five percent of American youth are ineligible for military service for physical, mental, or educational reasons, or due to criminal records.) The prime recruiting base seems to be narrowing by geographic area and to families of veterans, increasingly turning military service into a "family guild." Immediately after taking office, Defense Secretary Robert Gates directed the Army and Marine Corps to increase their headcounts in response to the pressures of Iraq and Afghanistan. Regrettably, this decision collided with the evaporating pool of suitable military recruits. The Army recently released a report that studied suicide prevention and the Army's mental-health issues. The report revealed a broader range of rising high-risk behaviors and criminality in the Army's ranks. Part, maybe most, of the increasing incidence of suicide in the Army is related to the strain of wartime deployments. But the report noted that 68 of the 120 suicides (57 percent) the Army suffered during the first half of 2010 were to soldiers who had zero or one deployment. Over the past five years, the Army has suffered from increasing rates of discipline problems, crime, and drug use. The suicide prevention report noted that during this time, enlistment waivers increased and soldiers who previously would have been dismissed during initial training for unsuitability were instead retained, presumably due to the requirement to increase the Army's head count. Indeed, the Army calculated that one-third of the soldiers recruited to meet the Army's higher end-strength would have been dismissed from the service under the previous quality standards. It seems highly likely that the Army's retention of soldiers it would previously have found unsuitable for service is related to the increased suicide rate, along with other behavior problems. Thus, in spite of sharply increased (and in my view, well-deserved) compensation, the Army has reached an upper boundary on its size -- unless Army leaders and the country are willing to accept rapidly declining quality and rapidly increasing trouble at the margin. The increasing U.S. population is not offsetting the declining propensity to volunteer for military service or the shrinking percentage of the youth cohort medically, mentally, or socially qualified to serve. If the Army has reached the bottom of its U.S.-based recruiting pool, where could it go for additional manpower if it needed to? The U.S. military has a long tradition of recruiting non-citizens into its ranks. This would be a tempting option for expansion although language, culture, and security clearance problems place limits on its use. Instead, foreign auxiliary forces, organized, trained, and equipped by U.S. special operations forces, are likely to be used to supplement deployed U.S. forces, especially during long low-intensity stabilization operations.

### 1nc oversight

#### Cyber war infeasible and critical infrastructure is safe – takes out both advantages

Clark, MA candidate – Intelligence Studies @ American Military University, senior analyst – Chenega Federal Systems, 4/28/’12 (Paul, “The Risk of Disruption or Destruction of Critical U.S. Infrastructure by an Offensive Cyber Attack,” American Military University)

The Department of Homeland Security worries that our critical infrastructure and key resources (CIKR) may be exposed, both directly and indirectly, to multiple threats because of CIKR reliance on the global cyber infrastructure, an infrastructure that is under routine cyberattack by a “spectrum of malicious actors” (National Infrastructure Protection Plan 2009). CIKR in the extremely large and complex U.S. economy spans multiple sectors including agricultural, finance and banking, dams and water resources, public health and emergency services, military and defense, transportation and shipping, and energy (National Infrastructure Protection Plan 2009). The disruption and destruction of public and private infrastructure is part of warfare, without this infrastructure conflict cannot be sustained (Geers 2011). Cyber-attacks are desirable because they are considered to be a relatively “low cost and long range” weapon (Lewis 2010), but prior to the creation of Stuxnet, the first cyber-weapon, the ability to disrupt and destroy critical infrastructure through cyber-attack was theoretical. The movement of an offensive cyber-weapon from conceptual to actual has forced the United States to question whether offensive cyber-attacks are a significant threat that are able to disrupt or destroy CIKR to the level that national security is seriously degraded. It is important to understand the risk posed to national security by cyber-attacks to ensure that government responses are appropriate to the threat and balance security with privacy and civil liberty concerns. The risk posed to CIKR from cyber-attack can be evaluated by measuring the threat from cyber-attack against the vulnerability of a CIKR target and the consequences of CIKR disruption. As the only known cyber-weapon, Stuxnet has been **thoroughly analyzed** and **used as a model** for predicting future cyber-weapons. The U.S. electrical grid, a key component in the CIKR energy sector, is a target that has been analyzed for vulnerabilities and the consequences of disruption predicted – the electrical grid has been used in multiple attack scenarios including a classified scenario provided to the U.S. Congress in 2012 (Rohde 2012). Stuxnet will serve as the weapon and the U.S. electrical grid will serve as the target in this risk analysis that concludes that there is a low risk of disruption or destruction of critical infrastructure from a an offensive cyber-weapon because of the complexity of the attack path, the limited capability of non-state adversaries to develop cyber-weapons, and the existence of multiple methods of mitigating the cyber-attacks. To evaluate the threat posed by a Stuxnet-like cyber-weapon, the complexity of the weapon, the available attack vectors for the weapon, and the resilience of the weapon must be understood. The complexity – how difficult and expensive it was to create the weapon – identifies the relative cost and availability of the weapon; inexpensive and simple to build will be more prevalent than expensive and difficult to build. Attack vectors are the available methods of attack; the larger the number, the more severe the threat. For example, attack vectors for a cyberweapon may be email attachments, peer-to-peer applications, websites, and infected USB devices or compact discs. Finally, the resilience of the weapon determines its availability and affects its usefulness. A useful weapon is one that is resistant to disruption (resilient) and is therefore available and reliable. These concepts are seen in the AK-47 assault rifle – a simple, inexpensive, reliable and effective weapon – and carry over to information technology structures (Weitz 2012). The evaluation of Stuxnet identified malware that is “unusually complex and large” and required code written in multiple languages (Chen 2010) in order to complete a variety of specific functions contained in a “vast array” of components – **it is one of the most complex threats ever analyzed by Symantec** (Falliere, Murchu and Chien 2011). To be successful, Stuxnet required a **high** **level of technical knowledge across multiple disciplines**, a laboratory with the target equipment configured for testing, and a foreign intelligence capability to collect information on the target network and attack vectors (Kerr, Rollins and Theohary 2010). The malware also needed careful monitoring and maintenance because it could be easily disrupted; as a result Stuxnet was developed with a high degree of configurability and was upgraded multiple times in less than one year (Falliere, Murchu and Chien 2011). Once introduced into the network, the cyber-weapon then had to utilize four known vulnerabilities and four unknown vulnerabilities, known as zero-day exploits, in order to install itself and propagate across the target network (Falliere, Murchu and Chien 2011). Zero-day exploits are **incredibly difficult to find** and fewer than twelve out of the 12,000,000 pieces of malware discovered each year utilize zero-day exploits and this rarity makes them valuable, zero-days can fetch $50,000 to $500,000 each on the black market (Zetter 2011). The use of four rare exploits in a single piece of malware is “unprecedented” (Chen 2010). Along with the use of four unpublished exploits, Stuxnet also used the “first ever” programmable logic controller rootkit, a Windows rootkit, antivirus evasion techniques, intricate process injection routines, and other complex interfaces (Falliere, Murchu and Chien 2011) all **wrapped up in “layers of encryption** like Russian nesting dolls” (Zetter 2011) – including custom encryption algorithms (Karnouskos 2011). As the malware spread across the now-infected network it had to utilize additional vulnerabilities in proprietary Siemens industrial control software (ICS) and hardware used to control the equipment it was designed to sabotage. Some of these ICS vulnerabilities were published but some were unknown and **required such a high degree of inside knowledge** that there was speculation that a Siemens employee had been involved in the malware design (Kerr, Rollins and Theohary 2010). The unprecedented technical complexity of the Stuxnet cyber-weapon, along with the extensive technical and financial resources and foreign intelligence capabilities required for its development and deployment, indicates that the malware was likely developed by a nation-state (Kerr, Rollins and Theohary 2010). Stuxnet had very limited attack vectors. When a computer system is connected to the public Internet a host of attack vectors are available to the cyber-attacker (Institute for Security Technology Studies 2002). Web browser and browser plug-in vulnerabilities, cross-site scripting attacks, compromised email attachments, peer-to-peer applications, operating system and other application vulnerabilities are all vectors for the introduction of malware into an Internetconnected computer system. Networks that are not connected to the public internet are “air gapped,” a technical colloquialism to identify a physical separation between networks. Physical separation from the public Internet is a common safeguard for sensitive networks including classified U.S. government networks. If the target network is air gapped, infection can only occur through physical means – an infected disk or USB device that **must be physically introduced** into a possibly access controlled environment and connected to the air gapped network. The first step of the Stuxnet cyber-attack was to initially infect the target networks, a difficult task given the probable disconnected and well secured nature of the Iranian nuclear facilities. Stuxnet was introduced via a USB device to the target network, a method that suggests that the attackers were familiar with the configuration of the network and knew it was not connected to the public Internet (Chen 2010). This assessment is supported by two rare features in Stuxnet – having all necessary functionality for industrial sabotage fully embedded in the malware executable along with the ability to self-propagate and upgrade through a peer-to-peer method (Falliere, Murchu and Chien 2011). Developing an understanding of the target network configuration was a significant and daunting task based on Symantec’s assessment that Stuxnet repeatedly targeted a total of five different organizations over nearly one year (Falliere, Murchu and Chien 2011) with physical introduction via USB drive being the only available attack vector. The final factor in assessing the threat of a cyber-weapon is the resilience of the weapon. There are two primary factors that make Stuxnet **non-resilient**: the complexity of the weapon and the complexity of the target. Stuxnet was highly customized for sabotaging specific industrial systems (Karnouskos 2011) and needed a large number of very complex components and routines in order to increase its chance of success (Falliere, Murchu and Chien 2011). The **malware required eight vulnerabilities** in the Windows operating system **to succeed** and therefore would have failed if those vulnerabilities had been properly patched; four of the eight vulnerabilities were known to Microsoft and subject to elimination (Falliere, Murchu and Chien 2011). Stuxnet also required that two drivers be installed and required two stolen security certificates for installation (Falliere, Murchu and Chien 2011); driver installation would have failed if the stolen certificates had been revoked and marked as invalid. Finally, the configuration of systems is ever-changing as components are upgraded or replaced. There is no guarantee that the network that was mapped for vulnerabilities had not changed in the months, or years, it took to craft Stuxnet and successfully infect the target network. Had specific components of the target hardware changed – the targeted Siemens software or programmable logic controller – the attack would have failed. Threats are less of a threat when identified; this is why zero-day exploits are so valuable. Stuxnet went to great lengths to hide its existence from the target and utilized multiple rootkits, data manipulation routines, and virus avoidance techniques to stay undetected. The malware’s actions occurred only in memory to avoid leaving traces on disk, it masked its activities by running under legal programs, employed layers of encryption and code obfuscation, and uninstalled itself after a set period of time, all efforts to avoid detection because its authors knew that detection meant failure. As a result of the complexity of the malware, the changeable nature of the target network, and the chance of discovery, Stuxnet is not a resilient system. It is a fragile weapon that required an investment of time and money to constantly monitor, reconfigure, test and deploy over the course of a year. There is concern, with Stuxnet developed and available publicly, that the world is on the brink of a storm of highly sophisticated Stuxnet-derived cyber-weapons which can be used by hackers, organized criminals and terrorists (Chen 2010). As former counterterrorism advisor Richard Clarke describes it, there is concern that the technical brilliance of the United States “has created millions of potential monsters all over the world” (Rosenbaum 2012). Hyperbole aside, technical knowledge spreads. The techniques behind cyber-attacks are “constantly evolving and making use of lessons learned over time” (Institute for Security Technology Studies 2002) and the publication of the Stuxnet code may make it easier to copy the weapon (Kerr, Rollins and Theohary 2010). **However**, this is something of a zero-sum game because knowledge works both ways and cyber-security techniques are also evolving, and “understanding attack techniques more clearly is the first step toward increasing security” (Institute for Security Technology Studies 2002). Vulnerabilities are discovered and patched, intrusion detection and malware signatures are expanded and updated, and monitoring and analysis processes and methodologies are expanded and honed. Once the element of surprise is lost, weapons and tactics are less useful, this is the core of the argument that “uniquely surprising” **stratagems like Stuxnet are single-use**, like Pearl Harbor and the Trojan Horse, the “very success [of these attacks] precludes their repetition” (Mueller 2012). This paradigm has already been seen in the “son of Stuxnet” malware – named Duqu by its discoverers – that is based on the same modular code platform that created Stuxnet (Ragan 2011). With the techniques used by Stuxnet now known, other variants such as Duqu are being discovered and countered by security researchers (Laboratory of Cryptography and System Security 2011). It is obvious that the effort required to create, deploy, and maintain Stuxnet and its variants is massive and it is not clear that the rewards are worth the risk and effort. Given the location of initial infection and the number of infected systems in Iran (Falliere, Murchu and Chien 2011) it is believed that Iranian nuclear facilities were the target of the Stuxnet weapon. A significant amount of money and effort was invested in creating Stuxnet but yet the expected result – assuming that this was an attack that expected to damage production – was minimal at best. Iran claimed that Stuxnet caused only minor damage, probably at the Natanz enrichment facility, the Russian contractor Atomstroyeksport reported that no damage had occurred at the Bushehr facility, and an unidentified “senior diplomat” suggested that Iran was forced to shut down its centrifuge facility “for a few days” (Kerr, Rollins and Theohary 2010). Even the most optimistic estimates believe that Iran’s nuclear enrichment program was only delayed by months, or perhaps years (Rosenbaum 2012). The actual damage done by Stuxnet is not clear (Kerr, Rollins and Theohary 2010) and the primary damage appears to be to a higher number than average replacement of centrifuges at the Iran enrichment facility (Zetter 2011). Different targets may produce different results. The Iranian nuclear facility was a difficult target with limited attack vectors because of its isolation from the public Internet and restricted access to its facilities. What is the probability of a successful attack against the U.S. electrical grid and what are the potential consequences should this critical infrastructure be disrupted or destroyed? An attack against the electrical grid is a reasonable threat scenario since power systems are “a high priority target for military and insurgents” and there has been a trend towards utilizing commercial software and integrating utilities into the public Internet that has “increased vulnerability across the board” (Lewis 2010). Yet the increased vulnerabilities are mitigated by an increased detection and deterrent capability that has been “honed over many years of practical application” now that power systems are using standard, rather than proprietary and specialized, applications and components (Leita and Dacier 2012). The security of the electrical grid is also enhanced by increased awareness after a smart-grid hacking demonstration in 2009 and the identification of the Stuxnet malware in 2010; as a result the public and private sector are working together in an “unprecedented effort” to establish robust security guidelines and cyber security measures (Gohn and Wheelock 2010).

