### 1NC

#### Statutory restrictions are controls or limits imposed by the legislative body

#### Blacks Online Legal Dictionary 13

(2nd Edition, http://thelawdictionary.org/statutory-restriction/)

Statutory Restriction- Limits or controls that have been place on activities by its ruling legislation.

#### Restrictions are prohibitions on action --- the aff is not

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

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

#### Restrictions on authority are distinct from conditions

William Conner 78, former federal judge for the United States District Court for the Southern District of New York United States District Court, S. D. New York, CORPORACION VENEZOLANA de FOMENTO v. VINTERO SALES, http://www.leagle.com/decision/19781560452FSupp1108\_11379

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

### Off

#### The affirmative represents a strategy of lip service restraint re-affirms executive power granting legitimacy to sovereign manipulation of law

 **Posner & Vermeule 10** Eric A. Posner [Kirkland & Ellis Distinguished Service Professor of Law] AND Adrian Vermeule [Jr. Professor of Law at Harvard Law School] “The Executive Unbound: After the Madisonian Republic”, Oxford: Oxford University Press, USA, 2010 [Questia] pp 3-5

Some commentators argue that the federal courts have taken over Congress’s role as aninstitutional check. It is true that the Supreme Court has shown little compunction about striking down statutes (although usually state statutes), and that it rejected some of the legal theories that the Bush administration used to justify its counterterrorism policies. However, the Court remains a marginal player. The Court ducked any legal rulings on counter terror policies until the 2004 Hamdi decision, and even after the Boumediene decision in 2008, no detainee has been released by final judicial order, from Guantánamo or elsewhere, except incases where the government chose not to appeal the order of a district judge. The vast majorityof detainees have received merely another round of legal process. Some speculate that judicialthreats to release detainees have caused the administration to release them preemptively. Yetthe judges would incur large political costs for actual orders to release suspected terrorists, andthe government knows this, so it is unclear that the government sees the judicial threats ascredible or takes them very seriously. The government, of course, has many administrativeand political reasons to release detainees, quite apart from anything the courts do. So the executive submits to judicial orders in part because the courts are careful not to give orders that the executive will resist.¶ In general, judicial opposition to the Bush administration’s counterterrorism policies took the form of incremental rulings handed down at a glacial pace, none of which actually stopped any of the major counterterrorism tactics of that administration, including the application of military power against Al Qaeda, the indefinite detention of members of Al Qaeda, targeted assassinations, the immigration sweeps, even coercive interrogation. The (limited)modifications of those tactics that have occurred resulted not from legal interventions but from policy adjustments driven by changed circumstances and public opinion, and by electoral victory of the Obama administration. However, the Obama administration has mostly confirmed and in some areas even expanded the counterterrorism policies of the Bush administration. Strong executive government is bipartisan. The 9/11 attack provided a reminder of just how extensive the president’s power is. The executive claimed the constitutional authority to, in effect, use emergency powers. Because Congress provided redundant statutory authority, and the Supreme Court has steadfastly refused to address the ultimate merits of the executive’s constitutional claims, these claims were never tested in a legal or public forum. But it is worth trying to imagine what would have happened if Congress had refused to pass the Authorization for Use of Military Force and the Supreme Court had ordered the¶ executive to release detainees in a contested case. We think that the executive, backed up as it was by popular opinion, would have refused to obey. And, indeed, for just that reason, Congress would never have refused its imprimatur and the Supreme Court would never have stood in the executive’s way. The major check on the executive’s power to declare an emergency and to use emergency powers is—political. The financial crisis of 2008–2009 also revealed the extent of executive power. Acting together, the Fed, the Treasury, and other executive agencies spent hundreds of billions of dollars, virtually nationalizing parts of the financial system. Congress put up a fuss, but it could not make policy and indeed hardly even influenced policy. Congress initially refused to supply a blank check, then in world-record time changed its mind and gave the blank check, then watched helplessly as the administration adopted policies different from those for which it said the legislation would be needed. Courts played no role in the crisis except to ratify executive actions in tension with the law.2'

#### This presentation of legitimacy continues crumbling the distinction between democracy and totalitarianism and reinforces death-centered thanatopolitics causeing genocide on the global scale.

**Hall 7** Lindsay Anne Hall [MA Political Science] “Death, Power, and the Body: A Bio-political Analysis of Death and Dying” May 7, 2007 (Research paper presented to faculty of the Virginia Polytechnic Institute and State University)¶ http://scholar.lib.vt.edu/theses/available/etd-05152007-134833/unrestricted/etd.pdf

Agamben, on the other hand, addresses the intertwinement of medicine, death, ¶ and power through his analysis of the modern individualís exposure to death. According ¶ to Agamben, Western culture has become “thanatopolitical,” which means that it is ¶ dominated by a politics of death that leaves us more and more exposed to both death and ¶ operations of power. For Agamben, death has become indistinct. It is both meaningful ¶ and meaningless, both individual and anonymous, both visible and invisible. Moreover, ¶ because modern society increasingly exposes individuals to death, liberal democracy ¶ becomes increasingly indistinguishable from totalitarian regimes, an issue I will explore ¶ in more detail in Chapter Three. While the issues that I am addressingólife sustaining ¶ technologiesóare merely one symptom of the greater problem that Agamben is himself ¶ concerned with, I hope that shedding more light on this particular space of power can ¶ allow us to think about and eventually challenge the greater politics of death operating in ¶ modern society.¶ In this study I will focus specifically on reconsidering the relations of power ¶ surrounding the decision to stop preserving life in the particular space of the hospital ¶ room. According to Foucaultís view, terminating life is nearly unthinkable in a biopolitical society. Thus, as Benjamin Noys elaborates, we ìtry so hard to preserve life, ¶ even at the cost of terrible suffering, because death is the limit to [bio-political] powerî ¶ (2005, 54). For Foucault, death has become ìshameful,î it is paramount to giving up, to ¶ letting go, or to admitting defeat (all things given a negative connotation in Western ¶ society) (2003c, 247). In this study I would like to reconsider these claims through ¶ Giorgio Agambenís argument that death has become more political as the boundary ¶ between life and death has become blurred. Such a state of being, he claims, exposes the ¶ body to death, and yetóas I am primarily concerned withóìsaturatesî the body with ¶ power (Agamben 1995, 164). ¶ As suggested by this synopsis, I am using Foucault as the starting point for my ¶ study. Though I ultimately bring in Agamben who question aspects of his analysis of ¶ power, I begin my first chapter with an in depth account of the ways in which Foucault ¶ believed power to be exercised upon the body. In this chapter I begin to hammer out the ¶ theoretical framework that I will then both use and challenge in order to analyze the ¶ space of the hospital room as a space of power. In The Birth of the ClinicóFoucaultís ¶ only sustained analysis of the medical disciplineóhe claimed that the body was suddenly ¶ made ìexhaustively legibleî with the birth of modern medicine. More precisely, he ¶ claims that it was ìfrom the integration of death into medicineÖthat Western man could ¶ [at last] constitute himself in his own eyes as an object of science,î grasping himself ¶ within his own language, and giving himself his own discursive existence (Foucault ¶ 1973, 197). In his later writings on power, however, Foucault gives this constitutive ¶ capacity of individuals to sexuality, not death, and as I have previously suggested, ¶ Foucault begins to look at death as a limit to power itself. Throughout this study I have ¶ attempted to reconcile this seeming contradiction in Foucaultís work through the work of ¶ Giorgio Agamben. ¶ My second chapter is an examination of what Agamben terms the ìzone of ¶ indistinctionî between life and death. For Agamben, the line between life and death has ¶ become increasingly blurred by a whole series of ìwaveringsî around both the time of¶ death and the question of who decides on this time. As Agamben claims, this decision is ¶ increasingly taken up by the medical profession, thus in the conclusion of this chapter I ¶ return to Foucaultís only sustained engagement with medical power, The Birth of the ¶ Clinic. In this section I argue that Agambenís analysis of the intertwinement between the ¶ medical discipline and power might benefit from some of the historical insights provided ¶ in Foucaultís analysis. While Agamben centers his analysis on post-World War II ¶ society, Foucaultís work demonstrates that the entanglement of medicine and sovereign ¶ power have a far longer history than perhaps Agamben realizes or is willing to engage ¶ with. ¶ In the third and final chapter of this study I examine how death is politicized. As ¶ Agamben argues, death is not a natural or biological moment but a political decision. In ¶ order to tackle the nature of this decision I look at the work of Peter Singer who ¶ compares two seemingly contradictory ethics, the ethics of the sanctity of life and the ¶ quality of life ethic. An Agambenean analysis of these ethics however, suggest some ¶ problems that Singer may have not been able to articulate because he fails to take into ¶ account the political nature of death. One of the criticisms that has been lodged against ¶ Singer is that his ethics closely parallels Nazi eugenics programs in which the medical ¶ establishment made decisions on whose life was worth living. This criticism bridges the ¶ gap between Singerís work and the point I have been making through this piece- biopower is intimately enmeshed with sovereignty. ¶ Foucault saw this combination at work primarily in totalitarian regimes. ¶ However, as Agamben argues, the distinctions between totalitarian regimes and ¶ democracies are crumbling. I argue in my Conclusion that modern power is increasingly ¶ an amalgamation between the bio-political and the thanatopolitical. For power can both ¶ manage life and expose us to death. What is crucial to take from this analysis is that we ¶ must formulate some sort of individual resistance to this power, even though techniques ¶ of modern bio-power (bureaucratic planning, statistical analysis, population control) may ¶ xpose us to death as a population rather than as individuals. This resistance must be ¶ something greater than simply a call for physician assisted suicide or an appeal for ¶ individual ownership of our bodies, it must first center on an engagement with what ¶ about life is really worth preserving.

