# 1AC

### Plan

#### The United States federal government should statutorily prohibit the authority of the President of the United States to authorize the preemptive use of offensive cyber-attacks.

### Adv- CyberWar

#### The Squo offensive cyber posture attacks risk retaliatory cycles and arms races

Moss 13

Columnist at The Diplomat Trefor Moss is an independent journalist based in Hong Kong. He covers Asian politics, defence and security, and was Asia-Pacific Editor at Jane’s Defence Weekly until 2009, Is Cyber War the New Cold War?, 4/19/13, <http://thediplomat.com/2013/04/19/is-cyber-war-the-new-cold-war/2/>

Although setting up a cybersecurity working group with China, Washington has also signaled it intends to escalate. U.S. Cyber Command and NSA chief General Keith Alexander signaled this shift of policy gears earlier this month when he [told Congress](http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?_r=4&) that of 40 new CYBERCOM teams currently being assembled, 13 would be focused on offensive operations. Gen Alexander also gave new insight into CYBERCOM’s operational structure. The command will consist of three groups, he said: one to protect critical infrastructure; a second to support the military’s regional commands; and a third to conduct national offensive operations. As cyber competition intensifies between the U.S. and China in particular, the international community approaches a crossroads. States might begin to rein in their cyber operations before things get further out of hand, adopt a rules-based system governing cyberspace, and start respecting one another’s virtual sovereignty much as they do one another’s physical sovereignty. Or, if attacks and counter-attacks are left unchecked, cyberspace may become the venue for a new Cold War for the Internet generation. Much as the old Cold War was characterized by indirect conflict involving proxy forces in third-party states, its 21stcentury reboot might become a story of virtual conflict prosecuted by shadowy actors in the digital realm. And as this undeclared conflict poisons bilateral relations over time, the risk of it spilling over into kinetic hostilities will only grow.

#### New rules change the restrained conduct of cyberwar up to this point – grant Obama unfettered power do define the threat – makes a cyber aggression inevitable

RT 13 < Hacker in chief: Obama given right to launch 'preemptive' cyberattacks, Published time: February 04, 2013 18:39, http://rt.com/usa/obama-us-administration-cyber-435/>#SPS

¶ A secret review has concluded that US President Obama has the authority to launch a preemptive cyber attack on any country on the basis that they are considered a ‘cyber threat’ – even if there is no concrete evidence of this threat.¶ It may not be long before the US conducts crippling attacks on foreign soil with little more than a mouse click, thereby sparing itself the effort of sending its military oversees or declaring war.¶ The Obama administration is currently drawing up a set of rules about how the US military can defend against or conduct cyberattacks, the New York Times reports. The Obama administration is also allowing intelligence agencies to declare potential threats. But even if these threats are nothing more than a suspicion without evidence, the military now has the authority to attack foreign nations, regardless of whether or not the US is involved in a conflict with them.¶ This would not only spare the US from sending its own troops overseas, but it would also allow the administration to make decisions without the deliberation that usually occurs before sending Americans into a conflict zone. And if the administration conducts an attack based on false premises, it would be saved the embarrassment that occurred when President George W. Bush sent thousands of US troops into a war with Iraq that lasted nearly 9 years, based on the false premise that Iraq possessed weapons of mass destruction and was a security threat.¶ With no overseas deployments necessary to conduct a cyberattack, the administration would have nothing to lose by anonymously targeting and destroying infrastructure based on its own suspicions of a threat. The administration’s new rules would also allow the military to operate domestically, the thought of which has always made many people uncomfortable. The White House in October [signed](http://rt.com/usa/news/directive-military-deployment-us-892/) a presidential policy directive that aims to “finalize new rules of engagement that would guide commanders when and how the military can go outside government networks to prevent a cyberattack that could cause significant destruction or casualties.”¶ A senior administration official told the Times that the US has so far kept its cyber capabilities restrained and that the new rules could allow the administration to exercise its full potential.¶ “There are levels of cyberwarfare that are far more aggressive than anything that has been used or recommended to be done,” the official said.¶ The administration has already used computer worms to cripple other countries’ infrastructure, including a series of attacks against Iran’s nuclear power plants, one of which took out nearly 1,000 of the 5,000 centrifuges of the Natanz plant. The attack was controlled from inside the Pentagon, which now has a new Cyber Command and a growing budget that would allow it to conduct more extensive cyberattacks. ¶ The Pentagon’s foundation of such an office demonstrates the administration’s preparation for cyberwarfare, in which both the US and terrorists can strike each other by taking down power grids, financial systems and communications networks. The Cyber Command office is experiencing a growing budget, while the Department of Defense is preparing for spending cuts and is slashing budgets for other Pentagon departments, indicating the importance of its work to the administration.¶ The rules have been in development for nearly two years, but they were leaked to the Times at a convenient moment for the administration: The New York Times, Bloomberg L.P., the Wall Street Journal and the Washington Post all claim that their computers have been penetrated by Chinese hackers and had been targeted for years. The computer security company Mandiant also alleged that Chinese hackers had stolen contacts, information and files from more than 30 US newspaper journalists and executives, many of which had written about Chinese leaders and political and legal issues in China.¶ But the Chinese Ministry of National Defense has denied that its people had anything to do with the suspected attacks, stating that “Chinese laws prohibit any action including hacking that damages Internet security.” The ministry also expressed anger about the accusations, stating that “to accuse the Chinese military of launching cyberattacks without solid proof is unprofessional and baseless.”¶ “We have seen over the last years an increase in not only the hacking attempts on government institutions but also nongovernmental ones,” US Secretary of State Hillary Clinton told reporters on Thursday, emphasizing that the Chinese “are not the only people who are hacking us.”¶ The administration has also recently announced that an unnamed American power station was crippled for weeks by cyberattacks, without releasing details about the location of the plant. With little proof about the alleged cyberattacks and the suspected threats, the White House now reserves the right to make major cyberwarfare decisions, despite Congress’ long-standing disapproval.¶ “The [National Security Administration’s] cyber security operations have been kept very, very secret, and because of that it has been impossible for the public to react to them,” said Electronic Privacy Information Center attorney Arnie Stepanovich in November. “[That makes it] very difficult, we believe, for Congress to legislate in this area.”¶ The Obama administration has long pushed for Congress to pass the Cyber Intelligence Sharing and Protection Act, which would grant the government greater access to the Internet and cybersecurity information from the private sector. US Homeland Security Secretary Janet Napolitano, [claims](http://rt.com/usa/news/napolitano-us-cyber-attack-761/) it is necessary to prevent a “cyber 9/11” attack that would knock out water, electricity and gas, causing destruction similar to that left behind by Hurricane Sandy.¶ But privacy advocates have long expressed concern that this measure would give the government access to Americans’ personal e-mails, online chat conversations, and other personal information that only private companies and servers might have access too, prompting Congress to reject the measure.¶ Alongside privacy concerns, the Obama administration’s increasing access to cybersecurity information and cyberwarfare capabilities provides the president with an unknown amount of power to conduct anonymous attacks on foreign infrastructure.¶ While using this technology to attack military objects, such as anti-aircraft or missile defense radars in war zones, would not surprise anyone, the US now also reserves the right to attack other countries with which it has not declared war.¶ With the US ranking first in a 2012 study that drew up a “Cyber Power Index”, other nations whose conduct conflicts with US wishes could become more vulnerable than ever – especially since International Law allows countries to defend themselves against foreign threats, and these “threats” can now be concluded based on vague intelligence analysis of a 'potential' cyber attack.

#### It goes nuclear

[we don’t even have to win escalation -- command and control hacking, crisis instability, and fracturing nuclear agreements all ensure independent nuclear response- congressional restrictions are key to solve]

Austin, 8/6

Director of Policy Innovation at the EastWest Institute, Costs of American Cyber Superiority, <http://www.chinausfocus.com/peace-security/costs-of-american-cyber-superiority/>

The United States is racing for the technological frontier in military and intelligence uses of cyber space. It is ahead of all others, and has mobilized massive non-military assets and private contractors in that effort. This constellation of private sector opportunity and deliberate government policy has been aptly labeled in recent months and years by so many credible observers (in The Economist, The Financial Times and the MIT Technology Review) as the cyber industrial complex. The United States is now in the unusual situation where the head of a spy agency (NSA) also runs a major military unified command (Cyber Command). This is probably an unprecedented alignment of Praetorian political power in any major democracy in modern political history. This allocation of such political weight to one military commander is of course for the United States to decide and is a legitimate course of action. But it has consequences. The Snowden case hints at some of the blow-back effects now visible in public. But there are others, less visible. The NSA Prism program exists because it is technologically possible and there have been no effective restraints on its international targeting. This lack of restraint is especially important because the command and control of strategic nuclear weapons is a potential target both of cyber espionage and offensive cyber operations. The argument here is not to suggest a similarity between the weapons themselves, but to identify correctly the very close relationship between cyber operations and nuclear weapons planning. Thus the lack of restraint in cyber weapons might arguably affect (destabilize) pre-existing agreements that constrain nuclear weapons deployment and possible use. The cyber superiority of the United States, while legal and understandable, is now a cause of strategic instability between nuclear armed powers. This is similar to the situation that persisted with nuclear weapons themselves until 1969 when the USSR first proposed an end of the race for the technological frontier of potential planetary devastation. After achieving initial capability, the U.S. nuclear missile build up was not a rational military response to each step increase in Soviet military capability. It was a race for the technological frontier – by both sides – with insufficient recognition of the consequences. This conclusion was borne out by a remarkable Top Secret study commissioned in 1974 by the U.S. Secretary of Defense, Dr James Schlesinger. By the time it was completed and submitted in 1981, it assessed that the nuclear arms build-up by both sides was driven – not by a supposed tit for tat escalation in capability of deployed military systems – but rather by an unconstrained race for the technological limits of each side’s military potential and by its own military doctrinal preferences. The decisions of each side were not for the most part, according to this now declassified study, a direct response to particular systems that the other side was building. In 1969, the USSR acted first to propose an end to the race for the technological frontier of nuclear weapons because it knew it was losing the contest and because it knew there was political sentiment in the United States and in its Allied countries that supported limitations on the unbridled nuclear fetish. As we ponder the American cyber industrial complex of today, we see a similar constellation of opposition to its power emerging. This constellation includes not just the political rivals who see they are losing in cyber space (China and Russia), but nervous allies who see themselves as the likely biggest victims of the American race for cyber superiority, and loyal American military commanders who can see the risks and dangers of that quest. It is time for the United States to take stock of the collateral damage that its quest for cyber military power, including its understandable quest for intelligence superiority over the terrorist enemy, has caused amongst its allies. The loss has not yet been seen at the high political level among allies, in spite of several pro forma requests for information from countries such as Germany. The loss of U.S. credibility has happened more at the popular level. Around the world, once loyal supporters of the United States in its war on terrorism had a reasonable expectation to be treated as faithful allies. They had the expectation, perhaps naïve, that privacy was a value the Americans shared with them. They did not expect to be subject to such a crude distinction (“you are all non-Americans now”). They did not want to know that their entire personal lives in cyber space are now recoverable – should someone so decide – by the running of a bit of software in the NSA. After the Prism revelations, so many of these foreign citizens with an internationalist persuasion and solidarity for the United States now feel a little betrayed. Yet, in the long run, the most influential voice to end the American quest for cyber military superiority may come from its own armed forces. There are military figures in the United States who have had responsibility for nuclear weapons command and control systems and who, in private, counsel caution. They advocate the need to abandon the quest for cyber dominance and pursue a strategy of “mutual security” in cyber space – though that has yet to be defined. They cite military exercises where the Blue team gets little or no warning of Red team disruptive cyber attack on systems that might affect critical nuclear command and control or wider war mobilization functions. Strategic nuclear stability may be at risk because of uncertainty about innovations in cyber attack capability. This question is worth much more attention. U.S. national security strategy in cyber space needs to be brought under stronger civilian oversight and subject to **more** rigorous public scrutiny. The focus on Chinese cyber espionage has totally preempted proper debate about American cyber military power. Most in the United States Congress have lined up to condemn Snowden. That is understandable. But where are the critical voices looking at the bigger picture of strategic instability in cyberspace that existed before Snowden and has now been aggravated because of him? The Russian and Chinese rejections of reasonable U.S. demands for Snowden’s extradition may be every bit as reasonable given their anxiety about unconstrained American cyber superiority.