#### Cyberattacks won’t result in nuclear war --- airgapping solves

Green 2 – editor of The Washington Monthly (Joshua, 11/11, The Myth of Cyberterrorism, http://www.washingtonmonthly.com/features/2001/0211.green.html)

There's just one problem: There is no such thing as cyberterrorism--no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer. Nor is there compelling evidence that al Qaeda or any other terrorist organization has resorted to computers for any sort of serious destructive activity. What's more, outside of a Tom Clancy novel, computer security specialists believe it is virtually impossible to use the Internet to inflict death on a large scale, and many scoff at the notion that terrorists would bother trying. "I don't lie awake at night worrying about cyberattacks ruining my life," says Dorothy Denning, a computer science professor at Georgetown University and one of the country's foremost cybersecurity experts. "Not only does [cyberterrorism] not rank alongside chemical, biological, or nuclear weapons, but it is not anywhere near as serious as other potential physical threats like car bombs or suicide bombers." Which is not to say that cybersecurity isn't a serious problem--it's just not one that involves terrorists. Interviews with terrorism and computer security experts, and current and former government and military officials, yielded near unanimous agreement that the real danger is from the criminals and other hackers who did $15 billion in damage to the global economy last year using viruses, worms, and other readily available tools. That figure is sure to balloon if more isn't done to protect vulnerable computer systems, the vast majority of which are in the private sector. Yet when it comes to imposing the tough measures on business necessary to protect against the real cyberthreats, the Bush administration has balked. Crushing BlackBerrys When ordinary people imagine cyberterrorism, they tend to think along Hollywood plot lines, doomsday scenarios in which terrorists hijack nuclear weapons, airliners, or military computers from halfway around the world. Given the colorful history of federal boondoggles--billion-dollar weapons systems that misfire, $600 toilet seats--that's an understandable concern. But, with few exceptions, it's not one that applies to preparedness for a cyberattack. "The government is miles ahead of the private sector when it comes to cybersecurity," says Michael Cheek, director of intelligence for iDefense, a Virginia-based computer security company with government and private-sector clients. "Particularly the most sensitive military systems." Serious effort and plain good fortune have combined to bring this about. Take nuclear weapons. The biggest fallacy about their vulnerability, promoted in action thrillers like WarGames, is that they're designed for remote operation. "[The movie] is premised on the assumption that there's a modem bank hanging on the side of the computer that controls the missiles," says Martin Libicki, a defense analyst at the RAND Corporation. "I assure you, there isn't." Rather, nuclear weapons and other sensitive military systems enjoy the most basic form of Internet security: they're "air-gapped," meaning that they're not physically connected to the Internet and are therefore inaccessible to outside hackers. (Nuclear weapons also contain "permissive action links," mechanisms to prevent weapons from being armed without inputting codes carried by the president.) A retired military official was somewhat indignant at the mere suggestion: "As a general principle, we've been looking at this thing for 20 years. What cave have you been living in if you haven't considered this [threat]?" When it comes to cyberthreats, the Defense Department has been particularly vigilant to protect key systems by isolating them from the Net and even from the Pentagon's internal network. All new software must be submitted to the National Security Agency for security testing. "Terrorists could not gain control of our spacecraft, nuclear weapons, or any other type of high-consequence asset," says Air Force Chief Information Officer John Gilligan. For more than a year, Pentagon CIO John Stenbit has enforced a moratorium on new wireless networks, which are often easy to hack into, as well as common wireless devices such as PDAs, BlackBerrys, and even wireless or infrared copiers and faxes. The September 11 hijackings led to an outcry that airliners are particularly susceptible to cyberterrorism. Earlier this year, for instance, Sen. Charles Schumer (D-N.Y.) described "the absolute havoc and devastation that would result if cyberterrorists suddenly shut down our air traffic control system, with thousands of planes in mid-flight." In fact, cybersecurity experts give some of their highest marks to the FAA, which reasonably separates its administrative and air traffic control systems and strictly air-gaps the latter. And there's a reason the 9/11 hijackers used box-cutters instead of keyboards: It's impossible to hijack a plane remotely, which eliminates the possibility of a high-tech 9/11 scenario in which planes are used as weapons. Another source of concern is terrorist infiltration of our intelligence agencies. But here, too, the risk is slim. The CIA's classified computers are also air-gapped, as is the FBI's entire computer system. "They've been paranoid about this forever," says Libicki, adding that paranoia is a sound governing principle when it comes to cybersecurity. Such concerns are manifesting themselves in broader policy terms as well. One notable characteristic of last year's Quadrennial Defense Review was how strongly it focused on protecting information systems.

#### No retaliation

NBC 11 [NBC News, May 31, 2011, "Sources: US decides cyber attack can be 'act of war'", http://www.nbcnews.com/id/43224451/ns/us\_news-security/t/sources-us-decides-cyber-attack-can-be-act-war/#.UiS6OJLVCSo]

In its first formal cyber strategy, the Pentagon has concluded that computer sabotage by another country could constitute an act of war, administration and military sources told NBC News on Tuesday, confirming a report in the Wall Street Journal.¶ The officials emphasize, however, that not every attack would lead to retaliation. Such a cyber attack would have to be so serious it would threaten American lives, commerce, infrastructure or worse, and there would have to be indisputable evidence leading to the nation state involved, NBC Pentagon correspondent Jim Miklaszewski said.¶ Unclassified parts of the 30-page strategy are expected to become public in June, the Wall Street Journal reported, attributing the disclosure to three defense sources who had read the report.¶ A military source described the strategy to the Journal this way: "If you shut down our power grid, maybe we will put a missile down one of your smokestacks."¶ Pentagon officials and others in Washington are still debating what would constitute an act of war, the Journal stated, though one idea gaining traction is that of "equivalence" — military retaliation would be triggered by a cyber attack that causes the kind of death, damage or high-level disruption that a traditional military attack would cause.

#### No accidents—safeguards and ocean targeting

**Slocombe 9** (Walter, senior advisor for the Coalition Provisional Authority in Baghdad and a former Under Secretary of Defense for Policy, he is a four-time recipient of an award for Distinguished Public Service and a member of the Council on Foreign Relations, “De-Alerting: Diagnoses, Prescriptions, and Side-Effects,” Presented at the seminar on Re-framing De-Alert: Decreasing the Operational Readiness of Nuclear Weapons Systems in the US-Russia Context in Yverdon, Switzerland, June 21-23)

Let’s start with Technical Failure – the focus of a great deal of the advocacy, or at least of stress on past incidents of failures of safety and control mechanisms.4 Much of the “de-alerting” literature points to a succession of failures to follow proper procedures and draw from that history the inference that a relatively simple procedural failure could produce a nuclear detonation. The argument is essentially that nuclear weapons systems are sufficiently susceptible of pure accident (including human error or failure at operational/field level) that it is essential to take measures that have the effect of making it necessary to undertake a prolonged reconfiguration of the elements of the nuclear weapons force for a launch or detonation to be physically possible. Specific measures said to serve this objective include separating the weapons from their launchers, burying silo doors, removal of fuzing or launching mechanisms, deliberate avoidance of maintenance measures need to permit rapid firing, and the like. . My view is that this line of action is unnecessary in its own terms and highly problematic from the point of view of other aspects of the problem and that there is a far better option that is largely already in place, at least in the US force – the requirement of external information – a code not held by the operators -- to arm the weapons Advocates of other, more “physical,” measures often describe the current arrangement as nuclear weapons being on a “hair trigger.” That is – at least with respect to US weapons – a highly misleading characterization. The “hair trigger” figure of speech confuses “alert” status – readiness to act quickly on orders -- with susceptibility to inadvertent action. The “hair trigger” image implies that a minor mistake – akin to jostling a gun – will fire the weapon. The US StratCom commander had a more accurate metaphor when he recently said that US nuclear weapons are less a pistol with a hair trigger than like a pistol in a holster with the safety turned on – and he might have added that in the case of nuclear weapons the “safety” is locked in place by a combination lock that can only be opened and firing made possible if the soldier carrying the pistol receives a message from his chain of command giving him the combination. Whatever other problems the current nuclear posture of the US nuclear force may present, it cannot reasonably be said to be on a “hair trigger.” Since the 1960s the US has taken a series of measures to insure that US nuclear weapons cannot be detonated without the receipt of both external information and properly authenticated authorization to use that information. These devices – generically Permissive Action Links or “PALs” – are in effect combination locks that keep the weapons locked and incapable of detonation unless and until the weapons’ firing mechanisms have been unlocked following receipt of a series of numbers communicated to the operators from higher authority. Equally important in the context of a military organization, launch of nuclear weapons (including insertion of the combinations) is permitted only where properly authorized by an authenticated order. This combination of reliance on discipline and procedure and on receipt of an unlocking code not held by the military personnel in charge of the launch operation is designed to insure that the system is “fail safe,” i.e., that whatever mistakes occur, the result will not be a nuclear explosion. Moreover, in recent years, both the US and Russia, as well as Britain and China, have modified their procedures so that **even if** a nuclear-armed missile were **launched**, it would go not to a “real” target in another country but – at least in the US case - to empty ocean. In addition to the basic advantage of insuring against a nuclear detonation in a populated area, the fact that a missile launched in error would be on flight path that diverged from a plausible attacking trajectory should be detectable by either the US or the Russian warning systems, reducing the possibility of the accident being perceived as a deliberate attack. De-targeting, therefore, provides a significant protection against technical error. These arrangements – PALs and their equivalents coupled with continued observance of the agreement made in the mid-90s on “de-targeting” – do not eliminate the possibility of technical or operator-level failures, but they come very close to providing absolute assurance that such errors cannot lead to a nuclear explosion or be interpreted as the start of a deliberate nuclear attack.6 The advantage of such requirements for external information to activate weapons is of course that the weapons remain available for authorized use but not susceptible of appropriation or mistaken use.

#### No transition wars or heg impact

**Parent 11**—Assistant Professor of Political Science at the University of Miami—AND—Paul K. MacDonald, Assistant Professor of Political Science at Williams College (Joseph M., Spring 2011, *International Security*, Vol. 35, No. 4, http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC\_a\_00034, RBatra)

Some observers might dispute our conclusions, arguing that hegemonic transitions are more conflict prone than other moments of acute relative decline. We counter that **there are deductive and empirical reasons to doubt this argument**. Theoretically, hegemonic powers should actually find it easier to manage acute relative decline. **Fallen hegemons still have formidable capability, which threatens grave harm to any state that tries to cross them.** Further, they are no longer the top target for balancing coalitions, and recovering hegemons may be influential because they can play a pivotal role in alliance formation. In addition, hegemonic powers, almost by definition, possess more extensive overseas commitments; they should be able to more readily identify and eliminate extraneous burdens without exposing vulnerabilities or exciting domestic populations. We believe the empirical record supports these conclusions. In particular, **periods of hegemonic transition do not appear more conflict prone** than those of acute decline. The last reversal at the pinnacle of power was the Anglo-American transition, which took place around 1872 and was resolved without armed confrontation. The tenor of that transition may have been influenced by a number of factors: both states were democratic maritime empires, the United States was slowly emerging from the Civil War, and Great Britain could likely coast on a large lead in domestic capital stock. Although China and the United States differ in regime type, similar factors may work to **cushion the impending Sino-American transition**. Both are large, relatively secure continental great powers, a fact that mitigates potential geopolitical competition.93 China faces a variety of domestic political challenges, including strains among rival regions, which may complicate its ability to sustain its economic performance or engage in foreign policy adventurism.94 Most important, the United States is not in free fall. Extrapolating the data into the future, we anticipate the United States will experience a “moderate” decline, losing from 2 to 4 percent of its share of great power GDP in the five years after being surpassed by China sometime in the next decade or two.95 Given the relatively gradual rate of U.S. decline relative to China, the incentives for either side to run risks by courting conflict are minimal. The United States would still possess upwards of a third of the share of great power GDP, and would have little to gain from provoking a crisis over a peripheral issue. Conversely, China has few incentives to exploit U.S. weakness.96 Given the importance of the U.S. market to the Chinese economy, in addition to the critical role played by the dollar as a global reserve currency, it is unclear how Beijing could hope to consolidate or expand its increasingly advantageous position through direct confrontation.

#### Their internal link to decapitation is the grid – that’s resilient

**Farrell et al, 02 -** research engineer in the Department of Engineering and Public Policy at Carnegie Mellon University and the executive director of the Carnegie Mellon Electricity Industry Center (Alexander, “Bolstering the Security of the Electric Power System,” Issues in Science and Technology, Spring, http://www.issues.org/18.3/farrell.html)

Turning out the lights¶ Many terrorism scenarios involve disruption of electric service, or "turning out the lights." Whether this would allow terrorists to create widespread fear and panic is open to question. In the United States, households lose power for an average of 90 minutes per year. For the most part, individuals and society cope with these outages well, and power companies respond rapidly to restore service. Facilities that have special needs for reliability, such as hospitals and airports, typically have backup generators.¶ The local distribution system is the source of most outages; these affect relatively small numbers of people. The bulk power (generation and transmission) system causes only a few outages each year. In its most recent report on failures in this part of the electric power system, the North American Electricity Reliability Council (NERC) identified 58 "interruptions, unusual occurrences, demand and voltage reductions, and public appeals" in 2000. Of these events, almost half (26) were due to weather, mostly thunderstorms. Operator or maintenance errors accounted for 12 events, another 12 were due to faulty equipment, and 2 (including the largest single event) were due to forest fires. Six outages occurred simply due to failure to have sufficient power to meet demand. Not all of these 58 events caused the lights to go out, but when they did, many customers were affected. Even so, recovery was typically swift. The largest single outage in 2000 affected more than 660,000 customers in New Mexico but lasted for less than four hours.¶ Natural challenges of even larger scale have been met. For example, in January 1998 an ice storm struck Southern Canada and New York State, felling 1,000 transmission towers and 30,000 distribution poles while sending thousands of tree branches into power lines. This event left 1.6 million people without power, some for more than a month. Almost a quarter-million people were forced to leave their homes. Insurance claims reached about $1 billion (Canadian). This event was disruptive and costly, but it did not create terror or significant loss of life.

#### No modeling - strategic incentive to maintain legal ambiguity

Waxman 11 [Matthew C. Waxman, Associate Professor, Columbia Law School; Adjunct Senior Fellow, Council on Foreign Relations; Member of the Hoover Institution Task Force on National Security and Law, Yale Journal of International Law, March 16, 2011, “Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," vol 36, http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1674565]