#### Our alternative is to shake out the rug from under the 1ac's mode of legal analysis - this is preferable to actualizing new and less oppressive societal formulations.

Singer 84 - Associate Professor of Law (Joseph William Singer, Associate Professor of Law at Boston University, 1984, [“The Player and the Cards: Nihilism and Legal Theory,” Yale Law Journal (94 Yale L.J. 1)

What shall we do then about legal theory? I think we should abandon the idea that what we are supposed to be doing is applying or articulating a rational method that will tell us once and for all (or even for our generation) what we are supposed to believe and how we are supposed to live. We should no longer view the project of giving a "rational foundation" for law as a worthwhile endeavor. If morality and law are matters of conviction rather than logic, we have no reason to be ashamed that our deeply felt beliefs have no "basis" that can be demonstrated through a rational decision procedure or that we cannot prove them to be "true" or "right." Rorty has distinguished between two broad types of theory: systematic and edifying. n165 Systematic philosophers build systems of thought that they claim explain large bodies of material, guide theoretical development, and generate answers to difficult questions. Systematizers can be either normal or revolutionary philosophers. The normal systematizers work within established tradition; the revolutionary systematizers seek to replace the established paradigm with a new, better, or truer paradigm of thought. Both try to establish a framework that will set bounds on the legitimate content of discourse. Edifying philosophers, on the other hand, seek to shake the rug out from under existing normal or abnormal systems of thought. They seek to make us doubt the necessity and coherence of our views. They seek to free us from feeling that we have "gotten" the answer and that we no longer need to question ourselves about what we stand for. Edifying philosophers do not seek to induce people to give up their moral views. They do not [\*58] argue against profound political commitment. Rather, they strive to make us realize that our views are matters of commitment rather than knowledge. n166 Legal scholars can perform an edifying role by broadening the perceived scope of legitimate institutional alternatives. n167 One way to do this is to demonstrate the contingent and malleable nature of legal reasoning and legal institutions. The greatest service that legal theorists can provide is active criticism of the legal system. Criticism is initially reactive and destructive, rather than constructive. But our mistaken belief that our current ways of doing things are somehow natural or necessary hinders us from envisioning radical alternatives to what exists. To exercise our utopian imagination, it is helpful first to expose the structures of thought that limit our perception of what is possible. Judges rationalize their decisions as the results of reasoned elaboration of principles inherent in the legal system. Instead of choosing among available descriptions, theories, vocabularies, and course of action, the official who feels "bound" reasons from nonexistent "grounds" and hides from herself the fact that she is exercising power. n168 By systematically and constantly criticizing the rationalizations [\*59] of traditional legal reasoning, we can demonstrate, again and again, that a wider range of alternatives is available to us. I therefore advocate the persistent demonstration in all doctrinal fields that both the legal rules in force and the arguments that are presented to justify and criticize them are incoherent. n169 They are incoherent because they are constructed in ways that make it impossible for them to satisfy their own claims to determinacy, objectivity and neutrality. n170 Legal theory is at war with itself. This kind of criticism would be useful even if we could not imagine a satisfactory alternative to traditional legal theory. Such criticism reminds us that legal theory cannot answer the question of how we are going to live together. We are going to have to answer that question ourselves.

### off

#### Call our next argument LIVING IN FEAR

#### Did you know somebody could have poisoned your corn-flakes this morning? The affirmative represents the ultimate culmination in paranoia induced politics - it is literally not worth the effort to vote for the aff.

Gartzke 12 - Associate Professor of Political Science at University of California San Diego (Erik, http://dss.ucsd.edu/~egartzke/papers/cyberwar\_12062012.pdf, December 7th 2012, The Myth of Cyberwar Bringing War on the Internet Back Down to Earth)

The notion that cyberspace is a new domain where old rules don't apply and where omnipresent vulnerabilities require extensive (and expensive) military reform is both intuitive and widely expressed. Cyberspace could constitute a hidden back door, enabling opponents to undermine U.S. national security and circumvent the terrestrial advantages of the existing western-dominated order. History makes clear that technological innovations or new modes of organization eventually topple every hierarchy.4 However, it is far from clear that we are in the midst of such a transition today. Lacking information about whether developments are transformational or merely incremental, it may make sense to begin with a few guidelines about when panic is in order, and when it is not. A reasonable level of caution is probably provided by common sense. Most readers will lock their doors at night, for example, and refrain from handling large sums of cash in dark alleyways. Imagining what others could do to harm each of us, however, can quickly slide into paranoia. It is not reasonable caution to believe that someone is intent on mischief simply because harm is possible. Even in the safest of societies, individuals, groups and entire communities are subject to an enormous variety of potential hazards. Much could be done to damage each of us, even though few of these possibilities are actually exercised, or experienced, with any regularity. The physical world hosts a multitude of venues for extremely unlikely accident or disease. A small number of people prefer to stay in their homes rather than risk being struck by lightening or struck down by botchulism. Still, individuals with these concerns often receive more attention from psychiatric professionals than from military planners. Being vulnerable should be novel to no one living in the modern world. Indeed, the capacity to harm in a highly integrated world is so ubiquitous that blood would coat the streets if it were not for the fact that relatively little relationship exists between the capacity to attack and the actual prospect that one is invaded, assaulted or otherwise done in.5 Just about anything is possible. Someone may have poisoned your morning Corn Flakes. Terrorists may have singled you out for vengeance, or you might just become one of the unlucky few who are in the wrong place at the wrong time. When a commuter steps outside to start her car or to catch the bus, it is impossible to be certain that no truck will jump the curb and that every asteroid will remain in the heavens. And yet, despite endless possibilities for damage or death, the vast majority of us have yet to harden our living rooms against cruise missiles or falling satellites. In dealing with known unknowns, we became comfortable with the fact that we are unprotected. Few homeowners in California carry earthquake insurance, for example, though it is by no means impossible that \the big one" will strike tomorrow. We do so because security itself has a price; protection from unlikely events is literally not worth the effort. One could buy that bulletproof vest relentlessly listed on Ebay, but then how often would it really be proper attire at the office or in the classroom? Unlike possibilities, the probabilities of esoteric catastrophe are by their nature minute. Unlikely events are unlikely, and so most of us go about our business, without paying undue attention to the potential menace from the skies or, for that matter, from our fellow citizens. Governments face similar realities. Many threats are conceivable, but few are likely to occur. All forms of security involve assessing risks and allocating limited resources to address tractable threats, making the largest ( nite) improvements in protection or, conversely, the greatest increases in in uence.6 Every dollar spent on national defense must be taken from objectives like education, infrastructure, or paying down the debt. Only extremely auent (or paranoid) populations pay the price of pursuing protection from the most exotic hazards. More to the point, protection is inevitably incomplete, and comes with its own consequences, including other forms of insecurity. The risk of attack is never zero, since a potent defense or deterrent endangers the security of others.7 If violence is a perennial possibility, why don't human beings live in consummate fear? Most of us are safe because the multitudes who are capable of causing us harm have little interest in doing so. For the most part, violence does little that potential perpetrators view as worth their while. Much of humanity is protected by an invisible shell of indi erence or ine caciousness. The stranger coming toward you on a busy city street could easily swing out his arm at the last minute, catching you under the chin. He could be carrying an Uzi, which in a fit of rage will leave you and other passersby on the pavement in a pool of intermingling body fluids. We see little such violence because it does little to benefit the violator, just as bludgeoning the odd shopper in the mall fails to profit the bludgeoner. Violence is costly, risky, and mostly unproductive. When we learn of violence, our natural inclination is to ask \why?" Like a police detective, we seek a motive. When on occasion violence occurs with no apparent logic as to target, it is remarkable, and puzzling. Most of us are capable of seriously damaging others, but for the most part we fail to exercise our capabilities because there is no positive reason to strike. The mere capacity to inflict harm is thus not a very good predictor of aggressive behavior. Because few of us are likely to be the target of an attack, each of us can greet each day with minimal anxiety, to say nothing of personal security, not because we are effectively protected from harm, but because harm is inconvenient, unnecessary or pointless for potential perpetrators. Attacking us (or others) serves no purpose. The internet makes it possible to interact with people just about anywhere on the globe as easily, or even more easily, than conversing with the neighbors next door. Initial attention to the mobility of cyberspace focused on the potential for good, but convenience also overcomes natural barriers to conflict. The supply of targets for cyber acts of aggression is certainly huge relative to the supply of perpetrators of physical violence. Viewed in this way, it is remarkable that cyber space is not predominantly the domain of fraud, identity theft, and other acts of predation, interspersed only by porn and the occasional Nigerian emailer looking to deposit millions in your bank account. Yet, if the internet makes it easy to reach out and touch others, it in no way makes those contacts profound. Casual attempts to undermine your welfare abound, but it is with equal casualness that we ignore the bulk of spam, or internet sites marketing lapsed software. Predation continues unabated on the world wide web, but if it is easy to reach us, contact is all the more superficial. The ease of contact is generally inversely related to the prevalence of transgression. Just as a pedestrian can be fairly comfortable walking in front of a stopped vehicle at an intersection, most internet traffic is benign, simply because perpetrators are rare and opportunities are many. Cyber space has not made life more dangerous for the multitudes. There are crimes on the internet, but it is far from clear that the internet has increased overall criminal behavior. Internet crime often substitutes for crimes that would otherwise have been committed in real space. Perhaps even more to the point, much of internet fraud and cyber violence is intrinsically tied to the physical domain; much of the harm initiated on the internet eventually gets perpetrated in more conventional ways. The safety that mass populations achieve from their numbers and anonymity in terms of targeting is denied political institutions and their representatives. Countries and organizations have facilities and personnel that can be targeted with violence. How might the ability to strike institutions and infrastructure change the risk of cyber attack? Once again, we must inquire not about what could happen but why individuals, groups or nations might be motivated to take action. Nations and organizations can be attacked through the internet, just as they have long been attacked in physical space. The ease with which such attacks can be perpetrated are an obvious, and much discussed, phenomenon. Physical space has always been an important barrier to conflict.8 Even today, the single best predictor of interstate conflict is the contiguity of national borders (Hensel 2000, Senese 2005). However, lowering the cost of transmission of an attack is only synonymous with increasing the appeal of a given approach to war if the approach is also effective in achieving certain ends. Beyond being anonymous and a multitude, the main thing that protects individuals from all types of violence is even more potent for political institutions; it is not clear in many cases how force will yield a change in the tide of the a airs of states or organizations. Cyber attacks can be appealing as political acts only to the degree that they affect the decisions organizations and sovereigns make with and without cyber violence. Since understanding when and how cyberwar influences politics is largely identical to understanding how conventional forms of military violence act upon politics, I turn next to an analysis of the nature of terrestrial warfare.