#### Cyber preemption escalates to a shooting war

Clarke 2009

(Richard Clarke, special adviser to the president for cybersecurity in the George W. Bush administration and chairman of Good Harbor Consulting, November/December 2009, “War from Cyberspace,” The National Interest, <http://web.clas.ufl.edu/users/zselden/coursereading2011/Clarkecyber.pdf>)

As in the 1960s, **the speed of war is rapidly accelerating.** Then, long-range ¶ ¶ missiles could launch from the prairie of ¶ ¶ Wyoming and hit Moscow in only thirtyfive minutes. Strikes in cyber war move at ¶ ¶ a rate approaching the speed of light. And ¶ ¶ **this speed favors a strategy of preemption, which means the chances that people can become trigger-happy are high.** **This**, in ¶ ¶ turn, **makes cyber war all the more likely.** ¶ ¶ If a cyber-war commander does not attack quickly, his network may be destroyed first. **If a commander does not preempt an enemy, he may find that the target nation has suddenly raised new defenses or even disconnected from the worldwide Internet.** ¶ ¶ There seems to be a premium in cyber war ¶ ¶ to making the first move.¶ ¶ And much as in the nuclear era, **there is a real risk of escalation with cyber war.** ¶ ¶ Nuclear war was generally believed to be ¶ ¶ something that might quickly grow out of ¶ ¶ conventional combat, perhaps initiated with ¶ ¶ tanks firing at each other in a divided Berlin. The speed of new technologies created ¶ ¶ enormous risks for crisis instability and miscalculation. Today, **the risks of miscalculation are even higher, enhancing the chances that what begins as a battle of computer programs ends in a shooting war.** Cyber ¶ ¶ war, with its low risks to the cyber warriors, ¶ ¶ may be seen by a decision maker as a way ¶ ¶ of sending a signal, making a point without ¶ ¶ actually shooting. An attacker would likely ¶ ¶ think of a cyber offensive that knocked out ¶ ¶ an electric-power grid and even destroyed ¶ ¶ some of the grid’s key components (keeping ¶ ¶ the system down for weeks), as a somewhat ¶ ¶ antiseptic move; a way to keep tensions ¶ ¶ as low as possible. But **for the millions of people thrown into the dark** and perhaps ¶ ¶ the cold, unable to get food, without access ¶ ¶ to cash and dealing with social disorder, ¶ ¶ **it would be in many ways the same as if bombs had been dropped on their cities. Thus, the nation attacked might well respond with “kinetic activity.”**

**That also causes miscalculation of nuclear forces**

**Clark and Andreasen 13**

(Richard A. Clarke, the chairman of Good Harbor Security Risk Management, was special adviser to the president for cybersecurity in the George W. Bush administration. Steve Andreasen, a consultant to the Nuclear Threat Initiative, was the National Security Council’s staff director for defense policy and arms control from 1993 to 2001, “Cyberwar’s threat does not justify a new policy of nuclear deterrence” June 14, 2013, <http://articles.washingtonpost.com/2013-06-14/opinions/39977598_1_nuclear-weapons-cyber-attack-cyberattacks>, KB)

President Obama is expected to unveil a new nuclear policy initiative this week in Berlin. Whether he can make good on his first-term commitments to end outdated Cold War nuclear policies may depend on a firm presidential directive to the Pentagon rejecting any new missions for nuclear weapons — in particular, their use in response to cyberattacks.¶ The Pentagon’s Defense Science Board concluded this year that **China and Russia could develop capabilities to launch an “existential cyber attack” against the United States** — that is, **an attack causing sufficient damage that our government would lose control of the country.** “**While the manifestation of a nuclear and cyber attack are** very **different**,” the board concluded, “in the end, **the existential impact to the United States is the same.”**¶ Because it will be impossible to fully defend our systems against existential cyberthreats, the board argued, the United States must be prepared to threaten the use of nuclear weapons to deter cyberattacks. In other words: I’ll see your cyberwar and raise you a nuclear response.¶ Some would argue that Obama made clear in his 2010 Nuclear Posture Reviewthat the United States has adopted the objective of making deterrence of nuclear attacks the “sole purpose” of our nuclear weapons. Well, the board effectively reviewed the fine print and concluded that the Nuclear Posture Review was “essentially silent” on the relationship between U.S. nuclear weapons and cyberthreats, so connecting the two “is not precluded in the stated policy.”¶ As the board noted, cyberattacks can occur very quickly and without warning, requiring rapid decision-making by those responsible for protecting our country. **Integrating the nuclear threat into the equation means making clear to any potential adversary that the United States is prepared to use nuc**lear weapon**s very early in response to a major cyberattack — and is maintaining nuclear forces on “prompt launch” status to do so.**¶ **Russia and China would** certainly take note — and presumably **follow suit**. Moreover, **if the United States, Russia and China adopted policies threatening an early nuclear response to cyber­attacks, more countries would surely take the same approach.**¶ It’s hard to see how this cyber-nuclear action-reaction dynamic would improve U.S. or global security. It’s more likely to lead to a new focus by Pentagon planners on generating an expanding list of cyber-related targets and the operational deployment of nuclear forces to strike those targets in minutes.¶ Against that backdrop, maintaining momentum toward reducing the role of nuclear weapons in the United States’ national security strategy (and that of other nations) — a general policy course pursued by the past five presidents — would become far more difficult. **Further reductions in nuclear forces and changes in “hair-trigger” postures, designed to lessen the risk of an accidental or unauthorized nuclear launch, would** also probably **stall**.¶ Fortunately, Obama has both the authority and the opportunity to make clear that he meant what he said when he laid out his nuclear policy in Prague in 2009. For decades, presidential decision directives have made clear the purpose of nuclear weapons in U.S. national security strategy and provided broad guidance for military planners who prepare the operations and targeting plans for our nuclear forces. An update to existing presidential guidance is one of the homework items tasked by the 2010 Nuclear Posture Review.¶ Cyberthreats are very real, and **there is** much we ne**ed to do to defend our military and critical civilian infrastructure against** what former defense secretary Leon E. Panetta referred to as **a “cyber Pearl Harbor”** — including enhancing the ability to take action, when directed by the president, against those who would attack us. We also need more diplomacy such as that practiced by Obama with his Chinese counterpart, Xi Jinping, at their recent summit. Multinational cooperation centers could ultimately lead to shared approaches to cybersecurity, including agreements related to limiting cyberwar.

**Criticizing the probability of our impacts is meaningless – all wars are low probability, what matters is that cyberwar is more likely to escalate than other conflicts, which uniquely warrants academic attention**

**Junio ‘13**

[Timothy J. Junio (Tim)is a doctoral candidate of political science at the¶ University of Pennsylvania and a predoctoral fellow at the Center for¶ International Security and Cooperation (CISAC) at Stanford University.¶ He also develops new cyber capabilities at the Defense Advanced¶ Research Projects Agency (DARPA). How Probable is Cyber War? Bringing¶ IR Theory Back In to the Cyber Conflict Debate, Journal of Strategic Studies, 36:1,¶ 125-133. ETB]

Two recent articles in the pages of this journal contribute to an¶ important debate about how information technology (IT) inﬂuences¶ international politics.1¶ Thomas **Rid and** Adam **Liff argue that** **cyber**¶ **‘war’** has never happened and probably **will not happen. A fundamental**¶ **problem** with these articles **is that Rid and Liff do not commit to a**¶ **theoretical framework regarding the causes of war.** **Doing so yields an**¶ **opposite conclusion:** i**nternational** r**elations theory identiﬁes many**¶ **mechanisms that may cause violent escalation with cyber weapons**.¶ This brief response article explains why **cyber war is sufﬁciently**¶ **probable to merit serious attention from scholars and practitioners**,¶ and proposes a theoretical research agenda. **First, domestic political**¶ **factors** – such as states’ command and control over cyber operations –¶ **must be problematized**. **The principal-agent approach demonstrates**¶ **how variation in incentives and preferences may make militaries more**¶ **likely to favor cyber attack than other kinds of bureaucracies.** This¶ matters in societies with poor civilian control over the military. Second,¶ **the unique material qualities of IT must be evaluated alongside**¶ **traditional mechanisms that cause war**. For instance, **the attribution**¶ **problem and computational complexity in modeling cyber operations**¶ **may increase the odds of inadvertent cyber war by causing states to**¶ **retaliate against the wrong targets or miscalculate the potential costs**¶ **and gains of attacking.**¶What is Cyber War? (Again. . .)¶ Rid and Liff do not deﬁne cyber war the same way, and there is no¶ disciplinary consensus. Rid, Liff, and this author at least agree on the¶ following: **cyber war is a coercive act involving computer network**¶ **attack. Network attack means information is disrupted, degraded, or**¶ **destroyed**. **‘Coercive’ means using force to change or preserve a political**¶ **status quo**. A point of contention is lethality, which Rid believes is¶ necessary for cyber ‘war’.2¶ This is an extreme and undesirable¶ requirement, particularly because (as Rid himself points out) non-lethal¶ cyber attacks may be more costly than conventional warfare.3¶ It is¶ important to note that Rid focuses on network attack, whereas Liff¶ considers a broader conﬂict process. This response addresses both.¶ The central point of Rid’s article is that it is difﬁcult to cause lethal¶ effects with cyber weapons, and that politically motivated, instrumental cyber attack has never killed anyone.4¶ While the empirics of his¶ article are sound – he describes recent cyber attacks accurately – **Rid**¶ **never explains what causes war or makes war more or less likely. The**¶ **arguments in his article are exclusively deﬁnitional, and do not directly**¶ **support his title’s assertion that ‘Cyber War Will Not Take Place**.’¶ Liff does better from a theoretical point of view; he links his article to¶ the bargaining approach to war.5¶ He does an excellent job of offering¶ counterpoints to four arguments about why cyber attack may increase¶ the probability of war. However, **Liff** never establishes why his¶ reasonable views are more plausible than their alternatives. This is¶ because he **is not explicit about assumptions that are necessary for his**¶ **arguments to hold, nor about the circumstances under which those**¶ **assumptions break down**. For example, Liff argues that private¶ information may make war less likely because states poorly estimate he gains from cyber attack.6¶ Although Liff is right to point out that¶ ambiguity in cyber operations is important, he is wrong to assume the¶ causal arrow points in one direction. Ambiguity can make war more or¶ less likely, because it may lead states to overestimate their potential¶ gains, overestimate their stealth, and/or underestimate their adversary’s¶ skill.¶ Finally, **it must be recognized that any future war is a low probability event. Crafting claims that particular conﬂict scenarios are improbable** is rather unimpressive**; what is important to understand is the potential cost and probability of cyber war relative to other kinds of conﬂict.**¶Causes of Cyber War¶ **The noted problems in the Rid and Liff articles could have been**¶ **avoided by drawing on structured theoretical approaches that are**¶ **common to the study of the causes of all kinds of warfare**. What would¶ such an approach look like? This response lacks the space to fully¶ develop one, but recommends a way forward. Literally **dozens of**¶ **arguments have been advanced in the political science discipline**¶ **regarding the causes of war, and very many of these offer reasons to**¶ **believe cyber war is** plausible or even **probable**.7¶ An approach,¶ advanced in James Fearon’s modern classic ‘Rationalist Explanations¶ for War,’ is to list assumptions that create an ideal condition in which¶ war should never happen.8¶ One way to structure scientiﬁc inquiry¶ regarding the probability of cyber war is to examine how **the unique**¶ **material qualities of IT affect each of the assumptions**. Table 1 offers a¶ cursory version of such an analysis to identify priority areas for further¶ study. Among a large number of revealed paths to cyber war, one –¶ principal-agent problems involving the bureaucracies that conduct¶ cyber operations – is detailed here to demonstrate the plausibility of¶ speciﬁc mechanisms and what follow-on empirical work should look¶ like.¶ Principal-Agent Problems¶ Rid and Liff appear to assume that states are unitary rational actors¶ (URAs), and do not explain the domestic political processes whereby¶ states make foreign policy choices. **Empirically and theoretically, it is important to relax the URA assumption and problematize who has**¶ **formal and actual release authority over cyber weapons.** **The principal agent approach**, for instance, **works from the premise that** individuals and **organizations often vary in their incentives and preferences, which could make war beneﬁcial for some at the cost of others**.9¶ **This** and¶ related **thinking inform how scholars study other military technologies,**¶ **such as nuclear weapons**. Scott Sagan points out **that although unauthorized nuclear war is improbable, it is sufﬁciently probable that people should worry a great deal about command and control (C2)** **issues**.10 Many anecdotes echo Sagan’s work. For example, a Russian¶ general was asked during the Cold War about his backup plan in the¶ event he could not open the safe containing his nuclear launch codes.¶ His answer was that he would bash the safe open with a sledgehammer¶ he kept nearby!11¶ Consideration of how bureaucracies do what they do – like keeping¶ emergency nuclear war sledgehammers – is of critical importance to the¶ cyber C2 question. Although controlling large organizations is a core¶ function of militaries, **the conduct of cyber operations is different from**¶ **other kinds of activity in a way that greatly magniﬁes the ‘strategic corporal’ problem. This is because constant cyber operations** other than¶ war **decrease the bureaucratic friction that normally alerts superiors to**¶ **aberrant behavior.** In the case of nuclear weapons, a long chain of¶ events is required before unauthorized activities occur. Someone¶ probably would notice a crazed general using his sledgehammer on¶ the launch codes safe, turning keys, fueling missiles, and so on. In¶ contrast, **it is a core function of cyber bureaucrats to access adversary**¶ **networks constantly, and to develop push-button solutions to minimize**¶ **lags during war**. Furthermore**, if the perception that cyber weapons are**¶ **non-lethal comes to be widely perceived** (as Rid would prefer), **it is**¶ **reasonable to conclude that** the threshold for their use will be lower¶ **than other kinds of weapons – even if the cost of cyber attacks is**¶ **greater.**¶While weak C2 is a necessary condition for a war caused by¶ principal-agent problems, it is not sufﬁcient, because bureaucracies¶ (agents) must also have different incentives or preferences from their¶ populations or leaders (the ‘principals’). A deep political science literature argues that militaries are more prone to favor offensive operations than other kinds of bureaucracies.12 Early evidence suggests that¶ **this ‘cult of the offensive’ operates regarding cyber warfare**. James¶ **Cartwright**, the former Vice Chairman of the US Joint Chiefs of Staff,¶ **calls for the United States to engage in more offensive cyber operations,**¶ **and reportedly created a bureaucracy to that end.**13 **This perspective exists in other countries; ofﬁcials with** South Korea’s Cyber Command¶ believe that ‘the best defense is a good offense’**, and that they should**¶ **preemptively disable menacing foreign servers.14** Chinese military¶ textbooks recommend ‘information offensive through computer network attack’in advance of conventional warfare.15 In contrast, nearly¶ all other bureaucracies – such as those responsible for diplomacy, law¶ enforcement, and homeland security – appear oriented toward cyber¶ defense.¶ **If this offensive mindset is observed in countries where civilians have**¶ **ﬁrm control over military organizations, then what is the risk from**¶ **countries with different civil-military relations?16 The thought of weak**¶ **or military-dominated states possessing advanced cyber capabilities is**¶ **troubling,** to say the least, **and offers highly plausible paths to cyber**¶ **wa**r. An example, **North Korea, already has demonstrated offensive**¶ **tendencies, as that government appears to have conducted disruptive**¶ **and destructive cyber attacks**.17¶ **Many potential paths to war result from a combination of ‘cult of the**¶ **offensive’ reasoning and weak C2. One is for militaries to justify cyber**¶ **attack as acts of self-defense or preemption. Another is for militaries to**¶ **conduct offensive cyber operations without informing their superiors.**¶ **Yet another is the potential for offensive biases to make them more**¶ **easily fall bait to ‘false ﬂag’ operations**. These are merely derivatives of¶ principal-agent problems that arise among politically motivated actors;¶ the outlook worsens when considering other incentives, such as proﬁt,¶ that may lead corrupt bureaucrats to sell lethal skills or software to the¶ highest bidder.¶ **So, how much should scholars and practitioners care about cyber wa**r?¶ A belief that cyber war is hyped appears to have motivated Rid and Liff¶ to pen their pieces. **A satisfying answer must explain at least two things:**¶ **the destructive potential of cyber war, and the probability that it will**¶ **happen. It appears uncontroversial that,** if **cyber war** happens, it **will be** ¶ **highly costly** even if not lethal. Few contest the idea that a successful¶ and sustained degradation of military capabilities, deprivation of¶ civilian services, destruction of ﬁnancial records, or other such ‘digital¶ Pearl Harbor’ scenarios, would be pretty bad.¶ On the other hand, there is little agreement in academic or policy¶ circles regarding whether or not cyber war will happen. **This response**¶ **offers an important corrective to narratives that cyber war is**¶ **improbable. A small number of premises lead to a conclusion that**¶cyber war is, at a minimum, plausible enough to merit serious¶ attention. Further research would do well to commit to theoretical¶ paradigms, such as the approach recommended in Table 1. This kind of¶ rigorous scholarship is a prerequisite to reducing the incidence of cyber¶ conﬂict and avoiding cyber war.