B. Technology, Power Shifts, and the Strategic Logic of Legal Interpretation¶ With these relationships between law and power in mind, the United States has an interest in regulating cyber-attacks, but it will be difficult to achieve such regulation through international use-of-force law or through new international agreements to outlaw types of cyber-attacks.143 That is because the distribution of emerging cyber-capabilities and vulnerabilities— vulnerabilities defined not only by the defensive capacity to block actions but also by the ability to tolerate and withstand attacks—is unlikely to correspond to the status quo distribution of power built on traditional measures like military and economic might.¶ It is not surprising that the United States seems inclined toward an interpretation of Articles 2(4) and 51 that allows it to classify some offensive cyber-attacks as prohibited “force” or an “armed attack” but does not otherwise move previously drawn lines to encompass economic coercion or other means of subversion in that classification. Nor is it surprising to see the United States out in front of other states on this issue. The power and vulnerability distribution that accompanies reliance on networked information technology is not the same as past distributions of military and economic power, and perhaps not to the United States’s advantage relative to rivals. Moreover, some U.S. strengths are heavily built on digital interconnectedness and infrastructure that is global, mostly private, and rapidly changing; these strengths are therefore inextricably linked to new and emerging vulnerabilities.144¶ Although some experts assess that the United States is currently strong relative to others in terms of offensive capabilities,145 several factors make the United States especially vulnerable to cyber-attack, including the informational and electronic interconnectedness of its military and public and private sectors, and political obstacles to curing some of these vulnerabilities through regulation.146 As the Obama administration’s 2010 National Security Strategy acknowledged:¶ The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority . . . . Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale.147¶ In other words, U.S. technological strengths create corresponding exposures to threats. The U.S. government is especially constrained politically and legally in securing its information infrastructure—which is largely privately held or privately supplied—against cyber-threats, and these constraints shape its international strategy. Proposals to improve cyber-security through regulation include promulgating industry standards to enhance the security of information technology products and protect networks and computers from intrusion, and, more invasively, expanding the government’s authority to monitor information systems and communications.148 Such proposals invariably face powerful antiregulatory industry pressures and heightened civil liberties sensitivities.149 Information technology industry groups and privacy organizations have together pushed back against moves to impose government security mandates and against more intrusive government cyber-security activities, arguing that they would stifle innovation, erode civil liberties, and fail to keep up with rapidly evolving threats amid a globalized economy.150 A reluctance to secure information systems domestically through government regulation then elevates U.S. government reliance on other elements of a defensive strategy.¶ In that light, U.S. legal interpretations and declaratory postures that define prohibited force in ways that extend narrow Charter interpretations to take account of cyber-warfare may be seen as part of an effort to sustain a legal order in which anticipated U.S. military and economic moves and countermoves against potential adversaries fit quite comfortably—that is, a legal order that preserves U.S. comparative advantages. In extending the foundational U.N. Charter prohibition on force to cyber-attacks by emphasizing their comparable effects to conventional military attacks, such interpretations help deny that arsenal to others by raising the costs of its use. At the same time, by casting that prohibition and complementary self-defense authority in terms that help justify military force in response, this interpretation reduces the costs to the United States of using or threatening to use its vast military edge (and it helps signal a willingness to do so).¶ Put another way, the United States appears to be placing hedged bets about what the future strategic environment will look like and how best to position itself to operate and compete in it. On balance, for example, the United States may prefer relatively clear standards with respect to cyber-actions that have immediate destructive effects—at least clear enough to justify armed response or deterrence to activities or scenarios deemed threatening—while at the same time preferring some permissive haziness with respect to intelligence collection and its own countermeasures in cyberspace. Such a posture allows the United States to protect itself from hostile penetrations while also preserving some latitude for those activities in which it may be relatively strong.151 Internally, that clarity facilitates planning for contingencies and deliberation about options;152 externally, it may help articulate and deter the crossing of red lines.153¶ In trying to explain what may be driving the U.S. interpretation, this Article is neither affirming nor denying this strategic logic, which is contingent on future capabilities and vulnerabilities that are both highly uncertain and shrouded in secrecy. Rather, it is trying to uncover and scrutinize some of the underlying assumptions.¶ There are several strategic reasons for the United States to be cautious in considering interpretations that expand narrow definitions of “force” and “attack” so that they include potentially broad categories of cyber-attacks— risks that are often not acknowledged or addressed in discussions of the U.S. interpretive trajectory. For one thing, the United States has generally defeated efforts by other states to interpret Articles 2(4) and 51 expansively to include economic coercion and other forms of political subversion.154 In thinking about the Charter regime as a whole, therefore, the United States may not want to reopen those debates. Cyber-attacks can allow state and nonstate actors to inflict massive harm without resort to arms, but that has long been true of many other instruments, including economic and financial means, covert subterfuge, and other widely used instruments. In that regard, one advantage of promoting legal regulation of cyber-attacks through a new treaty or international agreement instead of through Charter interpretation is that such efforts would have little if any effect on broader Charter law. An advantage, however, to working through Charter interpretation rather than new agreements is that Charter law can evolve incrementally and begin shaping international actors’ expectations through unilaterally initiated state practice without having to reach consensus (the difficulties of which are discussed in the next Section).¶ Depending on the relative risk of different types of future cyber-attack scenarios, it might also be in the United States’s strategic interest to legally delink cyber-activities from armed force instead of defining force by reference to effects, or at least to impose extremely high legal thresholds for treating cyberattacks equivalent to force or armed attack, in order to reduce the chances of military escalation from cyber-activities.155 As capabilities proliferate among state and nonstate actors to conduct various sorts of malicious, hostile, or intelligence-gathering activities in cyberspace, any normative constraints that come from treating some cyber-attacks as force prohibited by Article 2(4) and any deterrence value of treating them as armed attacks triggering self-defense rights under Article 51 might be outweighed by the dangers of lowering legal barriers to military force in a wider range of circumstances.156 That is, the value of promoting a right of armed self-defense against cyber-attacks may turn out to be quite low—since, among other things, it may be difficult to sufficiently prove one’s case publicly in justifying military responses—while doing so may introduce greater security instability to the international system by eroding normative constraints on military responses to nonmilitary harms.157¶ As the following Section explores, it is very difficult to assess these risk balances because the global security environment is shifting dramatically and unpredictably. Moreover, even if the United States could assess the risks accurately, other states may be operating under different sets of strategic assumptions about that future.¶ C. Divergent Interests and Implications for Charter Interpretation¶ Assuming the United States decides firmly on a legal interpretation going forward, the redrawing of legal lines on a map of inequitably distributed power and vulnerabilities would create winners and losers and would make it difficult to reach agreement on new legal boundaries, whether through interpretive evolution of the U.N. Charter or new conventions.158 In thinking about legal interpretations of Articles 2(4) and 51, success therefore depends on the ability of proponents to articulate and defend their legal lines using combinations of traditional and new forms of power for deterrence, self-defense, enforcement, and influence.¶ Again, one should not divorce analysis of any proposed content of Articles 2(4) and 51 from the processes by which it is interpreted, reinterpreted, enforced, and reinforced.159 The likely factual ambiguity surrounding cyberattacks and the pressures to take aggressive responsive or escalatory measures more quickly than those facts can be resolved may sometimes require strategic and military decisionmaking amid legal gray zones. Moreover, as involved states marshal their arguments amid these moves and countermoves, and as they consider their long-term interests, they may also calculate differently what Stone calls “the expected value . . . of built-in [legal] ambiguities as future political weapons.”160¶ That is, even if states widely share a common, minimum interest in restricting some cyber-attacks, states may have divergent interests regarding specific substantive content as well as the desired degree of clarity in the law. Salient differences will likely stem from asymmetries of geostrategic ambitions, internal and external commitment to legal norms generally, and the nature and extent of public-private institutional relationships.161¶ In contrast to the United States, some states that are developing offensive cyber-warfare capabilities (such as North Korea, according to many experts) are non-status-quo powers or aspiring regional powers,162 and they may prefer legal ambiguity as to cyber-attacks or narrow interpretations of Article 51 that would allow them—if they resort to cyber-attacks—to portray themselves as victims of any responsive military strikes.163 Offensive cyber-capabilities have the potential to shift or upset international balances of power, because some states are more vulnerable than others to cyber-attack (in terms of capacity to block actions as well as to tolerate or withstand them), and attacks could have a disproportionately large impact on countries or militaries that have a higher reliance on networked information systems.164 Developing an offensive cyberwarfare capability is likely to be less expensive in resources and diplomatic costs than competing economically or militarily with much stronger states, though legal flexibility or constraints could alter that calculus.165 On the other hand, some small states that are unlikely to develop sophisticated offensive or defensive systems may advocate international legal interpretations or new agreements that are very restrictive of cyber-attacks and define attacks broadly, seeing themselves as highly reliant on protective norms.166 Individually, though, they will have little power to promote those principles.¶ Like the United States, other major actors may have much to lose from cyber-attacks. However, they may calculate their short- and long-term strategic interests with respect to cyber-warfare and its regulation differently than the United States, in light of their own matrix of offensive and defensive capabilities, public-private institutional relationships, and asymmetries in the ways international law constrains different actors.167 Russia, for example, has proposed to the United Nations a draft statement of principles that would prohibit the development, creation, and use of cyber-attack tools. Meanwhile, though, Russia is engaged in developing cyber-attack capabilities,168 and some analysts are skeptical of Russia’s sincerity in proposing cyber-arms control agreements, especially given the difficulties of verifying them.169 China likely sees cyber-warfare capabilities as a way of equalizing the conventional military superiority of the United States,170 so it may be reluctant to concede legally “disarming” interpretations, at least without some reciprocal benefit or legal concession. Russia and China, which, as mentioned earlier, both reportedly exploit informal relationships with private actors (i.e., “citizen hackers”) to conduct attacks and collect intelligence in cyberspace, may also incline toward legal doctrine that makes it difficult to impute private cyber-actions to governments.171 Meanwhile, some European states have approached the legal relationship between cyber-attacks and force cautiously, perhaps because of general concerns about military escalation of crises and divergent strategic assessments among themselves.172¶ Differences in internal politics, ideology, and government control over information will also shape state interests in competing interpretations of Charter norms. With echoes of debates from prior eras,173 various types of states are likely to view cyber-threats differently and to distinguish offensive attacks from defensive measures differently. For instance, some states that tightly control information, including major powers like China, are especially concerned about internal political dissent and might therefore define what the United States sees as “Internet freedom” as a threat to vital security interests. Efforts to crack down on what they (or other states that exercise strong state control over Internet content) may view as defensive measures against hostile subversion may be viewed by the United States (or other states that value and promote free speech) as hostile, offensive measures.174 It is hard to envision a state in China’s position strongly endorsing or standing behind U.S. visions for international legal regulation of cyber-attacks without some unlikely concessions by the United States.175¶ From a policy standpoint, this should sound another cautionary note about efforts to build international legal consensus about cyber-attacks and the use of force, whether through Charter interpretation or new agreements. Emergent U.S. government inclinations toward effects-based interpretations of the Charter may be legally reasonable and protective of some core U.S. interests, as well as widely shared foreign interests. But even if they help in the short term to manage competing risks of too much or too little authority to employ cyberattacks, or too much or too little leeway to resort to armed self-defense in response, a coherent legal strategy can only be forged and advanced in the long term if it is integrated effectively with broader diplomacy and security strategy, including efforts to build and sustain offensive, defensive, deterrent, and intelligence capabilities—while others do the same based on a different set of objectives, capabilities, vulnerabilities, and constraints.

### 1nc cyber war

#### Global trade resilient

**Kim 13**

Soo Yeon Kim, of the National University of Singapore, associate professor of music at Nazareth College of Rochester, New York, Fellow of the Transatlantic Academy, based at the German Marshall Fund of the United States, The Monkey Cage, January 30, 2013, " Protectionism During Recessions: Is This Time Different?", http://themonkeycage.org/blog/2013/01/30/protectionism-during-recessions-is-this-time-different/

There is widespread agreement regarding the critical role of international institutions as “firewalls” against protectionism during this recession. Economic and non-economic international institutions have served as conveyors of information and mechanisms of commitment and socialization. Their informational function enhances the transparency and accountability of states’ trade policies, and they mitigate uncertainty when it is running high. Specialized international institutions devoted to trade, such as the WTO and preferential trade agreements (PTAs), also lock in commitments to liberal trade through legal obligations that make defections costly, thus creating accountability in the actions of its members. Equally important, international institutions are also arenas of socialization that help propagate important norms such as the commitment to the liberal trading system and cooperative economic behavior. In this connection, the degree to which a particular country was embedded in the global network of economic and non-economic international institutions has been found to be strongly correlated with fewer instances of protectionist trade measures.¶ Information provided to date by international institutions, with the exception of the GTA project, largely agree that states have not resorted to large-scale protectionism during this recession, in spite of the fact that the “great trade collapse” at the beginning of the current crisis was steeper and more sudden than that of its Great Depression predecessor. The WTO Secretariat, in addition to its regular individual reports on members’ trade policies under the Trade Policy Review Mechanism (TPRM), has issued more than a dozen reports on member states’ trade policies during the crisis. At the request of the G-20 countries, which pledged not to adopt protectionist trade measures at the onset of the crisis in 2008, the WTO, the OECD, and UNCTAD have produced joint reports on the trade and investment measures of the world’s largest trading states. They, too, find that G-20 countries had largely adhered to their commitment not to raise trade and investment barriers. In the World Bank’s Temporary Trade Barriers (TTB) project, an important and unique data collection that includes information on pre-crisis and crisis trade policy behavior, Bown finds that temporary trade barriers such as safeguards, countervailing and antidumping duties saw only a slight increase of usage by developed countries, in the neighborhood of 4%. In contrast, emerging market economies were the heavy users of TTBs, whose usage rose by almost 40% between 2008 and 2009.¶ As scholarly insights accumulate on the current recession and its impact on protectionism (or lack thereof), two questions emerge for further research. First, to what extent have governments employed policy substitutes that have the same effect as trade protectionism? International institutions may appear to have been successful in preventing protectionism, but governments may well have looked elsewhere to defend national economies. This question can be seen in the broader context of the “open economy trilemma,” in which governments may achieve only two of three macroeconomic policy objectives: stable exchange rates, stable prices, and open trade. Irwin argues that governments that abandoned the gold standard during the Great Depression were less protectionist, and their economies also suffered less from the recession. Existing scholarship also indicates that governments are likely to employ policy substitutes, opting for monetary autonomy when facing trade policy constraints, for example, due to membership in a preferential trade agreement. Moreover, at the time of writing, the International Monetary Fund (IMF) has announced that it has dropped its objections to capital controls, albeit cautiously and only under certain conditions, thus potentially providing another policy alternative for governments to achieve economic stability during this crisis. Future research may further extend the application to policy substitutes that are deployed during economic downturns.¶ Finally, why did firms not push for more protection? Protectionist policies are not adopted by governments in a political vacuum. In order to adopt trade defense measures such as anti-dumping duties, governments first conduct investigations to assess the extent of injury. Such investigations are initiated when firms apply for them through the domestic political process. If indeed governments did not appeal extensively or unusually to protectionist trade policies, the explanation to a significant degree lies in firm behavior. A distinguished body of research exists in this area that is due for a revisit in the age of extensive international supply chains, from Schattschneider’s classic examination of the domestic pressures that led to the Smoot-Hawley Act to Helen Milner’s study of export-dependent firms that resisted protectionism during the crisis of the 1920s and the 1970s. Milner rightly pointed out that “firms are central,” and over the years the export-dependent, multinational firm has evolved in tandem with the increasing complexity of the international supply chain. Today’s firm is not only heavily export-dependent but equally import-dependent in its reliance on intermediate inputs, whether through intra-firm trade or from foreign firms. The extensive international supply chain thus often puts exporting and importing firms on the same side of the political debate, especially when they are members of large multinational firms. Moreover, the study of firm-level behavior must extend beyond the developed world to consider firms in emerging market economies, which have been the heavy users of trade defense measures during the current recession. How the internationalization of production, driven by investment and trade in intermediate goods, restrained multinational firms from pushing for more protection remains an important question for further research.

#### No evidence linking the plan to recruitment – plan doesn’t do anything about the NSA scandal, which was about domestic surveillance, not overseas hacking operations

#### Circumvention blocks – means can’t solve transparency

**Davis 10** [“Congress’s Role in Cyber Warfare,” Stephen, Professor, Vermont Law School, Journal of National Security Law & Policy, http://jnslp.com/wp-content/uploads/2010/08/11\_Dycus.pdf]

The “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. Another potential obstacle to congressional involvement is the reportedly common but statutorily unauthorized practice of informal reporting to an even smaller “Gang of Four” – the leaders of the intelligence committees – generally for sensitive non-covert intelligence activities.

#### Alt-causes to hiring shortages – low pay, security clearances, bureaucratic blocks

**Ballenstadt 13** [“More Than 1 in 5 Cyber Jobs Vacant at Key DHS Division,” http://www.nextgov.com/cybersecurity/2013/09/more-one-five-cyber-jobs-vacant-key-dhs-subcomponent/70620/?oref=ng-dropdown]

More than one in five jobs at a key cybersecurity component within the Homeland Security Department are vacant, in large part due to steep competition in recruiting and hiring qualified personnel, according to a new report by the Government Accountability Office. ¶ The report, which assessed recruiting and hiring efforts at DHS overall, found that the Office of Cybersecurity and Communications – the subcomponent within the National Protection and Programs Directorate that houses cybersecurity personnel – has a vacancy rate of 22 percent.¶ NPPD officials cited challenges in recruiting cyber professionals because of the length of time taken to conduct security checks to grant top-secret security clearances as well as low pay in comparison with the private sector.¶ A lack of clearly defined skills or unique occupational series for cybersecurity positions is not only hindering recruitment efforts but also DHS’ efforts to measure cybersecurity hiring and attrition, GAO found. Without a defined career series and path, cybersecurity personnel are spread throughout a number of different occupational series within NPPD, meaning officials could not provide GAO with specific hire and loss data on the cyber workforce.