#### No, cyber weapons are just an added augment to existing capabilities, they do not change geostrategic calculus - they conflate intent with capabilities.

Gartzke 12 - Associate Professor of Political Science at University of California San Diego (Erik, http://dss.ucsd.edu/~egartzke/papers/cyberwar\_12062012.pdf, December 7th 2012, The Myth of Cyberwar Bringing War on the Internet Back Down to Earth)

A blitz of media, punditry and public pronouncements inform interested observers and policy makers that the next war is likely to be won or lost on the internet. Indeed, events such as the coordinated cyber attacks on Estonia and the Stuxnet worm seem to indicate that cyberwar has already begun. The sense of urgency surrounding cyberwar appears to be tied to perceptions that internet conflict is the newest phase in the ongoing revolution in military affairs, only this time the threat is directed at the sophisticated technological civilizations of the West, rather than at poor developing states or the recipients of inferior second-world military hardware.1 To believe a growing number of pundits and practitioners, cyberwar threatens to render existing military advantages impotent, exposing those nations most dependent on comprehensive information infrastructures to devastating and unpredictable attacks. If powerful states largely immune to terrestrial invasion can have their military might blunted and their factories and cities idled by foreign hackers, then perhaps this latest technological revolution really does presage a \Pearl Harbor" in which the United States and other great powers will be targets, rather than perpetrators, of shock and awe. There is a problem with the growing consensus of impending cyber apocalypse, however: it is far from clear that conflict over the internet can actually function as war. Discussions of cyberwar commit a common fallacy of arguing from opportunity to outcome, rather than considering whether something that could happen is at all likely, given the motives of those who are able to act. Cyber pessimism rests heavily on capabilities (means), with little thought to a companion logic of consequences (ends). Much that could happen in the world fails to occur, largely because those capable of initiating action discern no benefit from doing so. Put another way, advocates have yet to work out how cyberwar actually accomplishes the objectives that typically sponsor terrestrial military violence. Absent a logic of consequences, it is difficult to believe that cyberwar will prove as devastating for world a airs and for developed nations in particular as many seem to believe. This essay assesses the salience of the internet for carrying out functions commonly identified with terrestrial political violence. War is fundamentally a political process, as Clausewitz (1976[1832]) famously explained. States, groups and individuals threaten harm to deter or compel, generating influence through the prospect of damage or loss. Military violence can also be exercised to alter or maintain the balance of power and to resist or impose disputed outcomes. The internet is generally an inferior substitute to terrestrial force in performing the functions of coercion or conquest. Cyber \war" is not likely to serve as the final arbiter of competition in an anarchical world and so should not be considered in isolation from more traditional forms of political violence.2 In fact, the capacity for internet coercion is limited by the same factors that make cyberwar appear at first to be so intimidating. For threats or demands to prove effective, targets must believe both that an attack is likely to follow from noncompliance, and that the attack is destined to inflict unacceptable harm. Yet, as I detail here, the need to apprise targets of internet vulnerabilities in order to make cyber threats credible contrasts with the secrecy needed to ensure an efective attack. Since it is difficult to share operational details of planned attacks without compromising military efectiveness, cyberwar must be practiced more often than threatened. Here too, however, there are critical limitations to what can be achieved via the internet. It is one thing for an opponent to idle a country's infrastructure, communications or military capabilities. It is quite another to ensure that the damage inflicted translates into a lasting shift in the balance of national capabilities or resolve. Cyber attacks are unlikely to prove particularly potent in grand strategic terms unless they are accompanied by terrestrial military force or other actions designed to capitalize on temporary weakness effected over the internet. Perpetrators must therefore be prepared to exploit windows of opportunity generated by internet attacks through other modes of combat. Otherwise, there are few compelling reasons to initiate cyberwar in the rst place. The chief benefciaries of cyberwar are thus less likely to be weak or rising powers than those states that already possess important terrestrial military advantages. Conceived of in this way, the internet is less a revolution in military affairs than it is yet another set of technologies that extend existing disparities in power and influence.

#### The impact is pure war which results in psychological violence and the potential for lashout. Our alternative is not an advocacy but an argument about investing meaning in the ballot, you should vote for the status quo and refuse the affirmative's fear mongering.

Borg 2003 (Mark; PhD in psychoanalysis, practicing psychoanalyst and community/organizational consultant working in New York City. He is a graduate of the William Alanson White Institute's psychoanalytic certification program and continues his candidacy in their organizational dynamics program. He is co-founder and executive director of the Community Consulting Group, "Psychoanalytic Pure War: Interactions with the Post-Apocalyptic Unconscious": JPCS: Journal for the Psychoanalysis of Culture & Society, Volume 8, Number 1, Spring 2003, MUSE)

Paul Virilio and Sylvere Lotringer’s concept of “pure war” refers to the potential of a culture to destroy itself completely (12).2We as psychoanalysts can—and increasingly must—explore the impact of this concept on our practice, and on the growing number of patients who live with the inability to repress or dissociate their experience and awareness of the pure war condition. The realization of a patient’s worst fears in actual catastrophic events has always been a profound enough psychotherapeutic challenge. These days, however, catastrophic events not only threaten friends, family, and neighbors; they also become the stuff of endless repetitions and dramatizations on radio, television, and Internet.3 Such continual reminders of death and destruction affect us all. What is the role of the analyst treating patients who live with an ever-threatening sense of the pure war lying just below the surface of our cultural veneer? At the end of the First World War, the first “total war,” Walter Benjamin observed that “nothing [after the war] remained unchanged but the clouds, and beneath these clouds, in a field of force of destructive torrents and explosions, was the tiny, fragile human body”(84). Julia Kristeva makes a similar note about our contemporary situation, “The recourse to atomic weapons seems to prove that horror...can rage absolutely” (232). And, as if he too were acknowledging this same fragility and uncontainability, the French politician Georges Clemenceau commented in the context of World War I that “war is too serious to be confined to the military” (qtd. in Virilio and Lotringer 15). Virilio and Lotringer gave the name “pure war” to the psychological condition that results when people know that they live in a world where the possibility for absolute destruction (e.g., nuclear holocaust) exists. As Virilio and Lotringer see it, it is not the technological capacity for destruction (that is, for example, the existence of nuclear armaments) that imposes the dread characteristic of a pure war psychology but the belief systems that this capacity sets up. Psychological survival requires that a way be found (at least unconsciously) to escape inevitable destruction—it requires a way out—but this enforces an irresolvable paradox, because the definition of pure war culture is that there is no escape. Once people believe in the external possibility— at least those people whose defenses cannot handle the weight of the dread that pure war imposes— pure war becomes an internal condition, a perpetual state of preparation for absolute destruction and for personal, social, and cultural death.

### case - OCO

#### Even silky paws need claws. Offensive cyber operations are critical to U.S. deterrence and are not perceived as an act of aggression.