**Understanding the risks of current US posture reduces the chances of cyber war escalation- worst case assessments are the best preparation**

**Clarke and Knake ‘10**

[Richard Alan Clarke is the former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States. Robert K. Knake, Former international affairs fellow in residence @ CFR. Cyber War. ETB]

In the seminal 1983 movie about computers and war, War Games, ¶ starring a young Matthew Broderick, the tinny computer voice ¶ asked haltingly, “Do you want to play a game of thermonuclear war?” ¶ Why don’t we play a game of cyber war in order to elucidate some of ¶ the policy choices that shape a strategy. DoD runs such exercises, ¶ called Cyber Storm, annually. The CIA’s annual cyber war exercise, ¶ Silent Horizon, has been happening since 2007. For the purposes of ¶ this analysis, I’ll make the same request of you that I made of students ¶ at Harvard’s Kennedy School and national security bureaucrats sitting ¶ around the White House Situation Room conference table: “Don’t ¶ fight the scenario.” By that I mean, do not spend a lot of timerejecting ¶ thepremise that circumstances couldhappen someday that would ¶result inthe U.S. being on the edgeofconflict with Russia or China**. When U.S. cyber warriors talk about the “big one,” they usually** ¶ **have in mind a conflict in cyberspace with Russia or China**, the two ¶ nations with the most sophisticated offensive capability other than ¶ the U.S. **No one wants hostilities with those countries to happen.** ¶ **Thinking about it, for the purposes of understanding what cyber** ¶ **war would look like, does not make it more likely**. In fact, by understanding the risks of our current cyber war posture, we might reduce ¶ the chances of a real cyber war**.** **And if, despite our intentions, a** ¶ **cyber war does happen, it would be best to have thought in advance** ¶ **about how it could unravel.**¶ **Certainly, I did not want to see the attack of 9/11 happen, but I** ¶ **had chaired countless** “tabletop exercises,” or **war game scenarios,** **to** ¶ **get myself and the bureaucracy ready in case something like it did** ¶ **happen**. **When it came, we had already thought through how to re­**¶ **spond on the day of an attack and the few days thereafter**. We spent ¶ enormous effort to try to prevent attacks, but we also devoted some ¶ time to thinking about what we would do if one succeeded. **Had we** ¶ **not done so, that awful day would have been even worse**. **So**, **in that** ¶ **spirit of learning by visualizing, let’s think about a period of rising** ¶ **tensions** between the U.S. and China.

**Arguing against the practices of the USFG in the context of war powers allows for an engaged public that can expose the hypocrisy of the federal government – only focus on specific policy questions can actualize change by making it relevant to policy-makers –**

**Mellor 13**

The Australian National University, ANU College of Asia and the Pacific, Department Of International Relations,
“Why policy relevance is a moral necessity: Just war theory, impact, and UAVs,” European University Institute, Paper Prepared for BISA Conference 2013, DOA: 8-14-13

**This** section of the paper **considers** more generally **the need for** just war **theorists to engage with policy debate** **about the use of force**, **as** **well as to engage with the** more **fundamental moral and philosophical principles** of the just war tradition. **It draws on** John **Kelsay’s** **conception of just war thinking as being a social practice**,35 **as well as on** Michael **Walzer’s understanding of the role of the social critic in society**.36 It argues that the just war tradition is a form of “practical discourse” which is concerned with questions of “how we should act.”37 Kelsay argues that: **[T]he criteria of jus ad bellum and jus in bello provide a framework for structured participation in a public conversation about the use of military force** . . . **citizens who choose to speak in just war terms express commitments** . . . [i**]n the process of giving and asking for** **reasons for going to war**, **those who argue** in just war terms **seek to influence policy** **by persuading others that their analysis provides a way to express and fulfil the desire that military actions be** both **wise and just.38** He also argues that “**good just war thinking involves continuous and complete deliberation**, in the sense that one attends to all the standard criteria at war’s inception, at its end, and **throughout the course of the conflict**.”39 **This** is important as it **highlights the need for** just war **scholars to engage** **with the ongoing operations in war and the specific policies that are involved**. **The question of** **whether a particular** war is just or unjust, and the question of whether a particular **weapon (like drones**) **can be used in accordance with the jus in bello criteria**, only **cover a part of the overall justice of the war**. **Without an engagement with the reality of war**, **in** **terms of the policies used** in waging it, **it is impossible to engage with the “moral reality of war,”40 in terms of being able to discuss it and judge it in moral terms** Kelsay’s description of just war thinking as a social practice is similar to Walzer’s more general description of social criticism. The just war theorist, **as a social critic, must be involved with his or her own society and its practices**. In the same way that the social critic’s distance from his or her society is measured in inches and not miles,41 the just war **theorist must be close to and must understand the language through which war is constituted, interpreted and reinterpreted**.**42 It is only by understanding the values and language that their own society purports to live by that the social critic can hold up a mirror to that society to** **demonstrate** its **hypocrisy** **and to show the gap that exists** between its practice and its values.43 **The tradition** itself **provides a set of** **values and principles and**, as argued by Cian O’Driscoll, **constitutes a “language of engagement**” **to spur participation in public and political debate**.44 This language is part of “our common heritage, the product of many centuries of arguing about war.”45 **These principles and this language provide the terms through which people understand and come to interpret war, not in a deterministic way but by providing the categories necessary for moral understanding and moral argument about the legitimate and illegitimate uses of force**.46 **By spurring and providing the basis for political engagement the just war tradition ensures that the acts that occur within war are considered according to just war criteria and allows policy-makers to be held to account on this basis. Engaging with the reality of war requires** recognising that war is, as Clausewitz stated, **a continuation of policy**. **War**, according to Clausewitz, **is subordinate to politics and to political choices and these political choices can, and must, be judged and critiqued**.47 **Engagement and political debate are morally necessary** **as the alternative is disengagement and moral quietude**, **which is a sacrifice of the obligations of citizenship**.48 **This engagement must bring** just war **theorists into contact with the policy makers** **and** **will require work that is** accessible and **relevant to policy makers**, **however this does not mean a sacrifice of critical distance or an abdication of truth in the face of power.** **By engaging in detail** **with the policies being pursued** and their concordance or otherwise with **the principles of the just war tradition the policy-makers will be forced to account for their decisions and justify them in just war language.** **In contrast to the view**, **suggested** by Kenneth **Anderson, that “the public cannot be made part of the debate**” **and that “[w]e are** necessarily **committed into the hands of our political leadership**”,49 it is incumbent upon just war theorists to ensure that the public are informed and are capable of holding their political leaders to account. **To accept the idea that the political leadership are stewards and that accountability will not benefit the public, on whose behalf action is undertaken, but will only benefit al Qaeda,50 is a grotesque act of intellectual irresponsibility**. As Walzer has argued, it is precisely because it is “our country” that we are “especially obligated to criticise its policies.”51 This paper has discussed the empirics of the policies of drone strikes in the ongoing conflict with those associate with al Qaeda. It has demonstrated that there are significant moral questions raised by the just war tradition regarding some aspects of these policies and it has argued that, thus far, just **war scholars have not paid sufficient attention or engaged in sufficient detail with the policy implications of drone use.** **As such it has been argued that it is necessary for just war theorists to engage more directly with these issues and to ensure that their work is policy relevant**, **not in a utilitarian sense of abdicating from speaking the truth in the face of power**, **but by forcing policy makers to justify** their **actions according to the principles of the just war tradition, principles which they invoke themselves in formulating policy.** **By highlighting hypocrisy and providing the tools and language** **for the interpretation of action**, **the just war tradition provides the basis for the public engagement and political activism that are necessary for democratic politics.52**