#### Not enough domestic recruits will exist until 2022

**Jackson ‘10** (William, is a senior writer for GCN and the author of the CyberEye column, Oct 21, “Feds experiencing critical cybersecurity staff shortage”, <http://defensesystems.com/articles/2010/10/21/cyber-workforce-search.aspx?admgarea=DS>)

“We just don’t have enough people yet,” Philip Reitinger, deputy undersecretary in the National Protection and Programs Directorate, said Thursday at a forum on workforce development hosted in Washington by Deloitte. “This is going to be a continuing challenge for us.” DHS has been recruiting from other agencies as well as from the private sector, but Reitinger called that a “zero sum game,” because there are not enough trained professionals coming into the field to meet demand. “There are **not enough people to go around**.” The problem has been recognized for several years and a number of public-private initiatives are under way to identify students with the proper interests and abilities in high school or even earlier, and to provide them with educational opportunities and career paths. Several high school and collegiate cybersecurity competitions are flourishing, and the University of Maryland University College has established three cybersecurity degree programs to help fill the demand for tens of thousands of professionals in Maryland, which is home not only to the National Security Agency but also to the Pentagon’s new Cyber Command. It will be two to **12 years or even more** before these new pipelines begin supplying significant numbers of new workers, however. In the meantime, the federal government is at a disadvantage in this market because of its recruiting and hiring practices. “The current federal process is a disincentive to come in” to government work, said James Lewis, director of the technology and public policy program at the Center for Strategic and International Studies. He said the problem was not limited to cybersecurity. “It’s a larger workforce problem.” Reitinger agreed. “Hiring in the federal government has to be modernized across the board,” he said. DHS has obtained waivers from the Office of Personnel Management to use greater flexibility in its hiring process and has experimented with techniques, such as a virtual job fair conducted online. But this cannot make up for the lack of a trained workforce produced by strong science, technology, engineering and mathematics (STEM) programs. “This is a glaring weakness here in the United States,” said Jake Olcott, counsel to the Senate Commerce, Science and Transportation Committee. “Our **STEM educational system is not working** well right now.” Colleges and universities have offered computer science programs since the days of punch cards, but the integration of computer science with security, law, law enforcement, government policy and all things cyber is only just getting under way.

# 2nc

## solvency

### 2nc circumvention

#### Oversight won’t restrict Presidential secrecy

**Dycus 10** [“Congress’s Role in Cyber Warfare,” Stephen, Professor, Vermont Law School, Journal of National Security Law & Policy, http://jnslp.com/wp-content/uploads/2010/08/11\_Dycus.pdf]

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

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

**Dycus 10** [“Congress’s Role in Cyber Warfare,” Stephen, Professor, Vermont Law School, Journal of National Security Law & Policy, http://jnslp.com/wp-content/uploads/2010/08/11\_Dycus.pdf]

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

## counterplan

### 2nc solvency

#### Foreign specialists are key – declining university retention will cause substantial declines in US IT capital

**McCormack ‘10** (Ade, advises on e-skills and IT leadership issues. Trained as an astrophysicist, he went on to become a technologist. Today he advises organisations on how to maximise the return on their IT investment “The e-Skills Manifesto A Call to Arms,” 6/30, " http:eskills.eun.org/c/document\_library/get\_file?p\_l\_i|http://www.google.com/url?sa=t&source=web&cd=21&ved=0CB0QFjAAOBQ&url=http%3A%2F%2Feskills.eun.org%2Fc%2Fdocument\_library%2Fget\_file%3Fp\_l\_id%3D10713%26folderId%3D10511%26name%3DDLFE-2403.pdf&rct=j&q=%22cyber%20security%22%20immigration%20skills%20shortage%20visas&ei=7nFNTbHpK8L-8Abwn-idDg&usg=AFQjCNGfEMHGe7L87oJSDc7I95-KGWLe0Q)

Yet, despite such positives for U.S. IT practitioners, it is for several reasons far from clear that America as a country can maintain its IT practitioner strength; In a period of rising demand and in a striking reversal of the accelerating global trend towards liberalizing immigration rules for high-skilled workers46 , U.S. businesses’ access to foreign IT practitioners remains curtailed at levels far below those of the 1990s. With U.S. IT practitioner employment projected to grow rapidly and foreign-born IT entrepreneurs historically establishing up to half of Silicon Valley’s new technology firms47 , America’s current high-skilled immigration policy is sure to aggravate any future IT practitioner skill shortages and is **highly damaging** for the nation’s broader information technology prospects. At the same time, the U.S. domestic education system seems increasingly unable to produce the required additional IT practitioners during the next decade, especially considering ongoing state and local government budget cuts in education. U.S. computer sciences degrees at the Bachelor and Master’s level has been in general decline in recent years, while only seeing some growth at the much smaller doctoral level. Foreign human capital (here students) **play an important role** in the U.S. IT-related education system. While foreign students account for only a relatively minor share of IT-related U.S. bachelor degrees, at the master’s and particularly doctoral level, their presence looms large. A substantial part of the growth in the number of doctoral degrees given between 2003 and 2007 is thus related to a continued increase in the presence of foreign IT-related students at U.S. education institutions. Please Don’t Go The large inflow of foreign graduate level students to the United States is a clear testament to the persistent global attractiveness of its universities and has always been a source of economic strength, as the world’s best and brightest came first to study and then remained in the U.S. workforce and contributed to the U.S. economy after graduation. However, with increasing economic growth and opportunities in many of the countries of origin for America’s foreign IT-students (over half are from either China or India), it is increasingly uncertain that America can maintain its historical ability to hold on to the foreign students educated at its universities. Any decline in U.S. retention of foreign IT-related students **will rapidly worsen** any future IT practitioner skill shortages.”

## econ

### Trade

#### Rising powers won’t threaten markets—they rely on the existing order—and even if they challenge it, they stop short of war

Leslie H. Gelb 10, President Emeritus of the Council on Foreign Relations; was a senior official in the U.S. Defense Department from 1967 to 1969 and in the State Department from 1977 to 1979, November/December 2010, “GDP Now Matters More Than Force,” Foreign Affairs, Vol. 89, No. 6

To an unprecedented degree, the major powers now **need one another** to grow their economies, and they are loath to jeopardize this interdependence by allowing traditional military and strategic competitions to escalate into wars. In the past, U.S. enemies--such as the Soviet Union--would have rejoiced at the United States' losing a war in Afghanistan. Today, the United States and its enemies share an interest in blocking the spread of both Taliban extremism and the Afghan-based drug trade. China also looks to U.S. arms to protect its investments in Afghanistan, such as large natural-resource mines. More broadly, no great nation is challenging the balance of power in either Europe or Asia. Although nations may not help one another, they rarely oppose one another in explosive situations.

Given the receding threat of great-power war, leaders around the world can afford to elevate economic priorities as never before. To be sure, leaders throughout history have pursued economic strength as the foundation of state power, but power itself was equated with military might. Today, the prevailing idea is that economic strength should be applied primarily toward achieving economic--not military--ends. Money is what counts most, so most nations limit their spending on standing armies and avoid military interventions. What preoccupies most leaders is trade, investment, access to markets, exchange rates, additional riches for the rich, and a better life for the rest.

This trend is plain among the rising regional powers known as the BRIC countries (Brazil, Russia, India, and China) and among such others as Indonesia, Mexico, South Africa, and Turkey. Although these countries' leaders have major security concerns--such as India with regard to Pakistan--their paramount objective has become economic strength. For most, economic growth is their prime means of fending off internal political opposition.

China makes perhaps the best case for the primacy of economics. Although it might emerge as a spoiler decades hence, Beijing currently promotes the existing economic order and does not threaten war. Because Beijing has been playing the new economic game at a maestro level--staying out of wars and political confrontations and zeroing in on business--its global influence far exceeds its existing economic strength. China gains extra power from **others' expectations of its future growth.** The country has become a global economic giant without becoming a global military power. Nations do not fear China's military might; they fear its ability to give or withhold trade and investments.

## deterrence da

### 2nc impact overview

#### Deterrence is the only way to solve critical infrastructure attacks and IP theft – turns case

**Jensen** 20**12 (**“Cyber Deterrence.” Emory International Law Review. Vol 26 Issue 2 Page 773. Eric Talbot Jensenteaches and writes in the areas of Public International Law, Criminal Law, The Law of Armed Conflict, International Criminal Law, and National Security Law.  His recent scholarship has appeared in the Texas, Temple, Houston, and Israel Law Reviews, as well as the Stanford Law and Policy Review, Virginia Journal of International Law, Vanderbilt Journal of Transnational Law, and Stanford Journal of International Law.  Professor Jensen is a co-author on an Oxford University text analyzing application of the laws of war to the war on terror and is also co-authoring a law school casebook on the Law of Armed Conflict for Aspen Publishing).

The government is certainly not alone as a target for malicious computer operations. Private businesses are also being hacked at an alarming rate. In a recent incident targeting “proprietary corporate data, e-mails, credit-card transaction data and login credentials at companies in the health and technology industries,” more than 75,000 computers at more than 2,500 businesses in 196 countries were targeted.10 The presumed targets in these attacks were intellectual property and proprietary information that could be translated into economic gain for the attackers.11 According to Ty Sagalow, chairman of the Internet Security Alliance board of directors, “[a]n estimated $1 trillion was lost in the United States in 2008 through cyber attacks.”12 This is **more than the annual** **G**ross **D**omestic **P**roduct **of all but the top nineteen countries in the world**.13Among the most worrisome of hacking incidents are those focused on critical national infrastructure.14 This infrastructure is the backbone of United States’ transportation and economic systems.15 The cost of downtime alone from major attacks on critical national infrastructure “exceeds . . . $6 million per day.”16 The attacks have caused President Barack Obama to recently state, From now on, our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.17 President Obama’ s recognition of the role and importance of deterring malicious cyber operations, including cyber attacks, incorporates the traditional notions of deterrence to this modern risk to national security. Deterrence has been a part of Western political security doctrine since ancient Greece18 and played a particularly key role in the post-World War II nuclear world.19 It is equally important in today’s world of cyber operations20 and will continue to play a key role in the U.S. national security strategy.21 In fact, just as cyber operations offer unique capabilities as tools to accomplish national goals,22 they also present distinctive aspects of deterrence, both in line with traditional notions of deterrence and also some innovative and progressive ways of viewing deterrence.23 As the United States continues to develop and implement cyber deterrence strategies and capabilities,24 there are important legal issues that require consideration, including international law, the law of armed conflict (“LOAC”), and U.S. domestic law. This Article will identify and discuss six prominent theories of cyber deterrence and analyze legal issues associated with this vital area of national security. The law not only provides important factors that must be considered as cyber deterrence doctrine is solidified, but also provides significant insights into how these theories of cyber deterrence can best be utilized to support national strategic goals. Part I of this Article will examine some basic principles of deterrence that affect the application of the law, such as the difficulties of attribution and signaling. Part II will then outline six prominent theories of cyber deterrence and briefly describe some legal issues associated with them, including an analysis of how the law is an important consideration in applying these theories in modern U.S. national security strategy. The Article will conclude in Part III. I. DETERRENCE AND CYBER OPERATIONS The goal of deterrence is to prevent aggressive action . . . by ensuring that, in the mind of a potential adversary, the risks of the action outweigh the benefits, while taking into account the consequences of inaction.25 As mentioned in the Introduction, deterrence theory is not a new phenomenon26 and has played a significant role in national security theory.27 With the modern development of cyber operations, the U.S. Government, as well as academics and practitioners, have turned their attention to cyber deterrence.28 The nature of cyber operations has caused some to diminish the potential role for deterrence. Tang Lan and Zhang Xin have written “the anonymity, the global reach, the scattered nature, and the interconnectedness of information networks greatly reduce the efficacy of cyber deterrence and can even render it completely useless.”29 Despite this competing view, cyber deterrence continues to increase in importance30 as nations struggle with the vulnerability of both government and private sector cyber systems. Before discussing the prominent cyber deterrence theories and the attending legal issues, some comment on the unique aspects of cyber deterrence will be useful. A. Assumptions In approaching this topic, some assumptions are necessary. These assumptions undergird the subsequent legal analysis but are relatively uncontroversial, particularly in the cyber domain. 1. Full Spectrum Deterrence Required The initial assumption is that cyber deterrence is required across a much greater spectrum than most other weapons and actors, and certainly than was present in the post-World War II discussion of nuclear deterrence.31 Cyber operations are inherently different than many other weapons that harness state level violence, in that they are accessible to a broad range of actors including but not limited to states.32 For example, only states, and very few of those, have ever developed a nuclear capability.33 On the other hand, more than 140 nations are reported to have or be developing cyber weapons,34 and more than thirty countries are creating cyber units in their militaries.35 The recent Stuxnet malware36 has been labeled by some as the first real example of a cyber “armed attack” in violation of the UN Charter, if it proves to have been carried out by a nation or its agents.37 The computer security giant Symantec believes that a cyber threat such as Stuxnet could be created by as few as five to ten highly trained computer technicians in as little as six months.38 Many non-state actors with malicious intentions could muster those resources and use them to create significant damage. Additionally, very effective hacking tools are readily available for purchase on the Internet by anyone desiring to conduct cyber crime.39 For example, two Chinese authors have written that:¶ Citibank . . . suffered tens of millions of dollars in losses at the hands of criminals using “Black Energy” malware, which can be purchased online for only $40. And the “Zeus Trojan” and its variants that attacked 74,000 computers across 196 countries are also available online for a mere $700.40In a recent statement before Congress, General Keith Alexander, head of Cyber Command and the National Security Agency, stated “[i]n 2010 we saw cyber capabilities in use that could damage or disrupt digitally controlled systems and networked devices, and in some cases we are not sure whether these capabilities are under the control of a foreign government.”41 The ability for non-state actors and even individuals to harness the power of cyber weapons and use them at their discretion, with significant effects,42 has a serious impact on deterrence that was not an issue with the nuclear threat.43 In fact, “Russian experts believe that it is criminals and terrorists who present the greatest threat to the security of transnational cyberspace.”44 Additionally, cyber operations allow an adversary to accomplish a broad spectrum of effects. In nuclear deterrence, the effects were usually considered catastrophic, allowing a limited number of responses.45 In cyber operations, effects can be as small as the penetration of a system to observe what that system does,46 or the defacing of a web site.47 The effects can also be as large as destroying almost 1000 centrifuges, as Stuxnet is supposed to have done,48 or an electronic version of the attack on Pearl Harbor, as some warn about.49 This means that cyber deterrence theory must embrace a much larger spectrum of potential adversaries and account for being able to deter a much more diverse type of actor than most other previous modalities. Cyber deterrence must apply to the full spectrum of actors, from individuals to nations, and consider the full spectrum of actions, from small invasions into computer systems to large scale “attacks” that produce significant kinetic effects.

#### Perception of weak Presidential crisis response collapses heg

John R. Bolton 9, Senior fellow at the American Enterprise Institute & Former U.S. ambassador to the United Nations, “The danger of Obama's dithering,” Los Angeles Times, October 18, http://articles.latimes.com/2009/oct/18/opinion/oe-bolton18

Weakness in American foreign policy in one region often invites challenges elsewhere, because our adversaries carefully follow diminished American resolve. Similarly, presidential indecisiveness, whether because of uncertainty or internal political struggles, signals that the United States may not respond to international challenges in clear and coherent ways. Taken together, weakness and indecisiveness have proved historically to be a toxic **combination for America's global interests**. That is exactly the combination we now see under President Obama. If anything, his receiving the Nobel Peace Prize only underlines the problem. All of Obama's campaign and inaugural talk about "extending an open hand" and "engagement," especially the multilateral variety, isn't exactly unfolding according to plan. Entirely predictably, we see more clearly every day that diplomacy is not a policy but only a technique. **Absent** presidential leadership, **which at a minimum means** clear policy direction and persistence in the face of criticism and adversity**, engagement simply embodies** weakness and indecision.