Limnell & Hanska 13 - \*Director of Cyber Security at Stonesoft Corporation, Doctor of Military Science , \*\*Received his doctoral degree from the University of Tampere. He works as an officer in the Finnish Defense Forces and is currently affiliated with the National Defense University. (Dr. Jarno, Dr. Jan, http://www.infosecisland.com/blogview/23036-Silky-Paws-Need-Claws--The-Problems-of-Defensive-Cyberstrategies.html, March 25th 2013)

How many of us have not fondled and marveled at the silky softness of the paws of a cat – only to have fallen seconds later a victim of numerous bloody scratches. Wearing velvet gloves in the issues concerning cyber strategies is not a way to proceed if national security is at a stake. We might benefit more from following U.S. President Teddy Roosevelt’s motto: “speak softly and carry a big stick.” This can be reinterpreted in today’s context as advise not to speak in threatening and jingoistic tones but preparing simultaneously for use of force. For societies and armed forces there is today no credible defense without cyber capabilities. The cyber arms race has started, and its speed is accelerating. Nations and other entities are using online weapons, because they are thousands of times cheaper than conventional armaments. But they are not bloodless, as we would like to think. Cyber weapons can damage a physical object as badly as a traditional weapon. No responsible nation-state should aspire for the role of “North Korea of the cyber space”, issuing hollow threats in aggressive public messages but neither should we discard the notion that Realpolitik seems to be in our contemporary conjunction the way cyber policies work. The U.S. has thus far been the most vociferous proponent of the use of force in relation to cyber threats. These range from the assertion that a cyber attack, when it passes a certain undeclared threshold, will result in retaliation by kinetic weapons to the leaks suggesting that a presidential policy directive has provided the U.S. president with the ability to order a preemptive cyber strike. This is not the way to advance the peaceful development of cyber policies. The U.S. has chosen not only to shout its threats aloud, but also to wave the stick around. In the case of a superpower the claws can remain hidden – the paws themselves are sizable enough to deter aggression since it is obvious that even a careless pelt would cause damage. As is the case with any weapon, when talking about cyber threats, the motive is crucial. Russia today has approximately 5,000 nuclear weapons that could destroy the world several times over. However, Russia lacks the intention to use its nuclear weapons. The same goes for cyber weapons. China already has very destructive cyber weapons to use against the United States’ critical infrastructure. But China does not currently have the motivation to use its cyber weapons against the U.S. It is important to separate the intention and the capability, which together make the threat. In the case of small powers the problem is different and needs to be addressed differently. We are not aggressive in our policies – in the world of “Realcyber” we indeed cannot afford such an approach. We do not stomp around, but tread very softly in the international realm. There is, however, a difference between the soft, feline steps we do wisely to take and “frakfooting” around. If we write our cyberstrategies to be entirely defensive, without even including an offensive element, there is no way to deter aggression. A prospective cyber attacker does not shy away from probing for weaknesses and infiltrating systems and network if the severest result is that the attack will at some point peter out when defensive cyber capabilities are employed. The attack either failed, or was a partial or complete success. It would have been folly not to try, since even in the case of failure there would have been no risk of retaliation and damage from a counter-attack. When the defensive cyber strategy is coupled with offensive capabilities to be automatically employed in a counter-attack the prospective aggressor may be not be all that eager to initiate action – for fear of counter-action. It is an old maxim of Vegetius that if you want peace, prepare for war. Sic vis pacem, para bellum. In cyber strategy this is not war-mongery but a rational approach to security. And cyberwar is comparable to traditional war in many senses as a recent NATO commissioned report Tallinn Manual on the International Law Applicable to Cyber Warfare shows us. The findings of international law experts tell that while in most cases the appropriate response to a cyberattack would be in a retaliation confined to cyberspace, in those cases where the victim has suffered death of severe property damage, it is acceptable and lawful to retaliate with traditional kinetic weapons in its counter-strike. The report also finds that even individual hackers who undertake attacks are legitimate targets for counter-strikes. This basically implies that building and upholding capabilities for offensive cyberwar instead of restricting oneself to merely inventing systems of passive defense would thus not, even from the perspective of international, be considered as acts of aggression. The failure to create a system for offensives, to be used to protect oneself when attacked, might even lead to a situation where one becomes a more probable target of aggression. One of the “natural laws” of traditional Realpolitik was that weakness invites hostility and since cyberspace thus far has not politically developed into the same level of sophistication, agreements and pacts as the international relations of the physical world, it might be wise to adhere to the more pragmatic policy approaches of the past until cyberspace becomes more thoroughly regulated by international agreements. We initiated this article with an allegory by comparing cyber strategy to the behavior of a cat. Indeed, no small nation-state can uphold a distinguished status within the international community by adopting a mad-dog policy of random aggression against any real or perceived threat. Instead, quite a few of the attributes and characteristics of a cat have to be taken into account to master cyber security and create a strategy to answer all the requirements of the fluid developments of today. A plausible approach to cyber security must contain the feline elements of stealth, flexibility, adaptability and dexterity – and not discard the necessity of concealing sharp extendable claws to be used for one’s protection. To settle for mechanisms of passive defense equals not only having a tomcat castrated but declawed at the same time.

#### No cyber prolif

Libicki 12 - Senior Management Scientist at the RAND Corporation (Martin, "Crisis and Escalation in Cyberspace", http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND\_MG1215.pdf)

Nevertheless, the logic that states have to develop offensive cyber-weapons because their rivals do has little basis in theory or fact. First, states have little knowledge of exactly what weapons, as such, are in the arsenal of their rivals. 13 Indeed, if they actually knew precisely what weapons their foes had, they might well know what vulnerabilities such weapons targeted and would fix such vulnerabilities, thereby nullify-ing these weapons. Second, as noted, the best response to an offensive weapon is a defensive weapon, not another offensive weapon. Third, the whole notion of offense-versus-offense requires that the underlying dynamic of attack and retaliation actually makes sense as a warfight-ing and war-termination strategy. Were that so, deterrence would be primary. But deterrence is a very difficult notion in cyberspace. 14 States wanting to hide their own tracks in a cyberattack have a wealth of ways to do so and, often, more than enough motive. Incidentally, it is hard to imagine how an arms race in cyberspace could come close to having a major economic impact. The intellectual skills required to compete in this contest are so specialized that states will run out of such people well before they run out of money paying them.

#### Squo solves cyber aggression.

Nakashima 12 - Washington Post staff writer (Ellen, November 14, "Obama signs secret directive to help thwart cyberattacks", http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3\_story.html)

President Obama has signed a secret directive that effectively enables the military to act more aggressively to thwart cyber­attacks on the nation’s web of government and private computer networks. Presidential Policy Directive 20 establishes a broad and strict set of standards to guide the operations of federal agencies in confronting threats in cyberspace, according to several U.S. officials who have seen the classified document and are not authorized to speak on the record. The president signed it in mid-October. The new directive is the most extensive White House effort to date to wrestle with what constitutes an “offensive” and a “defensive” action in the rapidly evolving world of cyberwar and cyberterrorism, where an attack can be launched in milliseconds by unknown assailants utilizing a circuitous route. For the first time, the directive explicitly makes a distinction between network defense and cyber-operations to guide officials charged with making often-rapid decisions when confronted with threats. The policy also lays out a process to vet any operations outside government and defense networks and ensure that U.S. citizens’ and foreign allies’ data and privacy are protected and international laws of war are followed. “What it does, really for the first time, is it explicitly talks about how we will use cyber- operations,” a senior administration official said. “Network defense is what you’re doing inside your own networks. . . . Cyber-operations is stuff outside that space, and recognizing that you could be doing that for what might be called defensive purposes.” The policy, which updates a 2004 presidential directive, is part of a wider push by the Obama administration to confront the growing cyberthreat, which officials warn may overtake terrorism as the most significant danger to the country. “It should enable people to arrive at more effective decisions,” said a second senior administration official. “In that sense, it’s an enormous step forward.” Legislation to protect private networks from attack by setting security standards and promoting voluntary information sharing is pending on the Hill, and the White House is also is drafting an executive order along those lines. James A. Lewis, a cybersecurity expert at the Center for Strategic and International Studies, welcomed the new directive as bolstering the government’s capability to defend against “destructive scenarios,” such as those that Defense Secretary Leon E. Panetta recently outlined in a speech on cybersecurity. “It’s clear we’re not going to be a bystander anymore to cyberattacks,” Lewis said. The Pentagon is expected to finalize new rules of engagement that would guide commanders on when and how the military can go outside government networks to prevent a cyberattack that could cause significant destruction or casualties. The presidential directive attempts to settle years of debate among government agencies about who is authorized to take what sorts of actions in cyberspace and with what level of permission. An example of a defensive cyber-operation that once would have been considered an offensive act, for instance, might include stopping a computer attack by severing the link between an overseas server and a targeted domestic computer. “That was seen as something that was aggressive,” said one defense official, “particularly by some at the State Department” who often are wary of actions that might infringe on other countries’ sovereignty and undermine U.S. advocacy of Internet freedom. Intelligence agencies are wary of operations that may inhibit intelligence collection. The Pentagon, meanwhile, has defined cyberspace as another military domain — joining air, land, sea and space — and wants flexibility to operate in that realm. But cyber-operations, the officials stressed, are not an isolated tool. Rather, they are an integral part of the coordinated national security effort that includes diplomatic, economic and traditional military measures. Offensive cyber actions, outside of war zones, would still require a higher level of scrutiny from relevant agencies and generally White House permission.

### Case - Alliances

#### **US can’t solve modeling – the development of offensive capabilities is inevitable.**

Libicki 9 - Senior Management Scientist at the RAND Corporation (Martin, Senior Management Scientist at the RAND Corporation, "Cyberdeterrence and Cyberwar", http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND\_MG877.pdf)

Historically, arms control has always gone hand in hand with deter- rence and crisis stability, but it would be difficult to be optimistic about its prospects in cyberspace. A good deal depends on what one means by arms control. If the model were to be something like the treaties signed between the United States–NATO and the Soviet Union– Warsaw Pact, which limited certain classes of weapons and banned others, there is little basis for hope. 1 If, instead, the goal were a framework of international agreements and norms that could raise the diffi- culty of certain types of cyberattacks, some progress can be made. Why is it nearly impossible to limit or ban cyberweapons? First, although the purpose of “limiting” arms is to put an inventory-based lid on how much damage they can do in a crisis, such a consideration is irrelevant in a medium in which duplication is instantaneous. 2 Second, banning attack methods is akin to banishing “how-to” information, which is inherently impossible (like making advanced mathematics illegal). The same holds for banning knowledge about vulnerabilities. Third, banning attack code is next to impossible. Such code has many legitimate purposes, not least of which is in building defenses against attack from others. These others include individuals and nonstate actors, so the argument that one does not need defenses because offenses have been outlawed is unconvincing. In many, per- haps most cases, such attack code is useful for espionage, an activity that has yet to be banned by treaty. Furthermore, finding such code is a hopeless quest. The world’s information storage capacity is immense; much of it is legitimately encrypted; and besides, bad code does not emit telltale odors. If an enforcement entity could search out, read, and decrypt the entire database of the world, it would doubtless find far more interesting material than malware. Exhuming digital informa- tion from everyone else’s systems is hard enough when the authorities with arrest powers try it; it may be virtually impossible when outsiders try. The only barely feasible approach is to ban the activity of writing attack code, then hope that the fear of being betrayed by an insider who goes running to international authorities prevents governments from organizing small groups of elite hackers from engaging in such nefarious activities. If the international community had the manpower and access to enforce such norms, it could probably enforce a great many other, and more immediately practical, norms (e.g., against cor- ruption). Such a world does not exist.