**Debate about the repercussions of cyber preemption is good- it generates a broader literature base that encourages restraint**

**Magnuson ‘9**

[Stew, National Defense Magazine. <http://www.nationaldefensemagazine.org/archive/2009/June/Pages/USPlanstoDestroyEnemyComputerNetworksQuestioned.aspx> ETB]

¶ Retired Adm. William **Owen**, **former vice chairman of the Joint Chiefs of Staff,** said he **sees little evidence that there is a government-wide understanding of the repercussions of launching an attack on enemy computers. And that goes for the military as well.**¶¶ “My guess is that most of **the generals and admirals don’t really understand** **what** the hell **we’re** **playing with here** and we need to find a way to get some focused attention” on this topic, he told National Defense.¶ ¶ Owen is the co-author of a National Research Council report, “Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber-Attack Capabilities.”¶ ¶ The study — two-and-a-half years in the making — concludes that **policies and regulations for carrying out computer attacks are “ill-formed, undeveloped and highly uncertain,”** said Kenneth Dam, a former deputy secretary of state who also contributed to the report.¶ ¶ The authors could not identify any single authority in the government responsible for coordinating cyber-attacks or promulgating policy — if there is any policy at all. Further, there are no congressional committees designated to oversee the government’s efforts. ¶ ¶ In short, if the United States government goes on the offense in cyberspace, there may be a lack of accountability, the report concluded.¶ ¶ Secrecy has impeded widespread debate about the nature and implications of cyber-attack, the authors asserted. Much of the defense community’s efforts in this realm are top secret.¶ ¶ “It’s not so much secrecy, it’s actual silence. It just isn’t discussed,” Dam said at a press briefing. **There needs to be a public debate about the repercussions of launching cyber-attacks**, the report said. **In the early days of nuclear weapons, there was a great deal of literature coming out of think tanks, universities and other institutions about when and how to use atomic bombs. That just isn’t happening in this new kind of warfare**, Dam added.

#### War fuels structural violence

Goldstein 2001

IR professor at American University (Joshua, War and Gender, p. 412, Google Books)

First, peace activists face a dilemma in thinking about causes of war and working for peace. **Many peace scholars and activists support the approach, “if you want peace, work for justice.”** Then, if one believes that sexism contributes to war, one can work for gender justice specifically (perhaps. among others) in order to pursue peace. This approach brings strategic allies to the peace movement (women, labor, minorities), but rests on the assumption that injustices cause war. The evidence in this book suggests that **causality runs at least as strongly the other way. War is not a product of capitalism, imperialism, gender, innate aggression,** or any other single cause, **although all of these influence wars’ outbreaks and outcomes. Rather, war has in part** fueled and sustained **these and other injustices**.9 So, “if you want peace, work for peace.” Indeed, if you want justice (gender and others), work for peace. **Causality does not run just upward through the levels of analysis, from types of individuals, societies, and governments up to war. It runs downward too**. Enloe suggests that changes in attitudes towards war and the military may be the most important way to “reverse women’s oppression.” The dilemma is that peace work focused on justice brings to the peace movement energy, allies, and moral grounding, yet, in light of this book’s evidence, **the emphasis on injustice as the main cause of war seems to be** empirically inadequate.

**Squo makes Obama judge, jury, and executioner when it comes to cyberwarfare**

**Gosztola ‘13**

[Kevin Gosztola is a trusted author who publishes his writing regularly to OpEdNews and Open Salon and he is a 2009 Young People For Fellow. <http://dissenter.firedoglake.com/2013/02/04/legal-review-of-presidential-power-to-engage-in-preemptive-cyber-strikes-to-remain-secret/> ETB]

Finally, like with the drone program, President Barack **Obama is presiding over the creation and development of a power that previous presidents never imagined having.** **The** national security **state is effectively appointing him and all future presidents the** proverbial **judge, jury and executioner when it comes to cyber warfare.**¶ There is no indication that any group of members in Congress or judicial body will have to approve of a preemptive strike before it is carried out. As has become typical, the president wants to be able to conduct war without needing authorization.¶ **The policy will expand the imperial presidency and the public and civil society organizations, which** have a distinct interest in knowing what the government is doing, **will be kept in the dark on what is legal and illegal in cyber operations. The Congress will barely make any effort to defend its right to provide oversight of this new power.** And any future details on this power will mostly come from selective leaks provided by officials, who do not think they will face repercussions for talking to the press. **The policy itself, the rules for cyber war, will remain concealed.**

#### Our discussion raises awareness of cyber militarism and spills over to policy

**Owens et al. 09** (WILLIAM A. OWENS, AEA Holdings, Inc., Co-chair KENNETH W. DAM, University of Chicago, Co-chair THOMAS A. BERSON, Anagram Laboratories GERHARD CASPER, Stanford University DAVID D. CLARK, Massachusetts Institute of Technology RICHARD L. GARWIN, IBM Fellow Emeritus JACK L. GOLDSMITH III, Harvard Law School CARL G. O’BERRY, The Boeing Company JEROME H. SALTZER, Massachusetts Institute of Technology (retired) MARK SEIDEN, MSB Associates SARAH SEWALL, Harvard University WALTER B. SLOCOMBE, Caplin & Drysdale WILLIAM O. STUDEMAN, U.S. Navy (retired) MICHAEL A. VATIS, Steptoe & Johnson LLP, “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities”, pdf)

A historical analogy might be drawn to the study of nuclear issues. In many ways, today’s state of affairs **regarding public discourse on cyberattack is analogous to the nuclear debate** of 50 years ago. At that time, **nuclear policy issues were veiled in secrecy**, and **there was little public debate** about them. Herman Kahn’s books (On Thermonuclear War, Thinking the Unthinkable) were the first that addressed in the open literature what it might mean to fight a nuclear war. These **seminal pieces did much to raise the public profile of these issues and stimulated an enormous amount of subsequent work outside government that has had a real impact on nuclear policy**. From our perspective as the co-chairs of this study, the topic of cyberattack is so important across a multitude of national interests—not just defense or even just national security—that **it deserves robust and open discussion and debate**, both among thoughtful professionals in the policy, military, intelligence, law enforcement, and legal fields and among security practitioners in the private sector. But for such discussion and debate to be productive, they must be based on some **common foundation of information about the topic at hand.** Thus, **the report’s role in providing education and background is in our view its most important function.**

#### War facilitates lashout against the other

Rangelov and Kaldor 12

Iavor Rangelov and Mary Kaldor. 2012. Global Security Research Fellow at the Civil Society and Huamn Security Research Unit, Dept of Int’l Development at the Loncon School of Economics and Political Science; Professor of Global Governance and Director of the Civil Society and Human Security Research Unit. Persistent Conflict. Conflict, Security & Development 12:3.

One problem with the literature is the preoccupation with the term ‘conﬂict’. The Uppsala Conﬂict Data Program, which is the source of most statistics on conﬂict including the World Development Report, the Human Security Report and the SIPRI Yearbook on Armaments, Disarmament and International Security, deﬁnes conﬂict as a ‘contested incompatibility’. 7 The implicit assumption is that two or more sides have (legitimate) grievances that can be resolved either through violence or negotiation. Yet as Michel Wieviorka points out, violence may be the opposite of conﬂict; it may close down conﬂict. 8 Conﬂict is the normal human condition and is indeed a source of creativity in society. Democracy can be understood as a peaceful mechanism for managing conﬂict. In conditions of violence, people live in fear and dare not express their grievances. They may and probably do, of course, hate those who kill them or their neighbours and family and they may kill in revenge, but this does not mean they also have some underlying grievance that can be resolved. Their conﬂict is the consequence of violence rather than the other way round. Fine grained analyses of places where violence occurs, such as the ones included in this special issue, suggest that a range of motivations are relevant in explaining violence. For many, though not of course all, it is violence rather than the resolution of conﬂict that is the main goal. Firstly, violence constructs a context in which it is possible to mobilise around extremist ideologies. Xenophobic, fundamentalist, racist or ethnicist political philosophies tend to be marginal in peacetime. In violent situations, people learn to hate ‘the other’ and to seek the ‘protection’ of those who defend them against ‘the other’. Amartya Sen describes the Hindu–Muslim riots in 1947, and how people were ‘trapped into that vicious mode of thinking, and the more savage among them [. . .] were induced to kill “the enemies who kill us” (as they were respectively deﬁned)’. 9 Secondly, of course, violence creates a context for criminal gain—loot, pillage, hostage-taking, various kinds of smuggling. And ﬁnally, all kinds of personal motives, such as land disputes, family feuds, honour killings, excitement, adventure and perversion, are given free rein in violent contexts

#### The state must be engaged---action can be reoriented away from past abuses

Williams and Krause 97

Michael, assistant professor of political science at the University of Southern Maine and Keith, professor of political science at the Graduate Institute of International Studies, associate professor of political science at York University, Critical Security Studies: Concepts and Cases, edited by Krause and Williams, p. xvi

Many of the chapters in this volume thus retain a concern with the centrality of the state as a locus not only of obligation but of effective political action. In the realm of organized violence, states also remain the preeminent actors. The task of a critical approach is not to deny the centrality of the state in this realm but, rather, to understand more fully its structures, dynamics, and possibilities for reorientation. From a critical perspective, state action is flexible and capable of reorientation, and analyzing state policy need not therefore be tantamount to embracing the statist assumptions of orthodox conceptions. To exclude a focus on state action from a critical perspective on the grounds that it plays inevitably within the rules of existing conceptions simply reverses the error of essentializing the state. Moreover, it loses the possibility of influencing what remains the most structurally capable actor in contemporary world politics.

#### Simulated national security law debates preserve agency and enhance decision-making---avoids cooption

Donohue 13

Laura K. Donohue 13, Associate Professor of Law, Georgetown Law, 4/11, “National Security Law Pedagogy and the Role of Simulations”, <http://jnslp.com/wp-content/uploads/2013/04/National-Security-Law-Pedagogy-and-the-Role-of-Simulations.pdf>