### 2nc link wall

#### Plan allows Congress to vocally oppose crisis intervention --- or they literally don’t solve anything--- that destroys international perception of U.S. resolve

Waxman 8/25/13 Matthew Waxman, Professor of Law @ Columbia and Adjunct Senior Fellow for Law and Foreign Policy @ CFR, citing William Howell, Sydney Stein Professor in American Politics @ U-Chicago, and Jon Pevehouse, Professor of Political Science @ U-Wisconsin-Madison, “The Constitutional Power to Threaten War,” Forthcoming in Yale Law Journal, vol. 123, August 25, 2013, SSRN

When members of Congress vocally oppose a use of force, they undermine the president’s ability to convince foreign states that he will see a fight through to the end. Sensing hesitation on the part of the United States, allies may be reluctant to contribute to a military campaign, and adversaries are likely to fight harder and longer when conflict erupts— thereby raising the costs of the military campaign, decreasing the president’s ability to negotiate a satisfactory resolution, and increasing the probability that American lives are lost along the way. Facing a limited band of allies willing to participate in a military venture and an enemy emboldened by domestic critics, presidents may choose to curtail, and even abandon, those military operations that do not involve vital strategic interests.145

#### Notification kills effective cyber responses

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

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.

#### Consultation kills rapid response

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

8. Require consultation with the designated congressional committees in every possible instance before any significant use of cyber weapons.(Footnote 64 Begins) ¶ 64 . A National Research Council study suggests possible advance congressional approval of some offensive uses of cyber weaponry based on, inter alia, the scale of a contemplated attack, the target, and other circumstances. NATIONAL RESEARCH COUNCIL, supra note 3, at 56. Because of the possible need for immediate action, advance approval is not recommended here. Possible criteria for determining when a contemplated use is “significant” for these purposes are suggested supra note 31.

#### Disclosure kills deterrence

Goldsmith, 11 [[General Cartwright on Offensive Cyber Weapons and Deterrence](http://www.lawfareblog.com/2011/11/general-cartwright-on-offensive-cyber-weapons-and-deterrence/) By [Jack Goldsmith](http://www.lawfareblog.com/author/jack/) Tuesday, November 8, 2011 at 10:27 AM, Professor, Harvard Law, <http://www.lawfareblog.com/2011/11/general-cartwright-on-offensive-cyber-weapons-and-deterrence/>]

One cannot read too much into snippets of an interview, but of course matters are more complex than this. First, talking about offensive cyber-capabilities is a tricky business. Merely talking about the weapons in general terms, without revealing and perhaps demonstrating their capabilities, cannot advance deterrence very much. But on the other hand, too much detail about what the weapons can do make it easier, and potentially very easy, for adversaries to defend against these weapons by (among other things) closing the vulnerabilities that the weapons exploit. Moreover, openly demonstrating or even discussing cyber capabilities would further enflame the cyber arms race in ways that might be self-defeating. Second, revealing the circumstances in which these weapons will be used might invite infiltrations just short of those circumstances. “As soon as you declare a red line, you’re essentially telling people that everything up to that line is OK,” noted former Pentagon official Eric Sterner in the Reuters story. Third, and to my mind most fundamental, revealing the weapons capabilities and the (possible) circumstances of their use will not go far toward establishing deterrence unless the United States can credibly commit to using the weapons. This, I think, is hard to do. The main threat today is cyber-exploitation (i.e. espionage, theft, copying) that does not violate international law and that would not warrant any use of force under international law. I have a hard time understanding how a law-sensitive DOD will credibly commit to ever using cyber-weapons, or kinetic weapons for that matter, in response to even the most devastating cyber-exploitations.

#### Legal restrictions will only constrain America – maintaining military control of OCO’s crucial to prevent global cyberwar

**Baker 11** [Stewart, former official at the U.S. Department of Homeland Security and the National Security Agency, “Denial of Service,” Foreign Policy, Sept. 30, <http://www.foreignpolicy.com/articles/2011/09/30/denial_of_service>]

American lawyers' attempts to limit the scope of cyberwar are just as certain to fail as FDR's limits on air war -- and perhaps more so.¶ It's true that half a century of limited war has taught U.S. soldiers to operate under strict restraints, in part because winning hearts and minds has been a higher priority than destroying the enemy's infrastructure. But it's unwise to put too much faith in the notion that this change is permanent. Those wars were limited because the stakes were limited, at least for the United States. Observing limits had a cost, but one the country could afford. In a way, that was true for the Luftwaffe, too, at least at the start. They were on offense, and winning, after all. But when the British struck Berlin, the cost was suddenly too high. Germans didn't want law and diplomatic restraint; they wanted retribution -- an eye for an eye. When cyberwar comes to America and citizens start to die for lack of power, gas, and money, it's likely that they'll want the same.¶ More likely, really, because Roosevelt's bargain was far stronger than any legal restraints we're likely to see on cyberwar. Roosevelt could count on a shared European horror at the aerial destruction of cities. The modern world has no such understanding -- indeed, no such shared horror -- regarding cyberwar. Quite the contrary. For some of America's potential adversaries, the idea that both sides in a conflict could lose their networked infrastructure holds no horror. For some, a conflict that reduces both countries to eating grass sounds like a contest they might be able to win.¶ What's more, cheating is easy and strategically profitable. America's compliance will be enforced by all those lawyers. Its adversaries' compliance will be enforced by, well, by no one. It will be difficult, if not impossible, to find a return address on their cyberattacks. They can ignore the rules and say -- hell, they are saying -- "We're not carrying out cyberattacks. We're victims too. Maybe you're the attacker. Or maybe it's Anonymous. Where's your proof?" ¶ Even if all sides were genuinely committed to limiting cyberwar, as they were in 1939, history shows that it only takes a single error to break the legal limits forever. And error is inevitable. Bombs dropped by desperate pilots under fire go astray -- and so do cyberweapons. Stuxnet infected thousands of networks as it searched blindly for Iran's uranium-enrichment centrifuges. The infections lasted far longer than intended. Should we expect fewer errors from code drafted in the heat of battle and flung at hazard toward the enemy?¶ Of course not. But the lesson of all this for the lawyers and the diplomats is stark: Their effort to impose limits on cyberwar is almost certainly doomed.¶ No one can welcome this conclusion, at least not in the United States. The country has advantages in traditional war that it lacks in cyberwar. Americans are not used to the idea that launching even small wars on distant continents may cause death and suffering at home. That is what drives the lawyers -- they hope to maintain the old world. But they're being driven down a dead end.¶ If America wants to defend against the horrors of cyberwar, it needs first to face them, with the candor of a Stanley Baldwin. Then the country needs to charge its military strategists, not its lawyers, with constructing a cyberwar strategy for the world we live in, not the world we'd like to live in.

#### Executive flexibility is key to effective offensive cyber and deterrence

Bradbury 11 (Steven – partner @ Dechert, LLP, “The Developing Legal Framework for Defensive and Offensive Cyber Operations” March 2011, Cybersecurity: Law, Privacy, and Warfare in a Digital World, Harvard National Security Journal, Vol. 2)

Conclusion. So here’s my thesis: To my view, the lack of clarity on certain of these issues under international law means that with respect to those issues, the President is free to decide, as a policy matter, where and how the lines should be drawn on the limits of traditional military power in the sphere of cyberspace. For example, that means that within certain parameters, the President could decide when and to what extent military cyber operations may target computers located outside areas of hot fighting that the enemy is using for military advantage. And when a cyber attack is directed at us, the President can decide, as a matter of national policy, whether and when to treat it as an act of war. The corollary to all this is that in situations where the customs of war, in fact, are not crystallized, the lawyers at the State Department and the Justice Department shouldn’t make up new red lines — out of some aspirational sense of what they think international law ought to be — that end up putting dangerous limitations on the options available to the United States. Certainly, the advice of lawyers is always important, especially so where the legal lines are established or firmly suggested. No one would contend that the laws of war have no application to cyber operations or that cyberspace is a law free zone. But it’s not the role of the lawyers to make up new lines that don’t yet exist in a way that preempts the development of policy. 14 In the face of this lack of clarity on key questions, some advocate for the negotiation of a new international convention on cyberwarfare — perhaps a kind of arms control agreement for cyber weapons. I believe there is no foreseeable prospect that that will happen. Instead, the outlines of accepted norms and limitations in this area will develop through the practice of leading nations. And the policy decisions made by the United States in response to particular events will have great influence in shaping those international norms. I think that’s the way we should want it to work.

### at: deterrence fails

#### Deterrence works by changing the incentive model of adversaries.

Kramer et. al 12 (Franklin D. Kramer is a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He served as the assistant secretary of defense for international security affairs from 1996 to 2001. Stuart H. Starr is also a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He concurrently serves as the president of the Barcroft Research Institute. Larry Wentz is a senior research fellow in the Center for Technology and National Security Policy at the National Defense University., “Cyberpower and National Security”, p. 318)

Ends, Ways, and Means

The goal of a cyber deterrence strategy would be to influence an adversary’s decisionmaking calculus so decisively that it will not launch cyber attacks against the United States, its military forces, or its allies. Coordinated actions reduce the chances for attacker success, so that the dangers, costs, risks, and uncertainties of a cyber attack are perceived to outweigh any expected success, benefits, or rewards. In the case of an adversary who seeks to use threats of cyber attacks, or actual attacks, to coerce the United States into conduct that would serve its larger interests and goals, a cyber deterrence strategy will work if the adversary judges that this attempted coercion would not succeed and that the attack would provoke U.S. retaliation, resulting in a net strategic setback for the would-be attacker. For example, if Iran were to contemplate cyber attacks to try to coerce the United States into making political concessions in the Persian Gulf and Middle East, it might be deterred from this course if its decisionmakers were to judge that the cyber attack would not physically succeed in inflicting the desired damage; that even if the attack succeeded, the United States would not make the desired concessions; or that the United States would be likely to retaliate in ways that inflict unacceptable damage on Iran in return, in the cyber realm or elsewhere.

The same strategic calculus applies to Chinese use of cyber threats and attacks, as well as actions by other plausible adversaries in the cyber domain. Potential U.S. counteractions in such situations are encapsulated in the three principal ways of pursuing deterrence articulated in the JOC model: deterrence by denying benefits, deterrence by imposing costs, and deterrence by offering incentives for adversary restraint.

Deterrence by denying benefits entails credibly threatening to deprive the attacker of the benefits or gains being sought: convincing it that a cyber attack will not achieve its goals. Deterrence by imposing costs entails credibly threatening to impose costs, losses, and risks that are too painful to accept, thus convincing the adversary that punishment would outweigh any expected successes. Deterrence by encouraging restraint means convincing the adversary that not attacking will result in an acceptable, attractive outcome.

### 2nc deterrence o/w capability

#### Deterrence is the key to preventing war – perception of resolve outweighs actual capabilities

Kramer et. al 12 (Franklin D. Kramer is a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He served as the assistant secretary of defense for international security affairs from 1996 to 2001. Stuart H. Starr is also a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He concurrently serves as the president of the Barcroft Research Institute. Larry Wentz is a senior research fellow in the Center for Technology and National Security Policy at the National Defense University., “Cyberpower and National Security”, p. 318)

No cyber deterrence strategy can hope to be airtight to prevent all minor attacks. However, a strategy can increase the chances that major cyber attacks can be prevented; this could protect the United States and its allies not only from a single major attack but also from serial cyber aggressions and resulting damage. A worthwhile goal of a cyber deterrence strategy would be to transform medium-sized attacks into low-probability events and to provide practically 100 percent deterrence of major attacks.

A cyber deterrence strategy could contribute to other key defense activities and goals, including assurance of allies, dissuasion, and readiness to defeat adversaries in the event of actual combat. The goal of dissuading adversaries is crucially important. Thus far, the United States has not been noticeably forceful in stating its intentions to deter major cyber attacks and, if necessary, to respond to them with decisive force employing multiple instruments of power. Meanwhile, several countries and terrorist groups are reportedly developing cyber attack capabilities. Dissuasion of such activities is not an easy task: it requires investment in technical capabilities as well as building an internal consensus to employ these capabilities. If some of these actors can be dissuaded from entering into cyber competition with the United States and its allies, the dangers of actual cyber aggression will diminish.

How would a cyber deterrence strategy operate, and how can its potential effectiveness be judged? Deterrence depends on the capacity of the United States to project an image of resolve, willpower, and capability in sufficient strength to convince a potential adversary to refrain from activities that threaten U.S. and allied interests. As recent experience shows, deterrence can be especially difficult in the face of adversaries who are inclined to challenge the United States and otherwise take dangerous risks. In cases of failure, deterrence might well have been sound in theory but not carried out effectively enough to work. The aggressions of Saddam Hussein, Slobodan Milosevic, and al Qaeda might not have been carried out had these actors been convinced that the United States would respond with massive military force. These aggressions resulted because of a failure to communicate U.S. willpower and resolve, not because the attackers were wholly oblivious to any sense of restraint or self-preservation, nor because the logic of deterrence had lost its relevance.

## military

### 2nc cyberattacks

#### Attacks won’t escalate to war

Gray 13 [COLIN S. GRAY is Professor of International Politics and Strategic Studies at the University of Reading, England, worked at the International Institute for Strategic Studies and at the Hudson Institute before founding the National Institute for Public Policy, Author of 25 books, Strategic Studies Institute, April 2013, "MAKING STRATEGIC SENSE OF CYBER POWER: WHY THE SKY IS NOT FALLING", http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1147.pdf]

While much about cyber is cloaked either in official secrecy or is shrouded in a fog of uncertainty because of the subject’s immaturity, nonetheless it is safe enough to say now that cyber peril should not be regarded as a nuclear-like danger or set of dangers. This is not necessarily to claim that we should be relaxed about the inherent risks in our computer-networked existence, but it is to insist that cyber attack is not at all credibly comparable to a nuclear option. This claim is controversial to those of a “Cybergeddon” persuasion, but it would be a useful step forward for strategic net assessment were the more extreme disaster scenarios labeled clearly as the nonsense that they are. Krepinevich is convincing when he argues that: ¶ [D]espite the assertions of some, it also seems likely that cyber weapons have nowhere near the ability to inflict catastrophic destruction as that of a major nuclear attack. . . . Simply put, nuclear weapons remain in a class all their own.44¶ The same judgment is advanced by a technically more expert source on cyber, Martin C. Libicki, who holds that “[n]uclear warfare trumps all other forms.”45 Libicki may be wrong, but he advances and defends this conviction with no little authority. Given our ignorance of future technical feasibility, it has been necessary to examine the full range of possibility on the scale of threats by cyber. But the extra-physicality of the menace, and its substantially discretionary character—dependent as the menace has to be on our technical and tactical choices—means that nuclear menace continues unchallenged as a survival-level danger that could be caused by hostile strategic intent.¶ In short, on the evidence of careful, if limited, assessment to date, cyber is not akin to nuclear peril, and hypothetical nuclear analogies are more likely to mislead governments and frighten the public needlessly than they are to educate and warn prudently.46¶ Analogy, Tactical and Strategic. ¶ It matters profoundly whether nuclear analogy is appropriate for cyber. It is ironic, and it may even be one of strategic history’s few paradoxes, that somehow we have learnt to live with ineradicable nuclear facts. This is reality, despite the continuing awesome uncertainties that surround its likely meaning if expressed in violent military behavior. To some, indeed possibly to many, people who have sought to understand cyber power, its possibilities have appeared strategically unbounded. It can be difficult, if not impossible, to prove a negative. How can we be sure that cyber threats are not of a scale, notwithstanding their definitional nonphysicality, that begs plausibly for comparison with what is now usually regarded in the main as yesterday’s menace—nuclear attack?¶ Several categories of response can be offered to the alleged relevance of nuclear analogy, but suffice it for now to cite but two. First, except for highly unusual cases, cyber power is confined in its damaging effects to cyberspace. This is not to understate the problems that can be caused by cyber attack, but it is to claim firmly that the kind of damage and disruption that cyber might affect cannot compare with the immediate and more lasting harm that nuclear weapons certainly would cause. This is not guesswork. It is simply foolish to argue that understanding of cyber peril can be much advanced by nuclear analogy.