#### US legitimacy turns allies against it – kills effective coalitions

Ikenberry et al 9 **-** G. John Ikenberry is a professor of politics and international affairs at Princeton University, Michael Mastanduno is a professor of government and associate dean for social sciences at Dartmouth College, William C. Wohlforth is a professor of government at Dartmouth College, “Unipolarity, State Behavior, and Systemic Consequences”, World Politics, 61.1, Jan, MUSE

Unipolarity and Revisionism: Is the Unipole a Satisfied State? The stability of any international system depends significantly on the degree to which the major powers are satisfied with the status quo.17 In War and Change in World Politics, Robert Gilpin argued that leading states “will attempt to change the international system if the expected benefits exceed the expected costs.”18 In the quarter century since that book’s publication, international relations scholars have never seriously debated whether the “expected net gain” of systemic revisionism might be positive for the United States. It is hardly surprising that scholars set aside the question of revising the territorial status quo—it is hard to imagine plausible arguments for the utility of large-scale conquest in an age of nuclear weapons and economic globalization. But the territorial status quo is only a part of what Gilpin meant by “international system.” The other part comprises the rules, institutions, and standards of legitimacy that frame daily interactions. Why has there been no scholarly debate on whether the United States might seek to revise that aspect of the system? In the 1980s, to be sure, the question did not seem relevant. Scholars believed that the United States was in relative decline, so the costs of changing the system were simply assumed to be high, and a U.S. preference for the status quo appeared obvious. The transition from bipolarity to unipolarity arguably represented a dramatic power shift in favor of the United States, altering Gilpin’s equation toward revisionism. Yet the question of whether, as a new unipole, the United States might adopt a more revisionist stance has not figured centrally in international relations research. The reason was a key assumption built into almost all research on hegemonic stability and power transition theory: that the leading state in any international system is bound to be satisfied. Hence, research on the origins of satisfaction and revisionism is soverwhelmingly about subordinate states, not the dominant state.19 [End Page 12] Robert Jervis’s article in this issue demonstrates that this assumption is no longer tenable. While the case can be made that a unipole—particularly one that achieved this status in an international system already strongly shaped by its power and preferences—might rationally opt for conservatism,20 international relations scholarship is rich with hypotheses proposing that the opposite is equally if not more likely. Jervis argues that unipolarity offers powerful structural incentives for the leading state to be revisionist. These include the absence of countervailing power, the tendency for both the interests and the fears of the leading state to increase as its relative capabilities increase, and the psychological tendency to worry more about the future to the extent the present situation is desirable. Jervis also suggests that these structural incentives are reinforced by particular features of the American approach to unipolarity—the sense after the attacks of September 11, 2001, that the world could and must be transformed and the enduring and widespread belief that international peace and cooperation will be sustained only when all other important states are democratic. The structural and contingent features of contemporary unipolarity point plausibly in the direction of a revisionist unipole, one simultaneously powerful, fearful, and opportunistic. Unipolarity and the Provision of Public Goods Public or collective goods may be consumed by multiple actors without those actors necessarily having to pay the full costs of producing them. The classic theoretical insight is that if enough actors follow their rational self-interest and choose to free ride on the efforts of others, public goods will be underproduced or not produced at all.21 Overcoming the free-rider problem therefore requires cooperation among self-interested actors.22 A good part of the ir literature, in particular that associated with hegemonic stability theory, hypothesizes that cooperation in international relations requires the leadership of a dominant state.23 [End Page 13] Given its preponderance of economic and military resources, the dominant state has the ability to bear a disproportionate share of the costs of providing international collective goods such as an open world economy or a stable security order. The dominant state has an interest in bearing those costs because it benefits disproportionately from promoting systemwide outcomes that reflect its values and interests. During the cold war the United States took on the responsibilities that Kindleberger argued were needed to promote international economic stability, such as serving as an open market of last resort and allowing the use of its currency for exchange and reserve purposes. International economic stability among the Western powers reinforced their security alliance against the Soviet Union. The United States also bore a disproportionate share of the direct costs of Western alliance security. The Soviet Union, on its side of the international divide, ultimately shouldered disproportionate alliance costs as well.24 Waltz took the argument a step further, arguing that in the bipolar system the United States and the Soviet Union may have been adversaries but, as the two dominant powers, shared a mutual interest in system stability, an interest that prompted them to cooperate in providing public goods such as nuclear nonproliferation.25 Hedley Bull makes a similar point in his classic study of the international system as a society of states.26 How might the shift from a bipolar to a unipolar system affect the inclination of the now singularly dominant state to provide international public goods? Two hypotheses arise, with contradictory behavioral expectations. First, we might expect a unipole to take on an even greater responsibility for the provision of international public goods. The capabilities of a unipole relative to other major states are greater than those of either dominant power in a bipolar structure. The unipole’s incentive should be stronger as well, since it now has the opportunity to influence international outcomes globally, not just in its [End Page 14] particular subsystem. We should expect the unipole to try to “lock in” a durable international order that reflects its interests and values.27 A second hypothesis, however, suggests the opposite. We should expect a unipolar power to underproduce public goods despite its preponderant capabilities. The fact that it is unthreatened by peer competitors and relatively unconstrained by other states creates incentives for the unipole to pursue more parochial interests even at the expense of a stable international order. The fact that it is extraordinarily powerful means that the unipole will be more inclined to force adjustment costs on others, rather than bear disproportionate burdens itself. Two of the contributions below address these issues. Michael Mastanduno’s analysis of the global political economy shows that the dominant state will be both system maker and privilege taker—it will seek simultaneously to provide public goods and to exploit its advantageous structural position for parochial gain. It enlists the cooperation of other states and seeks, with varying degrees of success, to force adjustment burdens upon them. Jervis suggests that because the unipole has wide discretion in determining the nature and the extent of the goods provided, its efforts are likely to be perceived by less powerful states as hypocritical attempts to mask the actual pursuit of private goods.

#### Credibility being essential to effectively dealing with other nations is a myth- the US is the dominant actor and shouldn’t fixate on boosting its credibility. Turns the aff - focusing on credibility stunts effective US foreign policy

Stephen M. Walt [Professor of International Relations at Harvard]¶ Tuesday, September 11, 2012¶ Why are U.S. leaders so obsessed with credibility?¶ http://walt.foreignpolicy.com/posts/2012/09/11/the\_credibility\_fetish