The concept of simulations as an aspect of higher education, or in the law school environment, is not new.164 Moot court, after all, is a form of simulation and one of the oldest teaching devices in the law. What is new, however, is the idea of designing a civilian national security course that takes advantage of the doctrinal and experiential components of law school education and integrates the experience through a multi-day simulation. In 2009, I taught the first module based on this design at Stanford Law, which I developed the following year into a full course at Georgetown Law. It has since gone through multiple iterations. The initial concept followed on the federal full-scale Top Official (“TopOff”) exercises, used to train government officials to respond to domestic crises.165 It adapted a Tabletop Exercise, designed with the help of exercise officials at DHS and FEMA, to the law school environment. The Tabletop used one storyline to push on specific legal questions, as students, assigned roles in the discussion, sat around a table and for six hours engaged with the material. The problem with the Tabletop Exercise was that it was too static, and the rigidity of the format left little room, or time, for student agency. Unlike the government’s TopOff exercises, which gave officials the opportunity to fully engage with the many different concerns that arise in the course of a national security crisis as well as the chance to deal with externalities, the Tabletop focused on specific legal issues, even as it controlled for external chaos. The opportunity to provide a more full experience for the students came with the creation of first a one-day, and then a multi-day simulation. The course design and simulation continues to evolve. It offers a model for achieving the pedagogical goals outlined above, in the process developing a rigorous training ground for the next generation of national security lawyers.166 A. Course Design The central idea in structuring the NSL Sim 2.0 course was to bridge the gap between theory and practice by conveying doctrinal material and creating an alternative reality in which students would be forced to act upon legal concerns.167 The exercise itself is a form of problem-based learning, wherein students are given both agency and responsibility for the results. Towards this end, the structure must be at once bounded (directed and focused on certain areas of the law and legal education) and flexible (responsive to student input and decisionmaking). Perhaps the most significant weakness in the use of any constructed universe is the problem of authenticity. Efforts to replicate reality will inevitably fall short. There is simply too much uncertainty, randomness, and complexity in the real world. One way to address this shortcoming, however, is through design and agency. The scenarios with which students grapple and the structural design of the simulation must reflect the national security realm, even as students themselves must make choices that carry consequences. Indeed, to some extent, student decisions themselves must drive the evolution of events within the simulation.168 Additionally, while authenticity matters, it is worth noting that at some level the fact that the incident does not take place in a real-world setting can be a great advantage. That is, the simulation creates an environment where students can make mistakes and learn from these mistakes – without what might otherwise be devastating consequences. It also allows instructors to develop multiple points of feedback to enrich student learning in a way that would be much more difficult to do in a regular practice setting. NSL Sim 2.0 takes as its starting point the national security pedagogical goals discussed above. It works backwards to then engineer a classroom, cyber, and physical/simulation experience to delve into each of these areas. As a substantive matter, the course focuses on the constitutional, statutory, and regulatory authorities in national security law, placing particular focus on the interstices between black letter law and areas where the field is either unsettled or in flux. A key aspect of the course design is that it retains both the doctrinal and experiential components of legal education. Divorcing simulations from the doctrinal environment risks falling short on the first and third national security pedagogical goals: (1) analytical skills and substantive knowledge, and (3) critical thought. A certain amount of both can be learned in the course of a simulation; however, the national security crisis environment is not well-suited to the more thoughtful and careful analytical discussion. What I am thus proposing is a course design in which doctrine is paired with the type of experiential learning more common in a clinical realm. The former precedes the latter, giving students the opportunity to develop depth and breadth prior to the exercise. In order to capture problems related to adaptation and evolution, addressing goal [1(d)], the simulation itself takes place over a multi-day period. Because of the intensity involved in national security matters (and conflicting demands on student time), the model makes use of a multi-user virtual environment. The use of such technology is critical to creating more powerful, immersive simulations.169 It also allows for continual interaction between the players. Multi-user virtual environments have the further advantage of helping to transform the traditional teaching culture, predominantly concerned with manipulating textual and symbolic knowledge, into a culture where students learn and can then be assessed on the basis of their participation in changing practices.170 I thus worked with the Information Technology group at Georgetown Law to build the cyber portal used for NSL Sim 2.0. The twin goals of adaptation and evolution require that students be given a significant amount of agency and responsibility for decisions taken in the course of the simulation. To further this aim, I constituted a Control Team, with six professors, four attorneys from practice, a media expert, six to eight former simulation students, and a number of technology experts. Four of the professors specialize in different areas of national security law and assume roles in the course of the exercise, with the aim of pushing students towards a deeper doctrinal understanding of shifting national security law authorities. One professor plays the role of President of the United States. The sixth professor focuses on questions of professional responsibility. The attorneys from practice help to build the simulation and then, along with all the professors, assume active roles during the simulation itself. Returning students assist in the execution of the play, further developing their understanding of national security law. Throughout the simulation, the Control Team is constantly reacting to student choices. When unexpected decisions are made, professors may choose to pursue the evolution of the story to accomplish the pedagogical aims, or they may choose to cut off play in that area (there are various devices for doing so, such as denying requests, sending materials to labs to be analyzed, drawing the players back into the main storylines, and leaking information to the media). A total immersion simulation involves a number of scenarios, as well as systemic noise, to give students experience in dealing with the second pedagogical goal: factual chaos and information overload. The driving aim here is to teach students how to manage information more effectively. Five to six storylines are thus developed, each with its own arc and evolution. To this are added multiple alterations of the situation, relating to background noise. Thus, unlike hypotheticals, doctrinal problems, single-experience exercises, or even Tabletop exercises, the goal is not to eliminate external conditions, but to embrace them as part of the challenge facing national security lawyers. The simulation itself is problem-based, giving players agency in driving the evolution of the experience – thus addressing goal [2(c)]. This requires a realtime response from the professor(s) overseeing the simulation, pairing bounded storylines with flexibility to emphasize different areas of the law and the students’ practical skills. Indeed, each storyline is based on a problem facing the government, to which players must then respond, generating in turn a set of new issues that must be addressed. The written and oral components of the simulation conform to the fourth pedagogical goal – the types of situations in which national security lawyers will find themselves. Particular emphasis is placed on nontraditional modes of communication, such as legal documents in advance of the crisis itself, meetings in the midst of breaking national security concerns, multiple informal interactions, media exchanges, telephone calls, Congressional testimony, and formal briefings to senior level officials in the course of the simulation as well as during the last class session. These oral components are paired with the preparation of formal legal instruments, such as applications to the Foreign Intelligence Surveillance Court, legal memos, applications for search warrants under Title III, and administrative subpoenas for NSLs. In addition, students are required to prepare a paper outlining their legal authorities prior to the simulation – and to deliver a 90 second oral briefing after the session. To replicate the high-stakes political environment at issue in goals (1) and (5), students are divided into political and legal roles and assigned to different (and competing) institutions: the White House, DoD, DHS, HHS, DOJ, DOS, Congress, state offices, nongovernmental organizations, and the media. This requires students to acknowledge and work within the broader Washington context, even as they are cognizant of the policy implications of their decisions. They must get used to working with policymakers and to representing one of many different considerations that decisionmakers take into account in the national security domain. Scenarios are selected with high consequence events in mind, to ensure that students recognize both the domestic and international dimensions of national security law. Further alterations to the simulation provide for the broader political context – for instance, whether it is an election year, which parties control different branches, and state and local issues in related but distinct areas. The media is given a particularly prominent role. One member of the Control Team runs an AP wire service, while two student players represent print and broadcast media, respectively. The Virtual News Network (“VNN”), which performs in the second capacity, runs continuously during the exercise, in the course of which players may at times be required to appear before the camera. This media component helps to emphasize the broader political context within which national security law is practiced. Both anticipated and unanticipated decisions give rise to ethical questions and matters related to the fifth goal: professional responsibility. The way in which such issues arise stems from simulation design as well as spontaneous interjections from both the Control Team and the participants in the simulation itself. As aforementioned, professors on the Control Team, and practicing attorneys who have previously gone through a simulation, focus on raising decision points that encourage students to consider ethical and professional considerations. Throughout the simulation good judgment and leadership play a key role, determining the players’ effectiveness, with the exercise itself hitting the aim of the integration of the various pedagogical goals. Finally, there are multiple layers of feedback that players receive prior to, during, and following the simulation to help them to gauge their effectiveness. The Socratic method in the course of doctrinal studies provides immediate assessment of the students’ grasp of the law. Written assignments focused on the contours of individual players’ authorities give professors an opportunity to assess students’ level of understanding prior to the simulation. And the simulation itself provides real-time feedback from both peers and professors. The Control Team provides data points for player reflection – for instance, the Control Team member playing President may make decisions based on player input, giving students an immediate impression of their level of persuasiveness, while another Control Team member may reject a FISC application as insufficient. The simulation goes beyond this, however, focusing on teaching students how to develop (6) opportunities for learning in the future. Student meetings with mentors in the field, which take place before the simulation, allow students to work out the institutional and political relationships and the manner in which law operates in practice, even as they learn how to develop mentoring relationships. (Prior to these meetings we have a class discussion about mentoring, professionalism, and feedback). Students, assigned to simulation teams about one quarter of the way through the course, receive peer feedback in the lead-up to the simulation and during the exercise itself. Following the simulation the Control Team and observers provide comments. Judges, who are senior members of the bar in the field of national security law, observe player interactions and provide additional debriefing. The simulation, moreover, is recorded through both the cyber portal and through VNN, allowing students to go back to assess their performance. Individual meetings with the professors teaching the course similarly follow the event. Finally, students end the course with a paper reflecting on their performance and the issues that arose in the course of the simulation, develop frameworks for analyzing uncertainty, tension with colleagues, mistakes, and successes in the future. B. Substantive Areas: Interstices and Threats As a substantive matter, NSL Sim 2.0 is designed to take account of areas of the law central to national security. It focuses on specific authorities that may be brought to bear in the course of a crisis. The decision of which areas to explore is made well in advance of the course. It is particularly helpful here to think about national security authorities on a continuum, as a way to impress upon students that there are shifting standards depending upon the type of threat faced. One course, for instance, might center on the interstices between crime, drugs, terrorism and war. Another might address the intersection of pandemic disease and biological weapons. A third could examine cybercrime and cyberterrorism. This is the most important determination, because the substance of the doctrinal portion of the course and the simulation follows from this decision. For a course focused on the interstices between pandemic disease and biological weapons, for instance, preliminary inquiry would lay out which authorities apply, where the courts have weighed in on the question, and what matters are unsettled. Relevant areas might include public health law, biological weapons provisions, federal quarantine and isolation authorities, habeas corpus and due process, military enforcement and posse comitatus, eminent domain and appropriation of land/property, takings, contact tracing, thermal imaging and surveillance, electronic tagging, vaccination, and intelligence-gathering. The critical areas can then be divided according to the dominant constitutional authority, statutory authorities, regulations, key cases, general rules, and constitutional questions. This, then, becomes a guide for the doctrinal part of the course, as well as the grounds on which the specific scenarios developed for the simulation are based. The authorities, simultaneously, are included in an electronic resource library and embedded in the cyber portal (the Digital Archives) to act as a closed universe of the legal authorities needed by the students in the course of the simulation. Professional responsibility in the national security realm and the institutional relationships of those tasked with responding to biological weapons and pandemic disease also come within the doctrinal part of the course. The simulation itself is based on five to six storylines reflecting the interstices between different areas of the law. The storylines are used to present a coherent, non-linear scenario that can adapt to student responses. Each scenario is mapped out in a three to seven page document, which is then checked with scientists, government officials, and area experts for consistency with how the scenario would likely unfold in real life. For the biological weapons and pandemic disease emphasis, for example, one narrative might relate to the presentation of a patient suspected of carrying yersinia pestis at a hospital in the United States. The document would map out a daily progression of the disease consistent with epidemiological patterns and the central actors in the story: perhaps a U.S. citizen, potential connections to an international terrorist organization, intelligence on the individual’s actions overseas, etc. The scenario would be designed specifically to stress the intersection of public health and counterterrorism/biological weapons threats, and the associated (shifting) authorities, thus requiring the disease initially to look like an innocent presentation (for example, by someone who has traveled from overseas), but then for the storyline to move into the second realm (awareness that this was in fact a concerted attack). A second storyline might relate to a different disease outbreak in another part of the country, with the aim of introducing the Stafford Act/Insurrection Act line and raising federalism concerns. The role of the military here and Title 10/Title 32 questions would similarly arise – with the storyline designed to raise these questions. A third storyline might simply be well developed noise in the system: reports of suspicious activity potentially linked to radioactive material, with the actors linked to nuclear material. A fourth storyline would focus perhaps on container security concerns overseas, progressing through newspaper reports, about containers showing up in local police precincts. State politics would constitute the fifth storyline, raising question of the political pressures on the state officials in the exercise. Here, ethnic concerns, student issues, economic conditions, and community policing concerns might become the focus. The sixth storyline could be further noise in the system – loosely based on current events at the time. In addition to the storylines, a certain amount of noise is injected into the system through press releases, weather updates, private communications, and the like. The five to six storylines, prepared by the Control Team in consultation with experts, become the basis for the preparation of scenario “injects:” i.e., newspaper articles, VNN broadcasts, reports from NGOs, private communications between officials, classified information, government leaks, etc., which, when put together, constitute a linear progression. These are all written and/or filmed prior to the exercise. The progression is then mapped in an hourly chart for the unfolding events over a multi-day period. All six scenarios are placed on the same chart, in six columns, giving the Control Team a birds-eye view of the progression. C. How It Works As for the nuts and bolts of the simulation itself, it traditionally begins outside of class, in the evening, on the grounds that national security crises often occur at inconvenient times and may well involve limited sleep and competing demands.171 Typically, a phone call from a Control Team member posing in a role integral to one of the main storylines, initiates play. Students at this point have been assigned dedicated simulation email addresses and provided access to the cyber portal. The portal itself gives each team the opportunity to converse in a “classified” domain with other team members, as well as access to a public AP wire and broadcast channel, carrying the latest news and on which press releases or (for the media roles) news stories can be posted. The complete universe of legal authorities required for the simulation is located on the cyber portal in the Digital Archives, as are forms required for some of the legal instruments (saving students the time of developing these from scratch in the course of play). Additional “classified” material – both general and SCI – has been provided to the relevant student teams. The Control Team has access to the complete site. For the next two (or three) days, outside of student initiatives (which, at their prompting, may include face-to-face meetings between the players), the entire simulation takes place through the cyber portal. The Control Team, immediately active, begins responding to player decisions as they become public (and occasionally, through monitoring the “classified” communications, before they are released). This time period provides a ramp-up to the third (or fourth) day of play, allowing for the adjustment of any substantive, student, or technology concerns, while setting the stage for the breaking crisis. The third (or fourth) day of play takes place entirely at Georgetown Law. A special room is constructed for meetings between the President and principals, in the form of either the National Security Council or the Homeland Security Council, with breakout rooms assigned to each of the agencies involved in the NSC process. Congress is provided with its own physical space, in which meetings, committee hearings and legislative drafting can take place. State government officials are allotted their own area, separate from the federal domain, with the Media placed between the three major interests. The Control Team is sequestered in a different area, to which students are not admitted. At each of the major areas, the cyber portal is publicly displayed on large flat panel screens, allowing for the streaming of video updates from the media, AP wire injects, articles from the students assigned to represent leading newspapers, and press releases. Students use their own laptop computers for team decisions and communication. As the storylines unfold, the Control Team takes on a variety of roles, such as that of the President, Vice President, President’s chief of staff, governor of a state, public health officials, and foreign dignitaries. Some of the roles are adopted on the fly, depending upon player responses and queries as the storylines progress. Judges, given full access to each player domain, determine how effectively the students accomplish the national security goals. The judges are themselves well-experienced in the practice of national security law, as well as in legal education. They thus can offer a unique perspective on the scenarios confronted by the students, the manner in which the simulation unfolded, and how the students performed in their various capacities. At the end of the day, the exercise terminates and an immediate hotwash is held, in which players are first debriefed on what occurred during the simulation. Because of the players’ divergent experiences and the different roles assigned to them, the students at this point are often unaware of the complete picture. The judges and formal observers then offer reflections on the simulation and determine which teams performed most effectively. Over the next few classes, more details about the simulation emerge, as students discuss it in more depth and consider limitations created by their knowledge or institutional position, questions that arose in regard to their grasp of the law, the types of decision-making processes that occurred, and the effectiveness of their – and other students’ – performances. Reflection papers, paired with oral briefings, focus on the substantive issues raised by the simulation and introduce the opportunity for students to reflect on how to create opportunities for learning in the future. The course then formally ends.172 Learning, however, continues beyond the temporal confines of the semester. Students who perform well and who would like to continue to participate in the simulations are invited back as members of the control team, giving them a chance to deepen their understanding of national security law. Following graduation, a few students who go in to the field are then invited to continue their affiliation as National Security Law fellows, becoming increasingly involved in the evolution of the exercise itself. This system of vertical integration helps to build a mentoring environment for the students while they are enrolled in law school and to create opportunities for learning and mentorship post-graduation. It helps to keep the exercise current and reflective of emerging national security concerns. And it builds a strong community of individuals with common interests. CONCLUSION The legal academy has, of late, been swept up in concern about the economic conditions that affect the placement of law school graduates. The image being conveyed, however, does not resonate in every legal field. It is particularly inapposite to the burgeoning opportunities presented to students in national security. That the conversation about legal education is taking place now should come as little surprise. Quite apart from economic concern is the traditional introspection that follows American military engagement. It makes sense: law overlaps substantially with political power, being at once both the expression of government authority and the effort to limit the same. The one-size fits all approach currently dominating the conversation in legal education, however, appears ill-suited to address the concerns raised in the current conversation. Instead of looking at law across the board, greater insight can be gleaned by looking at the specific demands of the different fields themselves. This does not mean that the goals identified will be exclusive to, for instance, national security law, but it does suggest there will be greater nuance in the discussion of the adequacy of the current pedagogical approach. With this approach in mind, I have here suggested six pedagogical goals for national security. For following graduation, students must be able to perform in each of the areas identified – (1) understanding the law as applied, (2) dealing with factual chaos and uncertainty, (3) obtaining critical distance, (4) developing nontraditional written and oral communication skills, (5) exhibiting leadership, integrity, and good judgment in a high-stakes, highly-charged environment, and (6) creating continued opportunities for self-learning. They also must learn how to integrate these different skills into one experience, to ensure that they will be most effective when they enter the field. The problem with the current structures in legal education is that they fall short, in important ways, from helping students to meet these goals. Doctrinal courses may incorporate a range of experiential learning components, such as hypotheticals, doctrinal problems, single exercises, extended or continuing exercises, and tabletop exercises. These are important classroom devices. The amount of time required for each varies, as does the object of the exercise itself. But where they fall short is in providing a more holistic approach to national security law which will allow for the maximum conveyance of required skills. Total immersion simulations, which have not yet been addressed in the secondary literature for civilian education in national security law, may provide an important way forward. Such simulations also cure shortcomings in other areas of experiential education, such as clinics and moot court. It is in an effort to address these concerns that I developed the simulation model above. NSL Sim 2.0 certainly is not the only solution, but it does provide a starting point for moving forward. The approach draws on the strengths of doctrinal courses and embeds a total immersion simulation within a course. It makes use of technology and physical space to engage students in a multi-day exercise, in which they are given agency and responsibility for their decision making, resulting in a steep learning curve. While further adaptation of this model is undoubtedly necessary, it suggests one potential direction for the years to come.