### 2nc retaliation

#### No incentive to retaliate.

Libicki 12 “Crisis and¶ Escalation in¶ Cyberspace” Martin C. Libicki (Senior Management Scientist at RAND, focusing on the impacts of information technology on domestic and national security, He was also the editor of the RAND textbook, New Challenges New Tools for Defense Decisionmaking.) (The RAND Corporation is a nonprofit institution that helps improve¶ policy and decisionmaking through research and analysis) RAND Project Air Force, written for the Air Force. (The research described in this report was sponsored by the United States¶ Air Force under Contract FA7014-06-C-0001) ISBN: 978-0-8330-7678-6. Published 2012.

In great contrast to physical war, in which a failure to respond¶ means being overrun, the direct security implications of doing nothing¶ in the face of a cyberattack may be small. Cyberattacks, even a series of¶ them, may be less like physical warfare and more like raids (but with¶ mostly temporary, nonkinetic effects), and states that do not respond to¶ raids are not necessarily overrun as a result. Because retaliation cannot¶ disarm the attacker, the failure to react has no bearing on the attacker’s¶ ability to do damage—only its willingness.

### 2nc no modeling

#### Cyberweapons are inev --- US restraint does nothing --- norm setting is utopian

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

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

#### Pandora’s box has already been opened --- cyber-war inevitable

Mikko Hypponen 12, an authority on cybercrime and one of Foreign Policy’s ‘Top 100 Global Thinkers,’ is the chief research officer at F-Secure Corporation, “A Pandora’s Box We Will Regret Opening,” June 5, NYT, http://www.nytimes.com/roomfordebate/2012/06/04/do-cyberattacks-on-iran-make-us-vulnerable-12/a-pandoras-box-we-will-regret-opening

If somebody would have told me five years ago that by 2012 it would be commonplace for countries to launch cyberattacks against each other, I would not have believed it. If somebody would have told me that a Western government would be using cybersabotage to attack the nuclear program of another government, I would have thought that's a Hollywood movie plot. Yet, that's exactly what's happening, for real.¶ Cyberattacks have several advantages over traditional espionage or sabotage. Cyber attacks are effective, cheap and deniable. This is why governments like them. In fact, if Obama administration officials would not have leaked the confirmation that the U.S. government (together with the Israelis) was behind Stuxnet, we probably would have never known for sure.¶ In that sense, it's a bit surprising that the U.S. government seems to have taken the credit ­ and the blame ­ for Stuxnet. Why did they do it? The most obvious answer seems to be that it's an election year and the voters like to see the president as taking on adversaries like Iran. But we don't really know.¶ The downside for owning up to cyberattacks is that other governments can now feel free to do the same. And the United States has the most to lose from attacks like these. No other country has so much of its economy linked to the online world.¶ Other governments are already on the move. The game is on, and I don't think there's anything we could do to stop it any more. International espionage has already gone digital. Any future real-world crisis will have cyberelements in play as well. So will any future war. The cyberarms race has now officially started. And nobody seems to know where it will take us.¶ By launching Stuxnet, American officials opened Pandora's box. They will most likely end up regretting this decision.

#### Can’t stop cyberweapons --- incentives to use are too high

Dr. Paul Kaminski 13, Chairman of the Defense Science Board Task Force on Resilient Military Systems & PhD from Stanford, “Department of Defense Defense Science Board Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,” January, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

There is no single silver bullet to solve the threat posed by cyber-attack or warfare. Solving this problem is analogous to previous complex national security and military strategy developments including counter U-boat strategy in WWII, nuclear deterrence in the Cold War , commercial air travel safety and countering IEDs in the Global War on terrorism . The risks involved with these challenges were never driven to zero, but through broad systems engineering of a spectrum of techniques, the challenges were successfully contained and managed. ¶ There are several characteristics of the cyber challenge that collectively thwart our attempts to discover a closed-form solution to this national security issue. First, DoD’s comprehensive dependence on this vulnerable technology is a magnet to U.S. opponents. DoD’s dependency is not going to be reduced and will continue to grow. Thus, the adversary is not going away and their attraction to this weakness will increase. This adversarial persistence yields a never-ending challenge.¶ Secondly, there are no technical approaches that will comprehensively protect DoD against a determined adversary. DoD’s diligent work over decades attempting to drive inherent vulnerability out of these systems and components has resulted in some progress, although DoD has barely begun to address the daunting problem of operationally introduced vulnerabilities into systems which is compounded by the large dependence on the global supply chain. In the face of the evolving cyber threat, DoD must recognize the limits to vulnerability reduction and the effectiveness of protection mechanisms and move to employ the threshold of “good enough ” and work to reduce overall risk by managing all three risk parameters from a systems perspective.¶ Third, while there are many tests to demonstrate the vulnerability or weakness in a system, there will never be a test that demonstrates or proves the security of a system. This fact reinforces the need to seek “good enough” and the enduring existence of residual uncertainty. ¶ Finally, because the opponent’s advantage in exploiting/compromising /attacking DoD’s information technology is substantial (game - changing), they will be highly motivated in their pursuit, innovative in their approach, and adaptive to U.S. strategy. The adversary gets a vote and this brings us back to the never-ending challenge. (However, they have many of the same risks to their systems).

### at: critical infrastructure impact

#### No impact or escalation to attacks on critical infrastructure

Lewis 10 James A. Lewis (Director and Senior Fellow, Technology and Public Policy Program at the Center for Strategic and International Studies, formerly part of the Senior Executive Service (Foreign Service Officer) for the Department of State and Commerce, UN Group of Government Experts on Information Security, US Southern Command for Operation Desert Shield) “Thresholds for Cyberwar” Center for Strategic and International Studies. September 2010. Attacks on infrastructure will have only a minimal effect in short clashes of only a few months,¶ “go-with-what-you’ve-got” wars. The target nation’s industrial capacity and the production of¶ new weapons will be less important in these wars. We will not be fighting industrial-era wars of¶ attrition between large regular forces and lasting for years. An opponent could successfully¶ disrupt critical infrastructure, and if the target nation’s leadership was able to manage the¶ political implications of this, see little or no effect on opponent military capacity. It takes time¶ for a disruption of industrial capacity to translate into a degradation of effectiveness in fielded¶ forces. Attacks must be cumulative and persistent, to overcome opponent resilience and¶ response. A short war could be over before cyber attack on critical infrastructure provided¶ significant advantage. The effect of attacks on infrastructure is easy to overestimate. Cyber attacks will resemble those¶ actions where guerrillas plow up substations or pull down power pylons to remind the opposing¶ government that they are there and to erode its legitimacy. Guerrillas do not expect to win as a¶ result of these attacks. With the right leadership, large industrial nations are able to absorb many¶ blows before there is significant damage to their ability to wage war. In some conflicts, in fact,¶ there is a reluctance to do too much damage to infrastructure on the grounds that the attacking¶ force itself will soon rely on it. In state versus state conflict, the issues for attacks on¶ infrastructure in a peer/near-peer are if the military benefit of disabling infrastructure for some¶ periods are outweighed by the risk of escalation, and in a large state/small state conflict whether¶ the damage will harm any “nation-building’ required in a post conflict situation.

**Threats are exaggerated – infrastructure has inherent checks to prevent shutdowns**

**Derene, 09** – senior technology editor of Popular Mechanics, (Glenn, “How Vulnerable is U.S. Infrastructure to a Major Cyber Attack?”, Popular Mechanics Magazine, October 1, 2009, http://www.popularmechanics.com/technology/military/4307521)

"Honestly, I think **the threat is overblown**," says Bruce Schneier, author of Schneier on Security. "**The risks today are due more to errors than to malicious intent**." He sees Donahue's story as nothing more than a tenebrous rumor. Nevertheless, Schneier thinks vulnerabilities in infrastructure will eventually become a real national-security threat. The problem is that the errors that Schneier refers to can cause bad things to happen. **Much of computer hacking is predicated on exploiting glitches in commonly used systems**. Such exploits on a Windows PC are irritating, but at a nuclear facility, they can be unnerving. In August 2006, a glitch shut down the Browns Ferry nuclear power plant in northern Alabama. Plant administrators lost control of recirculation pumps on one of the plant's reactors because of excessive data traffic on the control-system network. The plant was forced to go offline temporarily. **Nuclear plants are designed to shut down in the event of major malfunctions to prevent a Chernobyl-style catastrophe**. But they also generate almost 20 percent of U.S. power. What if a hacker exploited a coding error in a cooling system to shut down a sizable piece of the nation's power supply? Incidents of digital malfunctions that cause danger to human life are rare, but such events have happened. In June 1999, in Bellingham, Wash., shortly before a routine delivery of gasoline by the Olympic Pipe Line Co., a worker updated a database for the company's pipeline computer-control system. According to a report by the National Transportation Safety Board, a simple typo in the database caused the system to fail, disabling remote control for the pipeline's operators, 98 miles away in Renton, Wash. Pressure began to build in the line, so the operator issued a command to open a secondary pump to relieve it, but the system was unresponsive. A weak point in the pipeline ruptured, releasing 237,000 gal of gasoline into nearby Whatcom Creek. An hour and a half later, the gasoline ignited. The ensuing fireball scorched more than a mile of riverbank, killing three people, including two 10-year-old boys, and damaged the city's water-treatment facility.

# 1nr

## nietzsche

### 2nc overview

#### 9/11 tore a rift in the nation’s identity which the government inscribed with a narrative of victimhood – the aff reasserts this innocent helplessness by placing the responsibility of protection squarely in the hands of the law – that erodes agency while assuaging our civil consciousness allowing the government to wage endless wars – use the ballot to jump from the twin towers in the face of the 1ac’s catastrophe – that disruption of sovereign control through willful demise is a prerequisite to any productive action

**Duschinsky, ’11** Professor at University of Northumbria (Robbie Duschinsky, Spring 2011, “Nietzsche: Through the Lens of Purity,” Journal of Nietzsche Studies Iss. 41)//CC

By contrast, Joanne Faulkner demonstrates both the salience of the theme of purity in Nietzsche and the important contemporary stakes in conducting such a reading.23 In the context of examining discourses of innocence in post–9/11 reconstructions of American identity, Faulkner proposes that at the core of social contract theory is an assumption that a state of personal and communal innocence has to be set aside to enter into the dirtying, compromised, fallen world of civil association. For Faulkner, it is this guilt that, as Nietzsche states, is the precondition of sovereign individuals who can make promises and who take responsibility for themselves and their actions. The implication is that the innocent can have no effective political agency and must be protected. The innocent victims of 9/11 have mandated war abroad and the curtailment of civil liberties at home, as "an eternally aggrieved icon of national identity: a perennially threatened and victimized creature of ressentiment who 'in order to exist first needs a hostile external world.'"24 Against this, Faulkner sets Nietzsche's notion of the innocence of becoming, which insists that there is no transcendent realm against which our lives can be judged. The innocence of becoming poses rather that creative activity and choices, based on the available options that chance presents to the individual, serve as their own justification.25 The metaphysical purity of innocent victim-hood has made certain bellicose actions on the part of state institutions appear as natural and seemingly neutral. Thus Faulkner's work indicates the stakes in using Nietzsche for considering alternative ways of seeing innocence and purity.

#### the 1ac is the will to will – when power reaches its peak it turns back on itself – now the government must fight itself – that’s the death-knell of civilization

**Kroker 2k11.** Arther Kroker, professor of political science at Victoria University, director of the Pacific Centre for Technology and Culture, “The Arab Spring: The Contradictions of Obama’s Charismatic Liberalism,” CT Theory, <http://www.ctheory.net/articles.aspx?id=679>, January 27th, 2011

Delivered on June 4, 2009 at Cairo University, this speech provided Obama with an opportunity to address the world community of Muslims. The setting of the speech was politically volatile, with Egyptian faculty and students in attendance taking careful note of the American occupation of Iraq as well as the American invasion of Afghanistan. In the United States, powerful media voices demanded a new crusade against Islam while in the Muslim world the most violent forms of political resistance against American soldiers were widely viewed as morally justified. To the highly selective targeting of Muslims by all the policing strategies involved in the War on Terror, the Islamic counter-response was as sudden as it was terminal -- the destruction by suicide bombs, by IEDs, by the sword, of American targets of opportunity. To the American military's documented acquiescence in war crimes by the Shia-dominated security forces against Sunni Muslims, young Arab resistance fighters sought out opportunities for revenge killings that would have maximum media impact. In all this, Obama was no innocent. His endorsement of the concept of a "Just War" motivated his strong and persistent support for the invasion of Afghanistan. While he may have decried the use of extra-judicial procedures such as the rendition of political suspects to torture chambers in Egypt, Jordan, Syria, and Eastern and Central Europe, his concern with American security led him to support draconian surveillance and policing tactics in America, including bunkering North America in a Perimeter Defence. For all his protestations against Bush's Guantanamo, the prison has still not been closed, and Obama has proved reluctant to provide the full measure of judicial protections for CIA nominated terrorist suspects. All this to say, the Obama that rose tospeak in that sun drenched Cairo day was a fully contradictory figure, compromised by a war raging not only in America itself but in his own liberal heart--ideals versus realities, reason versus passion. As the French philosopher Jean-Paul Sartre might have said, Obama was entangled in the "practico-inert" of the War on Terror with all its political nomenclature concerning bodies that needed to be secured by the power of government and bodies that don't matter and, hence, could be **disavowed, excluded, marginalized**. At the same time, by force of political conviction Obama was driven to transcend the limitations of his political predicament. In this sense, his speech in Cairo was a way of throwing his general political project into the future, breaking with the past in order to negotiate new pathways through a fully uncertain future. This is evident in the first measures of the speech that began with a political confession of responsibility: We meet at this time of great tension between the United States and Muslims around the world -- tension rooted in historical forces that go **beyond any current policy debate**. The relationship between Islam and the West includes centuries of coexistence and cooperation, but also conflict and religious wars. More recently, tension has been **fed by colonialism** that denied rights and opportunities to many Muslims, and a Cold War in which Muslim-majority countries were often treated as proxies without regard to their own aspirations. Moreover, the sweeping change brought by modernity and globalization led many Muslims to view the West as hostile to the traditions of Islam. There we have it: colonialism as the source of political disenfranchisement of Muslims and a Cold War that resulted in many "Muslim-majority countries" being treated as pawns in the larger games involved in the clash of imperial powers. Political history of this order surely sows the seeds of distrust and suspicion among subject populations, providing fertile ground for the growth of resistance networks among those who refuse to bend to the will to colonial domination. For Obama, the results are as self-evident as they are dangerous. Violent extremists have exploited these tensions in a small but potent minority of Muslims. The attacks of September 11, 2001 and the continued efforts of these extremists toengage in violence against civilians has led many in my country to view Islam as inevitably hostile not only to America and Western countries, but also to human rights.All this has bred **more fear and more mistrust**. If the aim of **effective political rhetoric** is to **frame the interpretation of events in advance**, implicitly def**ining what is considered to be intelligible and consequently within the boundaries of moral acceptability and what is considered to be unintelligible and thus to be disavowed**, marginalized, and excluded, Obama's opening statement is noteworthy. Rather than side with majoritarian American opinion that continues to hold that the events of 9/11 had no historical context, representing an irrational act of extremist violence against an unsuspecting nation, Obama does something different. He brings into intelligibility the events of 9/11, noting that the story of domination and power that was implicit to the history of colonialism and the Cold War finds its inevitable result in what the historian, Chalmers Johnson, once described as "**blowback**." [[1]](http://www.ctheory.net/articles.aspx?id=679#_edn1) Of course, Chalmers went to his death noting that America was caught up in a fatal mythological spiral associated with the rise and fall of empires. From Chalmers' perspective, the migration of the United States from Republic to Empire has **inevitably fatal consequences**, committing American future to the classic rhythms of political mythology whereby the project of grasping for power, particularly the power of global domination, creates in its wake unpredictable historical consequences: **melancholic subjectivity as the keynote of American subjectivity, gathering hints of nemesis abroad, followed by spectacular acts of revenge-taking by subjected populations**. Perhaps it was with something like this in mind that led Obama to break with the harsh policies of the Bush regime, encapsulated in all its bitterness and sense of American exceptionalism in the phrase -- "You're either with us or against us." Presiding in the bleak aftermath of the Bush administration with poll after poll confirming profound mistrust of American intentions in Muslim countries, Obama chose not to evade issues of mistrust, fear and skepticism but to do the opposite, namely to turn directly into the wind of Islamic discontent. In doing so, **Obama's Cairo speech is a lesson in the metaphysics of power**. While the Bush administration implicitly operated on the basis of a theory of power that held that power must always expand, must always seek out new opportunities for control, that the world must be subjected to military policies aimed at "full spectrum dominance," Obama's theory of power is different. Perhaps at some point he might have reflected on Nietzsche'sThe Will to Power wherein Nietzsche argued that power **always seeks external resistances in order to thrive**, that power establishes boundaries and limits in order both to test its strength as well as to mobilize its energies. In the most mature stages of the development of power, a period that Nietzsche described as "**completed nihilism**," the will to power, **finding itself without external enemies of merit**, turns back on itself, **making of itself its own opposition**. Considered in terms of political theory, while the Bush administration represented the highpoint of American will to power before its political fortunes stalled in the face of gathering global opposition, the Obama administration may be **the quintessential expression of power as the will to will**, that point where power, **having tested its outer limits, turns back upon itself**. In retrospect, the Bush political administration probably represented the last bacchanalian feast of power in its purest form. Here, the power of American empire having no manifest enemy was finally liberated to be power in its final stage -- **power as a pure sign**. Globally hegemonic in its military claims to "full spectrum dominance" of time and space as well as "metabolic domination" of the world population, the feast of American power expanded with **implosive energies** -- a financial sector that transformed the machinery of capitalist transactions into an economic landscape where money in the form of credit finally **floated free of any solvency requirements**; a housing sector that increasingly operated on the basis of purely virtual value standards, with the value of homes measured by aesthetic standards; and **a consumer sector where the delusional economy of zero credit requirements** made individual over-indebtedness a structural requirement of **the operation of the system as a whole**.