What's the biggest mistake the United States has made since the end of the Cold War? Invading Iraq? Helping screw up the Israel-Palestine peace process? Missing the warning signs for 9/11, and then overreacting to the actual level of danger that Al Qaeda really posed? Not recognizing we had a bubble economy and a corrupt financial industry until after the 2007 meltdown?¶ Those are all worthy candidates, and I'm sure readers can think of others. But today I want to propose another persistent error, which lies at the heart of many of the missed opportunities or sins of commission that we made since the Berlin Wall came down. It is in essence a conceptual mistake: a failure to realize just how much the world changed when the Soviet Union collapsed, and a concomitant failure to adjust our basic approach to foreign policy appropriately.¶ I call this error the "credibility fetish." U.S. leaders have continued to believe that our security depends on convincing both allies and adversaries that we are steadfast, loyal, reliable, etc., and that our security guarantees are iron-clad. It is a formula that reinforces diplomatic rigidity, because it requires us to keep doing things to keep allies happy and issuing threats (or in some cases, taking actions) to convince foes that we are serious. And while it might have made some degree of sense during the Cold War, it is increasingly counterproductive today.¶ One could argue that credibility did matter during the Cold War. The United States did face a serious peer competitor in those days, and the Soviet Union did have impressive military capabilities. Although a direct Soviet attack on vital U.S. interests was always unlikely, one could at least imagine certain events that might have shifted the global balance of power dramatically. For example, had the Soviet Union been able to conquer Western Europe or the Persian Gulf and incorporate these assets into its larger empire, it would have had serious consequences for the United States. Accordingly, U.S. leaders worked hard to make sure that the U.S. commitment to NATO was credible, and we did similar things to bolster U.S. credibility in Asia and the Gulf.¶ Of course, we probably overstated the importance of "credibility" even then. Sloppy analogies like the infamous "domino theory" helped convince Americans that we had to fight in places that didn't matter (e.g., Vietnam) in order to convince everyone that we'd also be willing to fight in places that did. We also managed to convince ourselves that credible nuclear deterrence depended on having a mythical ability to "prevail" in an all-out nuclear exchange, even though winning would have had little meaning once a few dozen missiles had been fired.¶ Nonetheless, in the rigid, bipolar context of the Cold War, it made sense for the United States to pay some attention to its credibility as an alliance leader and security provider. But today, the United States faces no peer competitor, and it is hard to think of any single event that would provoke a rapid and decisive shift in the global balance of power. Instead of a clear geopolitical rival, we face a group of medium powers: some of them friendly (Germany, the UK, Japan, etc.) and some of them partly antagonistic (Russia, China). Yet Russia is economically linked to our NATO allies, and China is a major U.S. trading partner and has been a major financier of U.S. debt. This not your parents' Cold War. There are also influential regional powers such as Turkey, India, or Brazil, with whom the U.S. relationship is mixed: We agree on some issues and are at odds on others. And then there are clients who depend on U.S. protection (Israel, Saudi Arabia, Afghanistan, Taiwan, etc.) but whose behavior often creates serious headaches for whoever is in the White House.¶ As distinguished diplomat Chas Freeman recently commented, "the complexity and dynamism of the new order place a premium on diplomatic agility. Stolid constancy and loyalty to pre-existing alliance relationship are not the self-evident virtues they once were. We should not be surprised that erstwhile allies put their own interest ahead of ours and act accordingly. Where it is to our long-term advantage, we should do the same."¶ What might this mean in practice? As I've noted repeatedly, it means beginning by recognizing that the United States is both very powerful and very secure, and that there's hardly anything that could happen in the international system that would alter the global balance of power overnight. The balance is shifting, to be sure, but these adjustments will take place over the course of decades. Weaker states who would like U.S. protection need it a lot more than we need them, which means our "credibility" is more their problem than ours. Which in turn means that if other states want our help, they should be willing to do a lot to convince us to provide it.¶ Instead of obsessing about our own "credibility," in short, and bending over backwards to convince the Japanese, South Koreans, Singaporeans, Afghans, Israelis, Saudis, and others that we will do whatever it takes to protect them, we ought to be asking them what they are going to do for themselves, and also for us. And instead of spending all our time trying to scare the bejeezus out of countries like Iran (which merely reinforces their interest in getting some sort of deterrent), we ought to be reminding them over and over that we have a lot to offer and are open to better relations, even if the clerical regime remains in power and maybe even if -- horrors! -- it retains possession of the full nuclear fuel cycle (under IAEA safeguards). If nothing else, adopting a less confrontational posture is bound to complicate their own calculations.¶ This is not an argument for Bush-style unilateralism, or for a retreat to Fortress America. Rather, it is a call for greater imagination and flexibility in how we deal with friends and foes alike. I'm not saying that we should strive for zero credibility, of course; I'm merely saying that we'd be better off if other states understood that our credibility was more conditional. In other words, allies need to be reminded that our help is conditional on their compliance with our interests (at least to some degree) and adversaries should also be reminded that our opposition is equally conditional on what they do. In both cases we also need to recognize that we are rarely going to get other states to do everything we want. Above all, it is a call to recognize that our geopolitical position, military power, and underlying economic strength give us the luxury of being agile in precisely the way that Freeman depicts.¶ Of course, some present U.S. allies would be alarmed by the course I'm suggesting, because it would affect the sweetheart deals they've been enjoying for years. They'll tell us they are losing confidence in our leadership, and they'll threaten to go neutral, or maybe even align with our adversaries. Where possible, they will enlist Americans who are sympathetic to their plight to pressure on U.S. politicians to offer new assurances. In most cases, however, such threats don't need to be taken seriously. And we just have to patiently explain to them that we're not necessarily abandoning them, we are merely 1) making our support more conditional on their cooperation with us on things we care about, and 2) remaining open to improving relations with other countries, including some countries that some of our current allies might have doubts about. I know: It's a radical position: we are simply going to pursue the American national interest, instead of letting our allies around the world define it for us.¶ The bottom line is that the United States is in a terrific position to play realpolitik on a global scale, precisely because it needs alliance partners less than most of its partners do. And even when allies are of considerable value to us, we still have the most leverage in nearly every case. As soon as we start obsessing about our credibility, however, we hand that leverage back to our weaker partners and we constrain our ability to pursue meaningful diplomatic solutions to existing conflicts. Fetishizing credibility, in short, is one of the reasons American diplomacy has achieved relatively little since the end of the Cold War.

#### China favors concessions and peaceful resolution—regime instability and empirics

**Asia Times 11** (Sudha Ramachandran, “China plays long game on border disputes,” Jan 27, 2011, <http://www.atimes.com/atimes/China/MA27Ad02.html>)

A Sino-Tajik border agreement that was ratified recently by Tajikistan's parliament flies in the face of images of China being a "bullying" and "belligerent" power that "will go to any length to fulfill its territorial ambitions". The agreement, which resolves a 130-year-old territorial dispute, requires Tajikistan to cede around 1,000 square kilometers of land in the Pamir Mountains to China. It means that China will receive roughly 3.5% of the 28,000 square kilometers of land

 it laid claim to. China's territorial concession has been hailed by Tajik Foreign Minister Hamrokhon Zarifi as a "victory for Tajik diplomacy". This is not the first time that China has made concessions to settle its territorial disputes. Under its border agreements with Kazakhstan and Kyrgyzstan, for instance, China received just 22% and 32% respectively of the land disputed with these countries. China's boundaries with Central Asia were originally drawn up under what China describes as "unequal treaties". It alleged that as a result of these treaties, Czarist Russia gained territory at its expense. It therefore refused to recognize these boundaries. Although the Soviet Union and China began negotiating a mutually acceptable border, a settlement remained elusive. With the breakup of the Soviet Union in 1990, the new Central Asian Republics - Tajikistan, Kazakhstan and Kyrgyzstan - inherited the disputes with China. In the 1990s, China began negotiating settlements with these countries. Border agreements with Kyrgyzstan and Kazakhstan were reached in 1996 and 1998 respectively. Border talks with Tajikistan were delayed by the civil war there. However, talks gathered momentum in the late 1990s and an agreement was reached in 2002. It was this agreement that was ratified recently. Analysts have drawn attention to the territorial concessions that China extended to resolve its many disputes. Of its 23 territorial disputes active since 1949, China offered "substantial compromises" in 17, usually agreeing "to accept less than half of the territory being disputed," M Taylor Fravel, associate professor at the Massachusetts Institute of Technology, pointed out in the article "Regime Insecurity and International Cooperation: Explaining China's Compromises in Territorial Disputes," published in the journal International Security. However, there is more to it than meets the eye. The territorial concessions that China is believed to have made are not quite as substantial as they appear to be. Srikanth Kondapalli, a China expert at the Jawaharlal Nehru University in New Delhi pointed out that China's strategy of stepping up territorial claims and then settling for less has enabled it to appear to be making a major territorial concession to reach a border resolution agreement. In several disputes, "whether China actually gave up territory or made a substantial concession is a debatable question," he told Asia Times Online. Still, in the quest for regional stability China overall "has been liberal in border dispute resolution", he said. What has prompted Beijing to seek compromise and extend concessions with regard to territorial disputes involving its land borders? Regime insecurity appears to have been an important motivating factor. According to Fravel, "China's leaders have compromised when faced with internal threats to regime security - the revolt in Tibet, the instability following the Great Leap Forward, the legitimacy crisis after the Tiananmen upheaval, and separatist violence in Xinjiang." The territorial concessions it made to Kazakhstan, Kyrgyzstan and Tajikistan in order to reach border agreements with them was prompted by a sharp surge in separatist violence in Xinjiang province in the early 1990s. The disintegration of the Soviet Union and the emergence of Kazakhstan, Kyrgyzstan and Tajikistan as independent republics stoked long-smoldering Uighur nationalism in Xinjiang and fueled Uighur aspirations for independence. This triggered apprehension in Beijing that Xinjiang would break away. Coming close on the heels of the Tiananmen uprising of 1989, which had undermined the Chinese government's legitimacy, the separatist violence in Xinjiang compounded Chinese regime insecurity, as it posed a threat to China's territorial integrity. This made it imperative for Beijing to nip Uighur unrest in the bud. China's strategy to deal with Uighur separatism has involved ruthless suppression of separatists and economic development of the Xinjiang region. However, the success of this strategy hinged on support from countries bordering Xinjiang - Kazakhstan, Kyrgyzstan and Tajikistan. Their cooperation was essential to get them to crack down on Uighur separatists taking sanctuary on their soil as well as to build robust trade ties that were needed for economic development in Xinjiang. Beijing thus traded territorial concessions for support from Kazakhstan, Kyrgyzstan and Tajikistan in its strategy to quell Uighur separatism. With the exception of its territorial disputes with India and Bhutan, China has settled all its other land-border disputes. In contrast, it has resolved none of its maritime border disputes, although the dispute in the Gulf of Tonkin with Vietnam is being discussed and those discussions are at an advanced stage of resolution. China's strategy for resolving its border disputes and the nature of its border-resolution mechanism provide useful pointers to what lies ahead. In the past, "it is when the contestant state is weak that China has moved quickly to resolve the dispute," points out Kondapalli. The way it went about handling its territorial disputes with the Soviet Union is indicative. Although China did discuss them with the Soviet Union, it was only when the USSR disintegrated that Beijing moved quickly to achieve resolution.

### 2NC

### Legal Lib

The executive will bypass your plan – empirics prove.