**Cyber threats are real – they facilitate dangerous armed social movements**

**Deibert and Rohozinski 2010**

(Ronald J, professor of Political Science and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto, and Rafal, Canadian expert and practitioner active in the fields of information security, cyber warfare, and the globalization of armed violence at the University of Toronto, 2010, International Studies Association, “Risking Security: Policies and Paradoxes of Cyberspace Security,” International Political Sociology, vol. 4, p. 22, BS)

Even among democratic states, **the explosion of civic networks has presented serious challenges**, though of a slightly different nature. **Just as progressive and social justice groups have made use of the Internet to advance global norms, so too have a wide variety of militant groups, extremists, criminal organizations, and terrorists to serve more ulterior purposes. Cyberspace has facilitated their activities** in much the same way as it has for more benign civil society networks that often get more attention, but **the aims of these groups are often criminal, covert, and sometimes violent. We call these risks through the network dark nets**, of which there are two different sorts (Deibert and Rohozinski 2008). **The most well known of the dark nets are armed social movements, which can represent a multiplicity of local causes, but whose ability to share tactics, contacts, and at times, drink from the same ideological well, make them appear as a uniﬁed global network. In the post-9/11 era, Al Qaeda and the Jihad movements represent the most visible manifestation of this kind of armed social movement. However, they are by no means the ﬁrst and only networks of this kind.** Many of the ‘‘new wars’’ (as Mary Kaldor calls them) that occurred during the 1990s were fought essentially as transnational civil wars where participants pursued both guerilla and conventional warfare against government and rival groups (Kaldor 1999). **In conﬂicts that included Sri Lanka, Somalia, former Yugoslavia, West Africa and Chechnya, ‘‘new wars’’ demonstrated that armed social movements are capable of challenging and at times defeating state actors without the need of state-based patrons or backers. More importantly, this new generation of armed social actors has also increasingly embraced cyberspace** (Rohozinski 2004). **They recognize the capacity afforded by cyberspace to ‘‘effect’’ both their supporters and opponents**. Signiﬁcantly, it was these groups, rather than militaries of the First World War, that were the ﬁrst to leverage cyberspace as means to wage information operations redeﬁning the main battleﬁeld away from the military and towards the political sphere (Weimann 2006b). **Beginning with the ﬁrst Chechen war, the video taping of attacks on the Russian military became more important than the military signiﬁcance of the attacks themselves.** When shown to supporters, as well as the Russian public (via rebroadcast in Russian television, and later on the Internet) their shock value was enough to convey the impression that the Russian military was being defeated. Similar tactics were adopted and further reﬁned by Hezbollah in its resistance against Israeli occupation of Southern Lebanon prior to their withdrawal in 2001, and again in the 2006 summer war. Attacks were documented and produced in the form of music videos, that were both broadcast across Hezbollah’s terrestrial TV station, (al Manar) as well as made available for download from a website, the movement established as part of its strategic communications and information warfare strategy (Pahlavi 2007; Wehrey 2002). **These video shorts proved highly effective**, and have since undergone several signiﬁcant evolutions, paralleling the spread and popularity of such on-line resources as YouTube and Twitter that are used by ‘‘civil’’ networks. **They are now one of the key instruments used by these movements to attract interest in their causes and are a signiﬁcant feature of the more than 4,500+ active jihad websites, chat rooms, and forums** (Weimann 2006a; Kimmage 2008). As the resources necessary for producing multimedia technologies continue to fall, and access to inexpensive digital cameras and computers increases, the threshold and number of video and other multimedia products in circulation has grown exponentially, while the age of the producers has declined. During the early months of the second Intifada, for example, several of the more compelling PowerPoint slides circulating on the Internet depicting the brutality of the Israeli reoccupation of the West bank were produced by a 14-year-old living in a refugee camp in Lebanon.

 **Cyber threats are real – cyberspace is organized transnationally, not governed centrally, constantly changes, and is difficult to regulate**

**Deibert and Rohozinski 2010**

(Ronald J, professor of Political Science and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto, and Rafal, Canadian expert and practitioner active in the fields of information security, cyber warfare, and the globalization of armed violence at the University of Toronto, 2010, International Studies Association, “Risking Security: Policies and Paradoxes of Cyberspace Security,” International Political Sociology, vol. 4, p. 15-16, BS)

Globalization is generating new security challenges. Modern societies confront a myriad of risks that threaten economic prosperity, undermine the safety and security of citizens, and cause signiﬁcant disruption to society and politics. These risks range from empowered and militant nonstate actors to technological and human-made processes, such as environmental degradation and global warming. **Risk mitigation has become a routine matter of good public policy. Cyberspace represents a special category of risk.**1 A term once found only in science ﬁction novels, cyberspace describes the human-made domain for action that exists as a consequence of an interconnected and interdependent global communications and computing infrastructure. **Cyberspace connects more than half of all humanity and is an indispensable component of political, social, economic, and military power worldwide. In strategic terms, cyberspace is accepted now as a domain equal to land, air, sea, and space. Predictably, in the post-9/11 era, cyberspace is the focus of security concerns as states weigh the risks and beneﬁts of omnipresent global connectivity. However, cyberspace presents special security challenges, for a variety of reasons. First, and most importantly, it is a communication network that is organized transnationally and not through the institutional structures of the state system. Although states and individuals may claim sovereignty or ownership over segments of cyberspace, particularly parts of its material infrastructure, or even opt out of it entirely, once in they are never fully in control. Cyberspace has emergent properties, in other words, that elude state control. Second, and closely related, cyberspace is operated as a mix of public and private networks. Governance of cyberspace, like its architecture, is distributed, and does not take place within a singular forum or point of control** (Dutton and Peltu 2007). Even the Internet Corporation for Assigned Names and Numbers (ICANN), that is most often associated with Internet governance issues, is only narrowly concerned with domain and routing management and not with the full panoply of cyberspace governance issues (Mueller 2002). **There are instead numerous sites of cyberspace governance, from spectrum allocation to copyright and intellectual property regulation to content ﬁltering and cyber-crime (among many others). Each of these sites involves numerous stakeholders, including governments, businesses, and civil society networks. In addition, private sector actors from multiple countries operate most of the core infrastructural components of cyberspace.** What James Der Derian (2003) calls ‘‘heteropolarity’’ perhaps best characterizes the state of cyberspace governance. **Third, unlike other domains, such as the sea, land, air, or space, cyberspace is a human-made domain in constant ﬂux based on the ingenuity and participation of users /////themselves. One of the core design features of cyberspace is the end-to-end principle, which allows for generative technologies to be introduced into cyberspace by end users as long as they conform to the basic protocols of interconnectivity** (Saltzer, Reed, and Clark 1984). **The latter introduces not only great variation and constant innovation, but also new and unforeseen security risks** (Zittrain 2007). **It also creates major problems for regulation, insofar as regulators are always chasing a moving target. In other words, cyberspace is a domain of constant transformation and a high degree of complexity. Fourth, cyberspace is comprised of both a material and a virtual realm—a space of things and ideas, structure and content.** Theorists and observers of cyberspace often focus on one of these elements to the exclusion or diminution of the other, but both are important and interdependent. Cyberspace is indeed a ‘‘consensual hallucination’’ as Gibson (1984) famously deﬁned it, but one that could not exist without the physical infrastructure that supports it. **Attempts to control and monitor the virtual realm of cyberspace often begin with interventions in the physical infrastructure, at key Internet chokepoints** (Deibert, Palfrey, Rohozinski, and Zittrain 2008). **However, these efforts are never entirely comprehensive; once released into cyberspace, the distributed properties of the network help ideas and information circulate, duplicate and proliferate. Even radical measures, such as disconnecting the Internet entirely as was done recently in Burma and Nepal, can only limit, but not entirely contain the ﬂow of ideas.**