#### death is inevitable, they can’t stop it. Proves the only thing that matters is the way we orient ourselves toward life. Their impact scenarios are irrelevant where living is “not good enough”

Nietzsche 1886 [fredrich, “beyond good and evil”, aph # 225, pg. 342]

Whether hedonism, or pessimism, or utilitarianism, or eudaimonianism (6)—all these ways of thinking, which measure the value of things according to pleasure and pain, that is, according to contingent circumstances and secondary issues, are ways of thinking in the foreground and naïveté, which everyone who knows about creative forces and an artistic conscience will look down on, not without ridicule and not without compassion. Compassion for yourself—that is, of course, not compassion the way you mean the term: it's not pity for social "needs," for "society" and its sick and unlucky people, with those depraved and broken down from the start, and with the way they lie on the ground all around us—even less is it compassion for the grumbling oppressed, the rebellious slave classes, who strive for mastery—they call it "Freedom." Our compassion is a higher compassion which sees further—we see how man is making himself smaller, how you make him smaller—and there are moments when we look at your compassion with an indescribable anxiety, where we defend ourselves against this compassion—where we find your seriousness more dangerous than any carelessness. You want, if possible—and there is no wilder "if possible"—to do away with suffering. What about us? It does seem that we would prefer it to be higher and worse than it ever was! Well being, the way you understand it, that's no goal. To us that looks like an end, a condition which immediately makes human beings laughable and contemptible, something which makes their destruction desirable! The culture of suffering, of great suffering, don't you realize that up to this point it is only this suffering which has created all the things which raise man up?

### 2nc fw

#### Their framework makes them extratopical—resolved means to personally think about things—fiat is extratopical and allows them to claim absurd solvency arguments that we can’t predict, which is a reason to reject the team.

**AHD 2k6.** American Heritage Dictionary

resolved v. To cause (a person) to reach a decision.

#### Their framework skips the important parts of policymaking – internal link turns their offense

**Carpentier 2011** (Nico, asst prof comm @  Vrije Universiteit Brussel “Policy’s Hubris: Power, Fantasy, and the Limits of (Global) Media Policy Interventions” The Handbook of Global Media and Communication Policy, First Edition.)

This discussion on the nature of policy brings us to an encounter with a set of key assumptions which will be theorized here as fantasies, using a Lacanian framework.4 The reason for using this framework is that there are implicit claims embedded within policy debates that are partially (discursive) power strategies but, partially also, fantasies about control and harmony. And within a Lacanian framework, fantasy beholds the promise of the unachievable wholeness and the harmonious resolution of social antagonism. Although this access to the Real is impossible, the fantasy, as such, and the desire for wholeness and harmony that lies behind it remain crucial driving forces and feed into the strategies that the diversity of (policy) actors develop. This also implies that these fantasies become part of our social realities in many different ways, for instance, as utopian driving forces for political activity and as discursive strategies for legitimating policies. A first fantasy has already been mentioned in the discussion about the classic perspective on policy. In the introductory part of his discussion of media policy, which carries the title “Is policy political?,” Freedman (2008: 2) refers to the mechanical perspective of policy-making, which marginalizes “political agency in favour of administrative technique and scientific principles” and becomes “the domain of small thoughts, bureaucratic tidiness and administrative effectiveness.” This fantasy of isolating policy from politics (and from the political) is a protective strategy to generate a harmonious and consensual zone within the social, out side political conflicts and antagonisms, which is believed to be governed by bureaucratic principles and/or legalistic mechanisms. This way of thinking is very much related to the ideology of “endism,” which proclaimed the end of ideology and claimed that this would lead to the replacement of politics by a managerial culture (see, for instance, Burnham (1941) and Bell (1960) ). More contemporary critical frameworks refer to (and critique) the post-political and the post-democratic, where the latter is defined by Rancière (2007: 88) as “the rule of the principle of unification of the multitude under the common law of the One.” Not only does this lead to the conflation of the “pays légal” and the “pays reél” (to use the two marvellous French concepts that allow us to distinguish between legislation and social practice), but it also becomes a form of strategic power that allows for the mobilization of actors (and their minds and bodies), discourses, and objects to legitimize the hegemonization of specific political projects by reverting to the claim that these projects are outside the political. However important this fantasy may be, it is structurally frustrated by the permanent reemergence of antagonisms and conflicts. This brings us to Mouffe’s (2005: 9) argument that the political is structurally defined by “power, conflict and antagonism.” Her work challenges the post-political status quo, which assumes that a societal consensus is reached or reachable. Not surprisingly, the last sentence of her 2005 book On the Political is a plea for “abandoning the dream of a reconciled world that would have overcome power, sovereignty and hegemony” (Mouffe 2005: 130; my emphasis). Through the contingency of the social, any hegemony and social imaginary, however phantasmagorically comforting it may be, remains vulnerable to contestation, and even the most sedimented and takenfor-granted certainties can become unfixed and fluid, as they are permanently vulnerable to rearticulation. In Mouffe’s (2005: 18) words: “What is at a given moment considered as the ‘natural’ order – jointly with the ‘common sense’ which accompanies it – is the result of sedimented practices; it is never the manifestation of a deeper objectivity exterior to the practices that bring it into being.”

#### the 1nc was an interpretation of the world through art – that’s the only way – voter issue

**Strong, ‘3** distinguished professor in the Department of Political Science at the University of California, San Diego (Tracy B. Strong, “Where are we when we are beyond good and evil,” 24 Cardozo L Rev.)//CC

The spirit that would become a free spirit at now a midway point, where he flies about the world in a kind of “curiosity mingled with tender contempt,” unattached to anything even by love or hatred. One step more and the distance of the midpoint fades in the astonishment of that which is at hand. He is besides himself, literally in ecstasy. This is still not the final stage; it is instead a stage in which the spirit realizes suddenly that the very distance it had from the world—its “tender contempt”—was itself generative of “for and against” and was, in that way, an injustice against the world. The astonishment of the close at hand is a consequence of the realization that one must not rest in the position that one’s critical distance provides. “You shall become master (Herr) over yourself; master also over your own virtues. Before they were your masters.”46 (Thus, to recall, he writes to Lou Salom6: “The old word once again: become who you are. First you must be liberated from your fetters; then you must be liberated from your liberation.”). The realization here is that the one becomes the perspective that one takes. But it is clear that perspectivalism is not a recommendation for a moderate and tolerant pluralism, nor even an agonistic one. Nietzsche clearly, as Babich notes, “does not claim the same value or right for every perspective.”47 In relation to morality, what does this mean? What kind of understanding is present here? What does he know? In the 1886 preface he added to the new edition of the Birth of Tragedy, Nietzsche notes that what he had hit upon in that book was the question of “the problem of knowledge—das Problem der Wissenschaft” a problem that cannot be understood on knowledge grounds alone. Nietzsche sees himself as having wanted to argue that the preconditions for the possibility of knowledge lies not in knowledge itself, but in art; and art cannot be understood except in the optic of “life.” He calls attention to how bad the book is in his present judgment and then indicates that it “settled accounts more with the profanum vulgus of the so-called educated than with the ‘people’.” His word for the operation that produces this knowledge (the knowledge, that is, that absolute truth is an illusion and that this illusion is the source of nihilism) is “what is Dionysian.” This means, in the end, to look at morality from the perspective, the optic, of life. What does this mean? Life, he tells us, “rests on appearance (Schein), art, deception, optics, the necessity of the perspectival and of error.” If you believe in a better life— Nietzsche’s next sentence starts “Christianity was from the beginning.. ..”—then you believe in a life that is not appearance. Yet a perspectival understanding of the world must always experience itself as inadequate, as refusing the last word. It means, in other words, that one knows that the world is always more than one makes of it, and yet that our knowledge of the world is what knowledge is. This means, however, that any claim of finality of knowledge is necessarily wrong. What difference does it then make to say that by virtue of what one is one does injustice to the world, that any structure of the world must acknowledge its own contingency, that is that one’s understanding of the world must always be defeasible? It means a number of things: This world must ultimately find itself condemned by virtue of the fact that it is only what one makes of it. This means that we must live in injustice to the world. What difference does it make to say that by virtue of what one is, one does injustice to the world, that is, that one must always understand the world in a manner that is principally and foundationally defeasible? It means at least that this world (the only world) must be seen as wanting when viewed from a moral and epistemological framework. In turn, this implies that the privileging of morality and epistemology—any structure of knowledge—will always be self-defeating.\*8 Yet this is not simply the recognition of the epistemological claim that one can never make final sense of the world. I can go now to a fuller text of a passage cited at the beginning of this essay. At the beginning of the fourth book of The Gay Science, Nietzsche finds himself making a New Year’s resolution. The recognition of the coterminousness of the sum and the cogito (“Sum, ergo cogito: cogito, ergo sum. Today each permits himself to express his desire, his most precious thought”)49 leads to this wish: “I want to learn more and more how to understand necessity in things as the beautiful in itself.” As noted above in the drafts of this version, Nietzsche had followed these words with, “[m]ay I weigh more and more with the pans of an aesthetic scale and less and less with those of a moral one.” Hence, in the 1886 preface to the Birth, we find a sentence that revises the most famous claim of the Birth. In that passage, he writes: “It is only as an aesthetic phenomenon that the existence of the world (Dasein der Welt) is justified.”50 Slight but important variations have come about. This sentence had appeared twice in the Birth and reads the first time: “It is only as an aesthetic phenomenon that existence (Dasein) and the world is eternally justified.” The second time it reads: “It is only as an aesthetic phenomenon that existence and the world appear justified.”51 Noteworthy is Nietzsche’s hesitation in the body of the text between “is eternally” and “appear.” The final formulation of this matter as “is” justifies the understanding that appearance, eternality, and being have finally come together in Nietzsche’s thought. Furthermore, in the 1872 text, existence and the world were separated, as he was still responding to an apparent Schopenhauerism that there is something behind the world of appearance. Now he writes of the Dasein of the world. As he himself notes, he had reasons to engage in a “self-critique.” He had finally come to the full understanding that there was no beyond. It is in this context that we can understand precisely what Nietzsche meant by a “lawgiver.” It is worth noting in this context that his admiration for the “Pre-Platonic” philosophers, as he noteworthily calls them, is for them as Wissenschaftlicher and as political men. Empedocles, who for Nietzsche might have provided a political alternative to Socrates, was a poet, religious teacher, statesman, physiologist (i.e., one of the physiologoi, those who understood physis) and, one supposes, a philosopher.

### 2nc at perm

#### The perm bankrupts the alt – there is no middle ground for their motivations

**Wrisley No Date** (George, Prof of Philosophy @ U Iowa, “What Should Our Attitude Towards Suffering Be,” Nietzsche and Suffeirng- A Choice of Attitudes and Ideals, <http://www.google.com/search?hl=en&q=site%3Ageorgewrisley.com+What+Should+Our+Attitude+Towards+Suffering+Be&aq=f&oq=&aqi>=) Zanezor

How should we comport ourselves to the suffering we find in our lives? When touching a hot stove or confronted with danger, our natural reactions are to pull back, to flee, to find safety. In general it seems that we naturally shy away from discomfort and pain—suffering of all types. The child laments his boring afternoon and the adult fears the impending death of a parent and the subsequent anguish the loss will bring, hoping and wishing they will never come. Suffering, it seems, is quite rightly seen as undesirable. However: When a misfortune strikes us, we can overcome it either by removing its cause or else by changing the effect it has on our feelings, that is, by reinterpreting the misfortune as a good, whose benefit may only later become clear. So, should we seek to abolish suffering as far as we can by removing its cause, or should we attempt to change our attitude toward suffering such that it is no longer seen as (always) undesirable? Taking Nietzsche seriously when he says that it is the meaning of our suffering that has been the problem, I will attempt to indirectly answer this question by looking at two possibilities found in Nietzsche for giving meaning to our suffering. The first possibility concerns a religious ethic that, according to Nietzsche, views suffering as undesirable, but which ultimately uses mendacious and deleterious means to provide a meaning for human suffering. The second possibility concerns the extent to which we can say Nietzsche endorsed the idea of giving meaning to suffering through acknowledging its necessary role in human enhancement and greatness. Since the religious ethic sees suffering as undesirable and thus something ultimately to be avoided (being itself the paradigmatic means for easing suffering), and the means it uses to give suffering meaning are ultimately mendacious, I will argue that if Nietzsche is significantly correct in both his attack on religious morality and his alternative ideal, we can take this as evidence that the avoidance of suffering is not the proper attitude. Unfortunately, I will not be able to address the question of whether Nietzsche is significantly correct in this paper. Secondly, given Nietzsche’s positive alternative—one that embraces the necessary role suffering has for the enhancement of human life—I will argue that we can take this as evidence that it is our attitude toward suffering that needs to be modified, i.e., we should modify so that we no longer see suffering as something to be avoided. Because of this, the middle position of avoiding suffering when possible and then seeing its positive attributes when it does occur does not recommend itself. That is, since it will be argued that suffering has a positive and necessary role to play, to seek to avoid it as far as possible and then to acknowledge its positive aspects when it does occur, is not really to acknowledge and accept suffering’s positive and necessary role. However, as we will see, all of this is complicated by the issue of the order of rank as found in Nietzsche’s writings.