Schwarz, senior counsel, and Huq, associate counsel at the Brennan Center for Justice at NYU School of Law, 2007 [Frederick A.O., Jr., partner at Cravath, Swaine & Moore, chief counsel to the Church Committee, and Aziz Z, former clerk for the U.S. Supreme Court, Unchecked and Unbalanced: Presidential Power in a Time of Terror, p. 153]

Familiar failings from the Cold War era and earlier history returned to haunt the nation in the wake of 9/11. But this time abuses were compounded by a new and dangerous idea. To justify illicit invasions of liberty and privacy, the executive branch's lawyers argued that the president has unlimited power to violate federal statutes. President Bush agreed. Specifically, he asserted under the Constitution a novel authority in the name of "national security" or "military necessity" to disregard permanently any law enacted by Congress. The Administration used this power to justify set-asides of long-standing federal statutes barring torture, indefinite detention, and warrantless spying. In the Cold War, the FBI and the CIA violated the law but hid or denied their actions. After 9/11, government overreaching claimed a legal basis through theories about "executive power." Abuse became official policy and practice of the United States. No sitting president before President Bush asserted or used power under the Constitution to set aside laws wholesale. Such power means a president can ignore statutes passed by Congress whenever he claims that "national security" or "military necessity" is at issue. This claim finds precedent in the seventeenth-century British kings' royal "prerogative" power to "suspend" or "dispense" with laws enacted by Parliament.' But that power, grounded in ideas about the "divine" right of kings, did not survive the English Civil War and the Glorious Revolution of 1688, which ended the Stuart dynasty. Certainly, it did not find its way into our founding documents, the 1776 Declaration of Independence and the Constitution of 1787.

Thats a legalistic trick - will still use Article II powers.

Goldsmith 13 (Jack, Henry L. Shattuck Professor at Harvard Law School, served as Assistant Attorney General, Office of Legal Counsel from 2003–2004, and Special Counsel to the Department of Defense from 2002–2003, “Eight Thoughts on the Broad Reading of Article II Inherent in Bobby’s Conjecture,” May 28, 2013, <http://www.lawfareblog.com/2013/05/eight-thoughts-on-the-broad-reading-of-article-ii-inherent-in-bobbys-conjecture/#more-19381>)

Third, Ben asks: “[H]ow do we feel about what we might term a militarily active peace—that is, a peace in which drone strikes and special forces operations take place regularly, a peace that is so minimally different from warfare that nobody (except Bobby) even noticed that we had transitioned from wartime to peacetime?” As Ben implies, if Bobby is right, the Obama administration’s post-AUMF “peace” or “no more war” trope **should not be taken too seriously**. It would be little more than a (domestic law) legalistic trick to say that we are not at “war” if we are regularly exercising the use of force around the globe, albeit in pinpoint fashion, just because the President would be acting in self-defense under Article II rather than pursuant to an AUMF. We are currently engaged in numerous and manifold military and paramilitary and intelligence operations in **many countries outside Afghanistan** (see Mark Mazzetti’s book for a recent description). The scale and persistence of the operations means that many of them would amount to “armed conflicts” even if they were justified as self-defense. And with some caveats about Obama administration practice below, they should (when conducted by DOD) at a minimum trigger at least the reporting provisions (and perhaps more) under the War Powers Resolution. Fourth, the stealth self-defensive war that Bobby describes and that I think the administration envisions in a post-AUMF world is even less bounded than the AUMF-war in this sense: force can be used wherever a threatening group meets the (slippery-at-best and auto-interpreted) “imminent threat” threshold, as long as the nation in question consents or is unwilling or unable to prevent the threat. The Article II war, unlike the AUMF war, requires no nexus to al Qaeda or its associates. Fifth, if it continues at anything like its current scale in a post-AUMF world, war based on Article II would be in even more need of congressional oversight and transparency than the AUMF war – especially in light the unboundedness described above, the Armed Services Committee’s apparent cluelessness about how DOD interprets its authorities today, and the Obama-era innovations **of classified annexes** to War Powers Resolution reports and the potential exclusion of many drone attacks from the WPR framework altogether. The revised AUMF that Bobby, Ben, Matt, and I proposed was designed precisely to bring accountability and oversight to such an extra-AUMF war. We have been criticized for wanting to expand the “war.” That was not our intention, for we assumed that the “war” would continue beyond the AUMF in any event and aimed to bring more accountability and oversight to it. Whether one likes our proposal or not, the nation must find some framework that interjects Congress into reviewing and approving the forthcoming self-defensive extra-AUMF Article II war. (A good place to begin, and indeed a book devoted in large part to establishing a congressional legal framework to check unilateral self-defensive presidential uses of force, and excessive reliance on covert action, is Harold Koh’s The National Security Constitution.)

#### The executive will arbitrarily define words - means even if you don't find my analysis compelling military lawyers are much smarter than that.

Pollack, 13 -- MSU Guggenheim Fellow and professor of history emeritus [Norman, "Drones, Israel, and the Eclipse of Democracy," Counterpunch, 2-5-13, www.counterpunch.org/2013/02/05/drones-israel-and-the-eclipse-of-democracy/, accessed 9-1-13, mss]

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

### Living in Fear K

Ceding the educational space as a site for politics makes authoritarianism inevitable

Giroux, 2006 (Henry A., “Dirty Democracy and State Terrorism: The Politics of the New Authoritarianism in the United States,” Comparative Studies of South Asia, Africa and the Middle East, Volume 26, Number 2)

Such circumstances require that pedagogy be embraced as a moral and political practice, one that is directive and not dogmatic, an outgrowth of struggles designed to resist the increasing depoliticization of political culture that is the hallmark of the current Bush revolution.**Education is the terrain where consciousness is shaped**, needs are constructed, and the capacity for individual self-refl ection and broad social change is nurtured and produced. Education has assumed an unparalleled signifi cance in shaping the language, values, and ideologies that legitimize the structures and organizations that support the imperatives of global capitalism. Efforts to reduce it to a technique or methodology set aside, education remains a crucial site for the production and struggle over those pedagogical and political conditions that provide the possibilities for people to develop forms of agency that enable them individually and collectively to intervene in the processes through which the material relations of power shape the meaning and practices of their everyday lives. Within the current historical context,**struggles over power take on a symbolic and discursive as well as** a material and **institutional form**. Thestruggle over education is about more than the struggle over meaning and identity; it is alsoabout how meaning, knowledge, and values are produced, authorized, and made operational within economic and structural relations of power. **Education**is not at odds with politics;it is an important and crucial element in any defi nition of the political and **offers** not only the theoretical tools for **a systematic critique of authoritarianism**but also a language of possibilityfor creating actual movements for democratic social change and a new biopolitics that affi rms life rather than death, shared responsibility rather than shared fears, and engaged citizenship rather than the stripped-down values of consumerism. At stake here is combining symbolic forms and processes conducive to democratization with broader social contexts and the institutional formations of power itself. The key point here is to understand and engage educational and pedagogical practices from the point of view of how they are bound up with larger relations of power. Educators, students, and parents need to be clearer about how power works through and in texts, representations, and discourses, while at the same time recognizing that power cannot be limited to the study of representations and discourses, even at the level of public policy. Changing consciousness is not the same as altering the institutional basis of oppression; at the same time,**institutional reform cannot take place without a change in consciousness capable of recognizing**not only **injustice** but also the very possibility for reform, the capacity to reinvent the conditions and practices that make a more just future possible. In addition, it is crucial to raise questions about the relationship between pedagogy and civic culture, on the one hand, and what it takes for individuals and social groups to believe that they have any responsibility whatsoever even to address the realities of class, race, gender, and other specifi c forms of domination, on the other hand. For too long, the progressives have ignored that **the strategic dimension of politics is inextricably connected to questions of critical education**and pedagogy, to what it means to acknowledge that education is always tangled up with power, ideologies, values, and the acquisition of both particular forms of agency and specifi c visions of the future. The primacy of critical pedagogy to politics, social change, and the radical imagination in such dark times is dramatically captured by the internationally renowned sociologist Zygmunt Bauman. He writes, Adverse odds may be overwhelming, and yet a democratic (or, as Cornelius Castoriadis would say, an autonomous) society knows of no substitute for education and self-education as a means to inf luence the turn of events that can be squared with its own nature, while that nature cannot be preserved for long without “critical pedagogy”—an education sharpening its critical edge, “making society feel guilty” and “stirring things up” through stirring human consciences. The fates of freedom, of democracy that makes it possible while being made possible by it, and of education that breeds dissatisfaction with the level of both freedom and democracy achieved thus far, are inextricably connected and not to be detached from one another. One may view that intimate connection as another specimen of a vicious circle—but it is within that circle that human hopes and the chances of humanity are inscribed, and can be nowhere else.59 Fortunately, power is never completely on the side of domination, religious fanaticism, or political corruption. Neither is it entirely in the hands of those who view democracy as an excess or burden. Educators need to develop a new discourse and a revitalized global politics whose aim is to foster a democratic pedagogyand political culture that embody the legacy and principles of social justice, equality, freedom, and rights associated with democratic notions of time, space, pluralism, power, discourse, identities, morality, and the future. But such a politics cannot be simply nation based. If it is to be effective, it has to fi nd ways to globalize both justice and resistance, use the new media as critical pedagogical tools, and form new alliances among various oppositional groups, taking seriously pedagogy as a political practice that crosses borders, affi rms difference, and generates new international alliances in the struggle for new public spaces. More and more individuals and movements at home and around the globe including students, workers, feminists, educators, writers, environmentalists, senior citizens, artists, and a host of others are organizing to challenge the dangerous slide on the part of the United States into the dark abyss of an authoritarianism that threatens not just the promise but the very idea of global democracy in the twenty-fi rst century.