# 2AC

### Case

**Masking Disad—discursive criticism masks the problem and prevents legitimate solutions.**

**Meisner 95**

(Mark, professor of environmental studies at York University, (Mark, “Resourcist Language: The Symbolic Enslavement of Nature”, Proceedings of the Conference on Communication and Our Environment, ed: David Sachsman, p. 242)

**Changing the language we use** to talk **about** non-human nature **is not a solution**. As I suggested, **language is not the problem**. Rather, **it s**eems **more like a contagious symptom of a deeper and multi-faceted problem that has yet to be fully defined**. Resourcist language is both an indicator and a carrier of the pathology of rampant ecological degradation. Further¬more, **language change alone can end up simply being a band-aid solution that gives the appearance of change and makes the problem all the less visible**. In a recent article on feminist language reform, Susan Ehrlich and Ruth King (1994) argue that because meanings are socially constructed, attempts at introducing nonsexist language are being undermined by a culture that is still largely sexist. The **words may have shifted, but the meanings and ideologies have not. The real world cure for the sick patient matters more than the treatment of a single symptom**. Consequently, **language change and cultural change must go together with social-moral change**. It is naive to believe either that language is trivial, or that it is deterministic.

#### 1. The “cyber” prefix is superior to alternatives- it is the best method of bridging information and governance

Arquilla and Ronfeldt ‘97

[John Arquilla earned his degrees in international relations from Rosary College (BA 1975) and Stanford University (MA 1989, PhD 1991). He has been teaching in the special operations program at the United States Naval Postgraduate School since 1993. He also serves as chairman of the Defense Analysis department. David Ronfeldt, adjunct research staff at RAND. In Athena’s Camp: Preparing for Conflict in the Information Age, RAND/MR-880-OSD/RC (1997). ETB]

Terms with “cyber-” as the prefix—e.g., cyberspace—are currently in vogue among¶ some visionaries and technologists who are seeking names for new concepts related to¶ the information revolution. The prefix is from the Greek root kybernan, meaning to¶ steer or govern, and a related word kybernetes, meaning pilot, governor, or helmsman.¶ The prefix was introduced by Norbert Wiener in the 1940s in his classic works creating¶ the field of “cybernetics” (which is related to cybernétique, an older French word¶ meaning the art of government). Some readers may object to our additions to the lexicon, but we prefer them to alternative terms like “information warfare,” which has¶ been used in some circles to refer to warfare that focuses on C3¶ I capabilities. In our¶ view, a case exists for using the prefix in that it bridges the fields of information and¶ governance better than does any other available prefix or term. Indeed, kybernan, the root of “cyber-,” is also the root of the word “govern” and its extensions. Perhaps rendering the term in German would help. A likely term would be Leitenkrieg, which¶ translates loosely as “control warfare” (our thanks to Denise Quigley for suggesting¶ this term).

**AND PAN HIMSELF ADMITS THAT CHINA THREAT CONSTRUCTION IS INEVITABLE AND REFLEXIVELY BASED ON CHINESE STATE BEHAVIOUR.**

Moran 2k11

[lee, pride of the fleet: china’ first aircraft carrier…”, <http://www.dailymail.co.uk/news/article-2024425/Chinas-aircraft-carrier-takes-seas--fuelling-fears-countrys-military-strength.html>]

The official state **Xinhua news agency** **added**: 'Building a strong navy that is commensurate with **China's rising status is a necessary step and an inevitable choice for the country** to safeguard its increasingly globalised national interests.'¶ But **Chengxin** Pan**, an expert on China at Deakin University in Australia,** warned it could unsettle neighbouring countries.¶ He said: 'For many neighbours, it may symbolise something different and more unsettling.¶ **'It is inevitable that neighbouring** countries will react with some alarm**, especially given recent disputes in the South China Sea** as well as the maritime incident between China and Japan last year.'¶ Refitting and test work will now continue on the carrier.¶ The Varyag, yet to be officially renamed, was towed from Ukraine in 2001 as an empty shell without engines, weapons systems or other crucial equipment.¶ Ashley Townshend, at the Lowy Institute for International Policy in Sydney, said China would need at least three carriers if it was 'serious' about having a viable carrier strike group.¶ He also said that it would have to develop support ships and aircraft for any carrier group, which could take ten years.¶ China's neighbours India and Thailand already have aircraft carriers, and Australia has ordered two multi-purpose carriers. The United States operates 11.¶ The former chief of the Philippine's navy Admiral Ferdinand Golez said his country should not be worried by the development. He said: 'The Philippines should not be concerned with this development.¶ 'An aircraft carrier is an offensive tool but I don't think China has the intention to use it to bully its neighbours.'¶ Before the launch, a Pentagon spokesman played down the likelihood of any immediate leaps from China's carrier programme. ¶ But that is just one part of China's naval modernisation drive, which has forged ahead while other powers tighten their military budgets to cope with debt woes. ¶ China has been building new submarines, surface ships and anti-ship ballistic missiles as part of its naval modernisation, which has triggered regional jitters that have fed into long-standing territorial disputes, and could speed up military expansion across Asia.¶ In the past year, China has had run-ins at sea with Japan, Vietnam and the Philippines. The incidents - boat crashes and charges of territorial incursions - have been minor, but the diplomatic reaction often heated. ¶ Chengxin **Pan added: 'Overall, the perception of a rapidly rising and potentially threatening China is likely to be reinforced and** Beijing will face enormous challenges in dispelling such a perception.'

### 2AC Cap

#### 2. Cap isn’t the root cause of anything; greed is – shift away turns the alt.

Aberdeen 3 (Richard, Political Activist, Philosopher, Hippie, He Doesn’t Link to Your Epistemology Arguments, “The Way: A Theory of Root Cause and Solution,” http://freedomtracks.com/uncommonsense/theway.html)

A view shared by many modern activists is that capitalism, free enterprise, multi-national corporations and globalization are the primary cause of the current global Human Rights problem and that by striving to change or eliminate these, the root problem of what ills the modern world is being addressed. This is a rather unfortunate and historically myopic view, reminiscent of early “class struggle” Marxists who soon resorted to violence as a means to achieve rather questionable ends. And like these often brutal early Marxists, modern anarchists who resort to violence to solve the problem are walking upside down and backwards, adding to rather than correcting, both the immediate and long-term Human Rights problem. Violent revolution, including our own American revolution, becomes a breeding ground for poverty, disease, starvation and often mass oppression leading to future violence. Large, publicly traded corporations are created by individuals or groups of individuals, operated by individuals and made up of individual and/or group investors. These business enterprises are deliberately structured to be empowered by individual (or group) investor greed. For example, a theorized ‘need’ for offering salaries much higher than is necessary to secure competent leadership (often resulting in corrupt and entirely incompetent leadership), lowering wages more than is fair and equitable and scaling back of often hard fought for benefits, is sold to stockholders as being in the best interest of the bottom-line market value and thus, in the best economic interests of individual investors. Likewise, major political and corporate exploitation of third-world nations is rooted in the individual and joint greed of corporate investors and others who stand to profit from such exploitation. More than just investor greed, corporations are driven by the greed of all those involved, including individuals outside the enterprise itself who profit indirectly from it. If one examines “the course of human events” closely, it can correctly be surmised that the “root” cause of humanity’s problems comes from individual human greed and similar negative individual motivation. The Marx/Engles view of history being a “class” struggle ¹ does not address the root problem and is thus fundamentally flawed from a true historical perspective (see Gallo Brothers for more details). So-called “classes” of people, unions, corporations and political groups are made up of individuals who support the particular group or organizational position based on their own individual needs, greed and desires and thus, an apparent “class struggle” in reality, is an extension of individual motivation. Likewise, nations engage in wars of aggression, not because capitalism or classes of society are at root cause, but because individual members of a society are individually convinced that it is in their own economic survival best interest. War, poverty, starvation and lack of Human and Civil Rights have existed on our planet since long before the rise of modern capitalism, free enterprise and multi-national corporation avarice, thus the root problem obviously goes deeper than this.

#### 3. Perm: do the plan and the alternative in every other instance. - Representations of capitalism as hegemonically dominant preclude the realization of actual social change. Changing this view is a pre-requisite to the alt.

**Gibson-Graham 06** – J.K., pen name shared by feminist economic geographers Julie Graham and Katherine Gibson (“The End of Capitalism (As We Knew It): A Feminist Critique of Political Economy”, pg 2-5)

The End of Capitalism (As We Knew It) problematizes "capitalism" as an economic and social descriptor.4 Scrutinizing what might be seen as throwaway uses of the term - passing references, for example, to the capitalist system or to global capitalism - as well as systematic and deliberate attempts to represent capitalism as a central and organizing feature of modern social experience, the book selectively traces the discursive origins of a widespread understanding: that capitalism is the hegemonic, or even the only, present form of economy and that it will continue to be so in the proximate future. It follows from this prevalent though not ubiquitous view that noncapitalist economic sites, if they exist at all, must inhabit the social margins; and, as a corollary, that deliberate attempts to develop noncapitalist economic practices and institutions must take place in the social interstices, in the realm of experiment, or in a visionary space of revolutionary social replacement. Representations of capitalism are a potent constituent of the anticapitalist imagination, providing images of what is to be resisted and changed as well as intimations of the strategies, techniques, and possibilities of changing it. For this reason, depictions of "capitalist hegemony" deserve a particularly skeptical reading. For in the vicinity of these representations, the very idea of a noncapitalist economy takes the shape of an unlikelihood or even an impossibility. It becomes difficult to entertain a vision of the prevalence and vitality of noncapitalist economic forms, or of daily or partial replacements of capitalism by noncapitalist economic practices, or of capitalist retreats and reversals. In this sense, "capitalist hegemony" operates not only as a constituent of, but also as a brake upon, the anticapitalist imagination.5 What difference might it make to release that brake and allow an anticapitalist economic imaginary to develop unrestricted?6 If we were to dissolve the image that looms in the economic foreground, what shadowy economic forms might come forward? In these questions we can identify the broad outlines of our project: to discover or create a world of economic difference, and to populate that world with exotic creatures that become, upon inspection, quite local and familiar (not to mention familiar beings that are not what they seem). The discursive artifact we call "capitalist hegemony" is a complex effect of a wide variety of discursive and nondiscursive conditions.7 In this book we focus on the practices and preoccupations of discourse, tracing some of the different, even incompatible, representations of capitalism that can be collated within this fictive summary representati n. These depictions have their origins in the diverse traditions of Marxism, classical and contemporary political economy, academic social science, modern historiography, popular economic and social thought, western philosophy and metaphysics, indeed, in an endless array of texts, traditions and infrastructures of meaning. In the chapters that follow, only a few of these are examined for the ways in which they have sustained a vision of capitalism as the dominant form of economy, or have contributed to the possibility or durability of such a vision. But the point should emerge none the less clearly: the virtually unquestioned dominance of capitalism can be seen as a complex product of a variety of discursive commitments, including but not limited to organicist social conceptions, heroic historical narratives, evolutionary scenarios of social development, and essentialist, phallocentric, or binary patterns of thinking. It is through these discursive figurings and alignments that capitalism is constituted as large, powerful, persistent, active, expansive, progressive, dynamic, transformative; embracing, penetrating, disciplining, colonizing, constraining; systemic, self-reproducing, rational, lawful, self-rectifying; organized and organizing, centered and centering; originating, creative, protean; victorious and ascendant; selfidentical, self-expressive, full, definite, real, positive, and capable of conferring identity and meaning.8 The argument revisited: it is the way capitalism has been "thought" that has made it so difficult for people to imagine its supersession.9 It is therefore the ways in which capitalism is known that we wish to delegitimize and displace. The process is one of unearthing, of bringing to light images and habits of understanding that constitute "hegemonic capitalism" at the intersection of a set of representations. This we see as a first step toward theorizing capitalism without representing dominance as a natural and inevitable feature of its being. At the same time, we hope to foster conditions under which the economy might become less subject to definitional closure. If it were possible to inhabit a heterogeneous and open-ended economic space whose identity was not fixed or singular (the space potentially to be vacated by a capitalism that is necessarily and naturally hegemonic) then a vision of noncapitalist economic practices as existing and widespread might be able to be born; and in the context of such a vision, a new anticapitalist politics might emerge, a noncapitalist politics of class (whatever that may mean) might take root and flourish. A long shot perhaps but one worth pursuing.