### at may

#### May is silly – there are no objective values one can struggle against – their card supports Hitler’s struggle to eradicate the Jews as much as it does the plan

**Curmudgeon 11** [September 14, 2011, The Curmudgeon's Attic, Pseudonymn of anonymous philosopher, J.D., University of Texas School of Law, “The Thing As It Is A Reply to Todd May’s “The Meaningfulness of Lives” in the New York Times”]

Todd May, a professor of philosophy at Clemson University, wrote this article as part of a philosophy series, The Stone, in something called The Opinionater (online content only) in the New York Times. Because I’ve had lunch and need something meaningful to do with my life until my next meal (you’ll understand the reference if you read to the end of the post), allow me to parse Mr. May’s observations, in the process, hopefully providing some clarity: *Who among us has not asked whether his or her life is a meaningful one? Who has not wondered — on a sleepless night, during a long stretch of dull or taxing work, or when a troubled child seems a greater burden than one can bear — whether in the end it all adds up to anything? On this day, too, when many are steeped in painful reminders of personal loss, it is natural to wonder about the answers.* Indeed, I have wondered these very things myself. Does it all add up to anything? The fact of one’s existence is unalterable. Descartes told us we know we exist because we can think about whether or not we do. But what does it mean for the fact of one’s existence to add up to anything? Nothing that we do will be remembered for long after we’re gone. Even the extravagant pains Egyptian pharaohs took to preserve their existence only haltingly succeeded, and they go back only about four or five thousand years. So **if “adding up to anything” means that we will be eternally remembered by other humans,** then **no, our lives don’t add up to anything**. But if it instead means that we are a tiny link in an eternal chain of events in space-time, specks in a vast universe to be sure, but still, specks, then the fact that we exist or existed adds up to as much as it possibly can. *A meaningful life is distinct from a happy life or a morally good one.* I just love philosophers that offer platitudes like this without offering any supporting reasoning. How do we know a meaningful life is distinct from a happy life or a morally good one? Perhaps just because the words have different meanings? Can a happy life be meaningful? How about a morally good one? Is meaningfulness decided by others, or by the one who is actually living the life? Happiness, we know, is subjective. Hitler may have been happy, and his life had great meaning, if meaning is determined by the effect one’s life has on others, and several million German citizens apparently thought it to be a morally good one at some point or another. So is this philosophical exegesis pointing us to meaningful, happy and moral life modeled after Hitler’s? *The philosopher Jean-Paul Sartre thought that, without God, our lives are bereft of meaning. He tells us in his essay “Existentialism,” “if God does not exist, we find no values or commands to turn to which legitimize our conduct. So, in the bright realm of values, we have no excuse behind us, nor justification before us.” On this view, God gives our lives the values upon which meaning rests. And if God does not exist, as Sartre claims, our lives can have only the meaning we confer upon them.* For Sartre, meaningfulness is more or less completely subjective. God’s existence can not be proved or disproved. God is a matter of belief, which is, of course, subjective. So if meaningfulness is subjective and God is also, then God can provide meaningfulness to one’s life. *This seems wrong on two counts. First, why would the existence of God guarantee the meaningfulness of each of our lives? Is a life of unremitting drudgery or unrequited struggle really redeemed if there’s a larger plan, one to which we have no access, into which it fits? That would be small compensation for a life that would otherwise feel like a waste — a point not lost on thinkers like Karl Marx, who called religion the “opium of the people.” Moreover, does God actually ground the values by which we live? Do we not, as Plato recognized 2500 years ago, already have to think of those values as good in order to ascribe them to God?* This paragraph screams for some clarification as to what one means when discussing God. Is God a beneficent, if also irascible and churlish, old man, looking over us, concerned with our personal welfare, much as God is described in the Old Testament story of the Exodus? Or is it an omniscient, omnipresent, omnipotent being not amenable to anthropomorphizing? Or, is God just generally, as Plato observed, a coalescence of our ideas of what is good as opposed to that which is evil? Without understanding the nature of the God referred to here, there is no way to know whether or not God’s existence matters. *Second, and more pointedly, must the meaningfulness of our lives depend on the existence of God? Must meaning rely upon articles of faith? Basing life’s meaningfulness on the existence of a deity not only leaves all atheists out of the picture; it leaves different believers out of one another’s picture. What seems called for is an approach to thinking about meaning that can draw us together, one that exists alongside or instead of religious views.* Again, we need to understand whether meaningfulness is subjectively determined by the individual, or is a quality decreed upon a life by others. If meaningfulness is subjectively determined, then belief in God is good enough to impart subjective meaningfulness (and possibly happiness, and maybe even allow one to live a morally good life). It doesn’t mean belief in God is necessary to achieve meaningfulness, it just means that it could be a path to meaningfulness. *A promising and more inclusive approach is offered by Susan Wolf in her recent and compelling book, “Meaning in Life and Why It Matters.” A meaningful life, she claims, is distinct from a happy life or a morally good one. In her view, “meaning arises when subjective attraction meets objective attractiveness.” A meaningful life must, in some sense then, feel worthwhile. The person living the life must be engaged by it. A life of commitment to causes that are generally defined as worthy — like feeding and clothing the poor or ministering to the ill — but that do not move the person participating in them will lack meaningfulness in this sense. However, for a life to be meaningful, it must also be worthwhile. Engagement in a life of tiddlywinks does not rise to the level of a meaningful life, no matter how gripped one might be by the game.* So Ms. Wolf apparently believes meaningfulness has an objective standard to which one seeking a meaningful life would be attracted. From whence does this objective standard arise? If tiddlywinks doesn’t cut the mustard, what about other games? Is being subjectively attracted to the game of football such that one spends one’s life engaged in it objectively attractive enough to qualify as meaningful? See what a mess to which all this pontificating resolves? *Often one defends an idea by giving reasons for it. However, sometimes the best defense is not to give reasons at the outset but instead to pursue the idea in order to see where it leads. Does it capture something important if we utilize it to understand ourselves? It’s this latter tack that I would like to try here. The pursuit of this core idea — that a meaningful life is both valued and valuable — allows us to understand several important aspects of our attitudes toward ourselves and others.* Valued by whom? Valuable on the basis of what metric? *In this pursuit, the first step we might take beyond what Wolf tells us is to recognize that lives unfold over time. A life is not an unrelated series of actions or projects or states of being. A life has, we might say, a trajectory. It is lived in a temporal thickness. Even if my life’s trajectory seems disjointed or to lack continuity, it is my life that is disconnected in its unfolding, not elements of several different lives. If a life has a trajectory, then it can be conceived narratively. A human life can be seen as a story, or as a series of stories that are more or less related. This does not mean that the person whose life it is must conceive it or live it narratively. I needn’t say to myself, “Here’s the story I want construct,” or, “This is the story so far.” What it means rather is that, if one reflected on one’s life, one could reasonably see it in terms of various story lines, whether parallel or intersecting or distinct. This idea can be traced back to Aristotle’s “Ethics,” but has made a reappearance with some recent narrative conceptions of what a self is. What makes a trajectory a meaningful one? If Wolf is right, it has to feel worthwhile and, beyond that, has to be engaged in projects that are objectively worthwhile. There is not much difficulty in knowing what feels worthwhile. Most of us are good at sensing when we’re onto something and when we’re not. Objective worthiness is more elusive. We don’t want to reduce it simply to a morally good life, as though a meaningful life were simply an unalienated moral life. Meaningful lives are not so limited and, as we shall see, are sometimes more vexed. So we must ask what lends objective worthiness to a life outside the moral realm. Here is where the narrative character of a life comes into play.* Now I’m really confused. A meaningful life has a trajectory that feels worthwhile and is engaged in projects that are objectively worthwhile? Writing this blog feels worthwhile to me, but is it objectively worthwhile? By what metric might it be judged? I write because I like writing. I have found writing to be the only way for me to learn what I am really thinking; writing is subjectively valuable to me, as I place great value on understanding how I think and feel, if only because failing to do so is detrimental to my own welfare. Is it objectively valuable? My wife might say I waste far too much time at this that I could otherwise spend in fruitful endeavors, i.e., at things that make money. But that’s just her subjective opinion of my subjective view towards its value. Is there some other authority to consult that could determine whether this is objectively valuable? Society at large would probably agree with my wife, but what if they and my wife are wrong, even by their own valuation metrics? What if I one day become rich and famous as The Curmudgeon? Will it then have objective value? ***What is the point of understanding what makes lives meaningful? Why not just live them?*** Indeed. Mr. May could have started and ended his exegesis on meaningfulness there. *There are values we associate with a good narrative and its characters that are distinct from those we associate with good morals. A fictional character can be intense, adventurous, steadfast or subtle. Think here of the adventurousness of Ishmael in “Moby-Dick,” the quiet intensity of Kip in “The English Patient,” the steadfastness of Dilsey in “The Sound and the Fury” or the subtlety of Marco Polo in “Invisible Cities.” As with these fictional characters, so with our lives. When a life embodies one or more of these values (or others), and feels engaging to the one who lives it, it is to that extent meaningful. There are narrative values expressed by human lives that are not reducible to moral values. Nor are they reducible to happiness; they are not simply matters of subjective feeling. Narrative values are not felt, they are lived. And they constitute their own arena of value, one that has not been generally recognized by philosophers who reflect on life’s meaningfulness. An intense life, for instance, can be lived with abandon. One might move from engagement to engagement, or stick with a single engagement, but always (well, often) by diving into it, holding nothing back. One throws oneself into swimming or poetry or community organizing or fundraising, or perhaps all of them at one time or another. Such a life is likely a meaningful one. And this is true even where it might not be an entirely moral one.* What in the world is a “narrative value”? Is it something that makes a story, or a life, interesting to others, or to the one who lives it? If so, I think rather highly of the narrative value of my life, as I suspect most others would feel of theirs. Like a microcosm of all lives lived in all times and all places, my life has been both tragedy and comedy, depending on whether feeling or thinking reigned paramount in my mind during the particular events comprising it. *We know of people like this, people whose intensity leads them to behavior that we might call morally compromised. Intense lovers can leave bodies in their wake when the embers of love begin to cool. Intense athletes may not be the best of teammates. Our attitudes toward people like this are conflicted. There is a sense in which we might admire them and another sense in which we don’t. This is because meaningful lives don’t always coincide with good ones. Meaningful lives can be morally compromised, just as morally good lives can feel meaningless to those who live them.* So meaningfulness must be grounded in subjectivity. Just because I might not admire someone who is famous just for being famous, or perhaps who is famous for doing others harm (instead of using the amorphous “morally bad”), they still might have led meaningful lives. I’m sure Britney Spears and Bernie Madoff believe their lives to be meaningful, no matter what is the opinion of others. For Britney, perhaps the essence of meaning in her life is that others have an opinion of her, whether good or bad. *We should not take this to imply that there is no relationship between meaningfulness and morality. They meet at certain moral limits. An evil life, no matter how intense or steadfast, is not one we would want to call meaningful. But within the parameters of those moral limits, the relationship between a meaningful life and a moral one is complicated. They do not map directly onto each other.* Who decides whether one’s life is evil? Going back to Hitler, who seems to be the essence of evil, imagine all the good that came of his life. Would Western Europe have enjoyed over a half century of unparalleled prosperity and freedom and peace had Hitler not coalesced and compelled the forces of freedom to defeat him? Would the nation state of Israel (regardless of whatever one thinks about the Israeli state at present) been revivified in Palestine had not the Holocaust happened? Good and evil are extraordinarily subjective matters. Germans thought victory over France, twenty years after the insult of the Treaty of Versailles, was good; the French, presumably, not so much. Meaningfulness is apparently, like good and evil, also a subjective matter. *Why might all this matter? What is the point of understanding what makes lives meaningful? Why not just live them? On one level, the answer is obvious. If we want to live meaningful lives, we might want to know something about what makes a life so. Otherwise, we’re just taking stabs in the dark. And in any event, for most of us it’s just part of who we are. It’s one of the causes of our lying awake at night.* I have never lain awake at night wondering whether life was meaningful in any overarching way. I have lain awake at night wondering whether the things I was doing were capable of meaningfully helping me achieve what I hoped to achieve. But **the hardest question in that regard is determining what is desired**, not whether actions taken to that end are meaningful or not.

#### May’s existential angst is caused by lots of Western privilege – let the world live and struggle

**Curmudgeon 11** [September 14, 2011, The Curmudgeon's Attic, Pseudonymn of anonymous philosopher, J.D., University of Texas School of Law, “The Thing As It Is A Reply to Todd May’s “The Meaningfulness of Lives” in the New York Times”]

*There is another reason as well. This one is more bound to the time in which we live. In an earlier column for The Stone, I wrote that we are currently encouraged to think of ourselves either as consumers or as entrepreneurs. We are told to be shoppers for goods or investors for return. Neither of these types of lives, if they are the dominant character of those lives, strike me as particularly meaningful. This is because their narrative themes — buying, investing — are rarely the stuff of which a compelling life narrative is made. (I say “rarely” because there may be, for example, cases of intensely lived but morally compromised lives of investment that do not cross any moral limit to meaningfulness.) They usually lack what Wolf calls “objective attractiveness.” To be sure, we must buy things, and may even enjoy shopping. And we should not be entirely unconcerned with where we place our limited energies or monies. But are these the themes of a meaningful life? Are we likely to say of someone that he or she was a great networker or shopper, and so really knew how to live? In what I have called an age of economics, it is even more urgent to ask the question of a meaningful life: what it consists in, how we might live one. Philosophy cannot prescribe the particular character of meaning that each of us should embrace. It cannot tell each of us individually how we might trace the trajectory that is allotted to us. But it can, and ought to, reflect upon the framework within which we consider these questions, and in doing so perhaps offer a lucidity we might otherwise lack. This is as it should be. Philosophy can assist us in understanding how we might think about our lives, while remaining modest enough to leave the living of them to us.* Let me clear things up. Buying stuff does not impart meaning to one’s life, except as the stuff bought is necessary for life’s continuation in space and time. The purpose and meaning to every life, human or otherwise, is found in its struggle to survive and propagate. We only get confused about whether life is meaningful when survival and propagation is so easy that we have energy left to expend on considering whether there might be something we’re missing. When our human capacities are tasked to the limits of their design in securing the necessaries of life, there is no question that life is meaningful. The mothers of starving children in Somalia, and the children themselves, have no existential angst arising from questions about the meaningfulness of their lives. They would scoff at this silly discussion. For them, meaningfulness is found in the struggle to get food, and the other of life’s necessaries, enough to survive. It is because we in the West are so rich and comfortable and well fed that we suffer existential angst about whether our lives are meaningful. But easily achieving life’s necessaries does not mean that life’s meaningfulness can then be found elsewhere.

It just means that we haven’t a clue what to do with all the extra time and energy industrialization has provided, which is the real question that Mr. May is trying reach: Once survival is more or less as assured as can be, what then? How can we find meaning in things we know aren’t as compellingly meaningful as the struggle to survive? We were designed for struggle, and as has become obvious over the last century or so, tend to fare quite poorly without it. But if there is any question that the essential meaningfulness of life is found in the struggle for survival, skip a few meals. After a time, depending on how fat decadent Western society has made you, the only meaningful activity in which you will wish to engage is the acquisition of food. Or as I like to say, **the meaning of life is lunch. A meaningful life is one spent struggling to attain it.**