#### Engineers solve.

**Fox 11**—Assistant Editor, InnovationNewsDaily (Stuart, 2 July 2011, “Why Cyberwar Is Unlikely ,” http://www.securitynewsdaily.com/cyberwar-unlikely-deterrence-cyber-war-0931/, RBatra)

. Even if an attacker were to overcome his fear of retaliation, the low rate of success would naturally give him pause. Any cyberattack would target the types of complex systems that could collapse on their own, such as electrical systems or banking networks. But experience gained in fixing day-to-day problems on those systems would allow the engineers who maintain them to **quickly undo damage caused by even the most complex cyberattack**, said George Smith, a senior fellow at Globalsecurity.org in Alexandria, Va. "You mean to tell me that the people who work the electrical system 24 hours a day don't respond to problems? What prevents people from turning the lights right back on?" Smith told SecurityNewsDaily. "And attacks on the financial system have always been a non-starter for me. I mean, [in 2008] the financial system attacked the U.S.!"

The paradox risk turns their impact calculus upside down – if your standard is a chain of plausible links, then existential risk becomes a race to the bottom.

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

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

The affirmative represents a strategy of power shifting concerning cyber security - couching the terms of that debate in apocalyptic frames invites military domination.

Schneier 11 (Bruce, founder, BT Managfsed Security Solutions; chief technology officer, BT Managed Security Solutions;MA, computer science, American U; “The threat of cyberwar has been hugely hyped” *CNN;* July 7, 2011; <http://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/>

There's a power struggle going on in the U.S. government right now. It's about who is in charge of cyber security, and how much control the government will exert over civilian networks. And by beating the drums of war, the military is coming out on top. "The United States is fighting a cyberwar today, and we are losing," [said](http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html?sid=ST2010031901063) former NSA director -- and current cyberwar contractor -- Mike McConnell. "Cyber 9/11 has happened over the last ten years, but it happened slowly so we don't see it," said former National Cyber Security Division director Amit Yoran. Richard Clarke, whom Yoran replaced, wrote an entire [book](http://www.harpercollins.com/books/Cyber-War/?isbn=9780061962233) hyping the threat of cyberwar. General Keith Alexander, the current commander of the U.S. Cyber Command, [hypes](http://www.wired.com/dangerroom/2010/04/pentagon-networks-targeted-by-hundreds-of-thousands-of-probes/) it every chance he gets. This isn't just rhetoric of a few over-eager government officials and headline writers; the entire national debate on cyberwar is plagued with [exaggerations](http://www.computerworld.com/s/article/9174682/Senators_ramp_up_cyberwar_rhetoric_) and [hyperbole](http://www.wired.com/dangerroom/2010/04/top-officer-fears-cyberwar-hearts-karzai-tweets-with-help/). Googling those [names](http://www.salon.com/news/opinion/glenn_greenwald/2010/03/29/mcconnell) and [terms](http://www.wired.com/threatlevel/2008/01/feds-must-exami/) -- as well as "cyber Pearl Harbor," "[cyber Katrina](http://www.businessweek.com/the_thread/techbeat/archives/2009/02/fearing_cyber_katrina_obama_candidate_for_cyber_czar_urges_a_fema_for_the_internet.html)," and even "cyber Armageddon" -- gives some idea how pervasive these memes are. Prefix "cyber" to something scary, and you end up with [something](http://www.computerworld.com/s/article/9173967/Cyberattacks_an_existential_threat_to_U.S._FBI_says) really scary. Cyberspace has all sorts of threats, day in and day out. Cybercrime is by far the largest: fraud, through identity theft and other means, extortion, and so on. Cyber-espionage is another, both government- and corporate-sponsored. Traditional hacking, without a profit motive, is still a threat. So is cyber-activism: people, most often kids, playing politics by attacking government and corporate websites and networks. These threats cover a wide variety of perpetrators, motivations, tactics, and goals. You can see this variety in what the media has mislabeled as "cyberwar." The attacks against Estonian websites in 2007 were [simple hacking](http://www.wired.com/threatlevel/2007/08/cyber-war-and-e/) attacks by ethnic Russians angry at anti-Russian policies; these were denial-of-service attacks, a normal risk in cyberspace and hardly unprecedented. A real-world comparison might be if an army invaded a country, then all got in line in front of people at the DMV so they couldn't renew their licenses. If that's what war looks like in the 21st century, we have little to fear. Similar [attacks](http://www.csoonline.com/article/443579/georgia-cyber-attacks-from-russian-government-not-so-fast) against Georgia, which accompanied an actual Russian invasion, were also probably the responsibility of citizen activists or [organized crime](http://www.csoonline.com/article/499778/georgia-cyberattacks-linked-to-russian-organized-crime). A series of power blackouts in Brazil was caused by criminal extortionists -- or was it [sooty insulators](http://www.wired.com/threatlevel/2009/11/brazil_blackout/)? China is [engaging](http://www.schneier.com/essay-227.html) in espionage, not war, in cyberspace. And so on. One problem is that there's no clear [definition](http://thehill.com/opinion/op-ed/70319-no-line-between-cyber-crime-and-cyber-war) of "cyberwar." What does it look like? How does it start? When is it over? Even cybersecurity experts don't know the answers to these questions, and it's dangerous to broadly apply the term "war" unless we know a war is going on. Yet recent news articles have claimed that China [declared](http://techcrunch.com/2007/10/18/cyberwar-china-declares-war-on-western-search-sites/) cyberwar on Google, that Germany attacked China, and that a group of young hackers declared cyberwar on Australia. (Yes, cyberwar is so easy that even kids can do it.) Clearly we're not talking about real war here, but a rhetorical war: like the war on terror. We have a variety of institutions that can defend us when attacked: the police, the military, the Department of Homeland Security, various commercial products and services, and our own personal or corporate lawyers. The legal framework for any particular attack depends on two things: the attacker and the motive. Those are precisely the two things you don't know when you're being attacked on the Internet. We saw this on July 4 last year, when U.S. and South Korean websites were [attacked](http://www.schneier.com/essay-280.html) by unknown perpetrators from North Korea -- or perhaps England. Or was it Florida? We surely need to improve our cybersecurity. But words have meaning, and metaphors matter. There's a power struggle going on for control of our nation's cybersecurity strategy, and the NSA and DoD [are](http://www.wired.com/dangerroom/2010/05/cyber-command-we-dont-wanna-defend-the-internet-but-we-just-might-have-to/) winning. If we frame the debate in terms of war, if we accept the military's expansive cyberspace definition of "war," we feed our fears. We reinforce the notion that we're helpless -- what person or organization can defend itself in a war? -- and others need to protect us. We invite the military to take over security, and to ignore the limits on power that often get jettisoned during wartime. If, on the other hand, we use the more measured language of cybercrime, we change the debate. Crime fighting requires both resolve and resources, but it's done within the context of normal life. We willingly give our police extraordinary powers of investigation and arrest, but we temper these powers with a judicial system and legal protections for citizens. We need to be prepared for war, and a Cyber Command is just as vital as an Army or a Strategic Air Command. And because kid hackers and cyber-warriors use the same tactics, the defenses we build against crime and espionage will also protect us from more concerted attacks. But we're not fighting a cyberwar now, and the risks of a cyberwar are no greater than the risks of a ground invasion. We need peacetime cyber-security, administered within the myriad structure of public and private security institutions we already have.

Their scenarios are a strategy of alarmism aimed at creating a permanent military-cyber-industrial complex.

Thompson 11 Mark, national security reporter, Time Magazine; Pulitzer Prize winner; “Cyber War Worrywarts” *Time Magazine*; August 8, 2011; <http://battleland.blogs.time.com/2011/08/08/cyber-war-worrywarts/>

Defense Secretary Leon Panetta whipped up the cyber-threat Friday during his get-acquainted visit to Nebraska's Offutt Air Force Base, home of the U.S. Strategic Command. "We could face a cyber attack that could be the equivalent of Pearl Harbor," he said. Such an attack, Panetta warned, could "take down our power grid system, take down our financial systems in this country, take down our government systems, take down our banking systems. They could virtually paralyze this country. We have to be prepared to deal with that." The whole debate over cyber war is getting really interesting. The ratio of scaremongers to calm logic -- currently about a 2-to-1 edge in favor of the Jules Verne crowd -- is reflected in a trio of major stories on the topic recently. This is from a recent Bloomberg BusinessWeek cover [story](http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html): This Code War era is no superpower stare-down; it's more like Europe in 1938, when the Continent was in chaos and global conflict seemed inevitable. [Here](http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109)'s the latest from Vanity Fair (which is where I always turn for the latest in balanced, relevant reporting on national-security matters): Hackers from many countries have been exfiltrating—that is, stealing—intellectual property from American corporations and the U.S. government on a massive scale, and Chinese hackers are among the main culprits. So it was a little like being a thirsty man stumbling into an oasis after weeks in the desert to drink the cool water [provided](http://www.nationaljournal.com/magazine/fear-of-cyberattack-may-be-biggest-threat-20110721) by Michael Hirsh in National Journal: In truth, cyberskeptics abound…These skeptics say that much of the alarm stems from a fear of the unknown rather than from concrete evidence of life-and-death threats. It is, they suggest, a 21st-century version of the medieval mapmakers who would mark the boundaries of the known world and then draw mythical beasts on the other side conveying the message: “Here, there be dragons.”…Critics worry that this fear is only going to create the biggest dragon of all: a permanent military-cyber industrial complex not unlike the one that President Eisenhower warned of at the dawn of the nuclear age...The danger is that the U.S. government will do what it has been arguably doing in spades since 9/11: overreact. Spend too much. Go overboard with surveillance. Crimp and constrain freedoms, this time involving the Internet. By George, I think Hirsh has nailed it. Next time there is some cyber hypester on television, pay attention to where his or her paycheck comes from. Nearly all of them work for corporations eager to use their voices as bellows to fan the flames of cyber-attack fears; others work for companies whose job it is to maximize the potential cyber threats so you will buy their software and expertise to defend against them.