#### The sort of capitalism they critique is a neoliberal form rooted in the aggressive drive to attack the other. This is the status quo, where rather than establish robust computer systems, we use offensive cyber operations to attack the other before they can attack us. The alternative is a shift from this combative, monopolistic form of capitalism to a more cooperative system.

**Gjelten, 13**

(Tom, correspondent for NPR, "First Strike: US Cyber Warriors Seize the Offensive", Jan/Feb, [www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive](http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive) NL)

In addition, **there are policy questions raised by the escalating government investment in offensive cyber war capabilities.** One fear is that **each new offensive cyberweapon introduced into use will prompt the development of an even more lethal weapon by an adversary and trigger a fierce cyber arms race. A hint of such an escalatory cycle may be seen in the confrontation with Iran over its nuclear program.** US officials suspect the Iranian government was responsible for the recent wave of cyber attacks directed against Aramco, the Saudi oil company, and may also have been behind a series of denial-of-service attacks on US financial institutions. **Such attacks could be in retaliation for the Stuxnet worm.**¶ Some writers foresee a dangerous new world, created by the United States and Israel with the deployment of Stuxnet. Misha Glenny, writing in the Financial Times, argued that the tacit US admission of responsibility for Stuxnet will act “as a starting gun; countries around the world can now argue that it is legitimate to use malware pre-emptively against their enemies.” One danger is that US adversaries, notably including Russia and China, may now cite the use of Stuxnet to support their argument that an international treaty regulating the use of cyberweapons may be needed. The United States has long opposed such a treaty on the grounds that it would undermine its own technological advantages in cyberspace and could also lead to efforts to regulate the Internet in ways that would harm freedom of expression and information.

**Overconcentration on offense is destabilizing- makes cyberwar inevitable**

**McGraw 13** <[Gary McGraw](http://www.tandfonline.com/action/doSearch?action=runSearch&type=advanced&searchType=journal&result=true&prevSearch=%2Bauthorsfield%3A(McGraw%2C+G)), PhD is Chief Technology Ofﬁcer of Cigital, and author of¶ Software Security (AWL 2006) along with ten other software security¶ books. He also produces the monthly Silver Bullet Security Podcast for¶ IEEE Security & Privacy Magazine (syndicated by SearchSecurity), Cyber War is Inevitable (Unless We Build Security In), Journal of Strategic Studies - Volume 36, Issue 1, 2013, pages 109-119, <http://www.tandfonline.com.proxy.library.cornell.edu/doi/pdf/10.1080/01402390.2012.742013>>#**SPS**

**Also of note is the balancing effect that extreme cyber vulnerability**¶ **has on power when it comes to cyber war.** In the case of the Stuxnet¶ attack, the balance of power was clearly stacked high against Iran.¶ Subsequently, however, Iran responded with the (alleged) hijacking of a¶ US drone being used for surveillance in Iranian airspace.10 **Ironically, it**¶ **may be that the most highly developed countries are more vulnerable to**¶ **cyber warfare because they are more dependent on modern high-tech**¶ **systems.** **In any case, failure to build security into the modern systems**¶ **we depend on can backlash, lowering the already low barrier to entry**¶ **for geopolitically motivated cyber conﬂict.** **Defending against cyber**¶ **attack (by building security in) is just as important as developing**¶ **offensive measures. Indeed it is more so.**¶ War has both defensive and offensive aspects, and understanding this¶ is central to understanding cyber war. **Over-concentrating on offense¶ can be very dangerous and destabilizing because it encourages actors to¶ attack ﬁrst and ferociously, before an adversary can.** **Conversely, when¶ defenses are equal or even superior to offensive forces, actors have less¶ incentive to strike ﬁrst because the expected advantages of doing so are¶ far lower.** **The United States is supposedly very good at cyber offense**¶ **today, but from a cyber defense perspective it lives in the same glass**¶ **houses as everyone else.** The root of the problem is that the systems we¶ depend on – the lifeblood of the modern world – are not built to be¶ secure.11¶ This notion of offense and defense in cyber security is worth teasing¶ out. Offense involves exploiting systems, penetrating systems with¶ cyber attacks and generally leveraging broken software to compromise¶ entire systems and systems of systems.12 Conversely, defense means¶ building secure software, designing and engineering systems to be¶ secure in the ﬁrst place, and creating incentives and rewards for systems¶ that are built to be secure.13 What sometimes passes for cyber defense¶ today – actively watching for intrusions, blocking attacks with network¶ technologies such as ﬁrewalls, law enforcement activities, and protecting against malicious software with anti-virus technology – is little more than a cardboard shield.14 **If we do not focus more attention on**¶ **real cyber defense by building security in, cyber war will be inevitable.**¶

#### 4. The desire for freedom and growth is innate – moving away risks totalitarianism, violence, poverty and war

Aligica ‘3 (Paul Aligica, Fellow at the Mercatus Center at George Mason University and Adjunct Fellow at the Hudson Institute, “The Great Transition and the Social Limits to Growth: Herman Kahn on Social Change and Global Economic Development”, April 21, http://www.hudson.org/index.cfm?fuseaction=publication\_details&id=2827)

Stopping things would mean if not to engage in an experiment to change the human nature, at least in an equally difficult experiment in altering powerful cultural forces: "We firmly believe that despite the arguments put forward by people who would like to 'stop the earth and get off,' it is simply impractical to do so. Propensity to change may not be inherent in human nature, but it is firmly embedded in most contemporary cultures. People have almost everywhere become curious, future oriented, and dissatisfied with their conditions. They want more material goods and covet higher status and greater control of nature. Despite much propaganda to the contrary, they believe in progress and future" (Kahn, 1976, 164). As regarding the critics of growth that stressed the issue of the gap between rich and poor countries and the issue of redistribution, Kahn noted that what most people everywhere want was visible, rapid improvement in their economic status and living standards, and not a closing of the gap (Kahn, 1976, 165). The people from poor countries have as a basic goal the transition from poor to middle class. The other implications of social change are secondary for them. Thus a crucial factor to be taken into account is that while the zero-growth advocates and their followers may be satisfied to stop at the present point, most others are not. Any serious attempt to frustrate these expectations or desires of that majority is likely to fail and/or create disastrous counter reactions. Kahn was convinced that "any concerted attempt to stop or even slow 'progress' appreciably (that is, to be satisfied with the moment) is catastrophe-prone". At the minimum, "it would probably require the creation of extraordinarily repressive governments or movements-and probably a repressive international system" (Kahn, 1976, 165; 1979, 140-153). The pressures of overpopulation, national security challenges and poverty as well as the revolution of rising expectations could be solved only in a continuing growth environment. Kahn rejected the idea that continuous growth would generate political repression and absolute poverty. On the contrary, it is the limits-to-growth position "which creates low morale, destroys assurance, undermines the legitimacy of governments everywhere, erodes personal and group commitment to constructive activities and encourages obstructiveness to reasonable policies and hopes". Hence this position "increases enormously the costs of creating the resources needed for expansion, makes more likely misleading debate and misformulation of the issues, and make less likely constructive and creative lives". Ultimately "it is precisely this position the one that increases the potential for the kinds of disasters which most at its advocates are trying to avoid" (Kahn, 1976, 210; 1984).

### 2AC: Abelist Language

#### The introduction of their critique of ableist language is a voting issue—calling us out for using an *unintentionally offensive term* might make them feel better for embarrassing us, but it doesn’t do anything to address ableist oppression and prevents constructive activism. Rejecting their “call out” strategy is crucial to constructive activism—vote against them to facilitate productive dialogue about ableist language.

Kinzel 11

Lesley Kinzel, blogger and social justice writer, has written for Newsweek and Marie Claire, was named one of the Feminist Press’s “40 Feminists Under 40,” 2011 (“On our difficult language, and the calling-out of,” Two Whole Cakes—a blog about body politics, social justice activism, and pop-cultural criticism from a feminist perspective, March 30th, Available Online at <http://blog.twowholecakes.com/2011/03/on-our-difficult-language-and-the-calling-out-of-same>)

We throw “that’s ableist” or “that’s racist” or “that’s fatphobic” around, I suspect, in the hope that such heavy judgement-bearing words will shock and embarrass the speaker out of using the offending language. And sometimes, it can work, at least in the short term, when we are merely thinking of our own self-preservation. But beyond that instant, this is not constructive activism. Using surprise, guilt, or humiliation as negative reinforcement to change behavior does nothing to instruct the person in question on why their behavior is causing problems; they stop simply because they don’t want to get in trouble. While the power shift this approach employs may feel awfully satisfying to those of us who have labored under some degree of oppression for much our lives—we get to dictate the terms of engagement, for once—merely shifting the power from one hand to another does nothing to change the destructive use of said power against us.¶ This practice of shaming people into behaving a certain way or using certain language does not truly address the underlying inclination; it does not unpack the thinking that allowed that speaker to feel entitled to say those things in the first place. Fear can be an effective motivator, but it’s not often a productive one, if our goal is broad and lasting cultural change. It is, after all, fear that motivates folks of all sizes to diet, that keeps queer folks in the closet, that makes women afraid to walk alone at night, that compels people of color to keep their heads down even in the face of overt discrimination and just get by. It is fear and shame that locks the systems that marginalize us in place, and as Audre Lorde has explained, in one of the most brilliant pieces of writing on social justice ever put to paper, there is little we can do while still holding on to the master’s tools.¶ Those of us who stand outside the circle of this society’s definition of acceptable women; those of us who have been forged in the crucibles of difference — those of us who are poor, who are lesbians, who are Black, who are older — know that survival is not an academic skill. It is learning how to stand alone, unpopular and sometimes reviled, and how to make common cause with those others identified as outside the structures in order to define and seek a world in which we can all flourish. It is learning how to take our differences and make them strengths. For the master’s tools will never dismantle the master’s house. They may allow us temporarily to beat him at his own game, but they will never enable us to bring about genuine change. And this fact is only threatening to those women who still define the master’s house as their only source of support.¶ Ideally, people should stop using certain language because they have developed an understanding of why that language is oppressive, and how their use of it contributes to inequality and marginalization, and not because they are afraid or ashamed of confusing social repercussions they do not understand. What we need is a commitment to giving people clear explanations—be they angry, or impassioned, or blunt—of why their words or behavior are problematic, or upsetting, or damaging. We need to resist relying on comfortable jargon to call people out, and to ditch the erroneous presumption that making someone feel stupid will encourage them to read more about a subject. It doesn’t work. Fear and shame don’t help people to understand how the language we use and the actions we undertake, even in our own small individual spheres, all conspire to create a social environment that oppresses us. Fear breeds resentment and, sometimes, hatred. These are not things we need more of. These are the things that put us here in the first place.

### 2AC Anthro

#### 1. FRAMEWORK—The aff is a normative statement. Vote aff if plan is a good idea, neg if it isn’t.

A. Solves their offense –the impact of the K is a reason the aff is bad.

B. Aff choice – they arbitrarily steal 9 minutes of offense, destroys the aff’s only advantage.

c. Vague alts are a voting issue – skews 2AC offense and creates a form of sandbagging which unfairly privileges the time benefits of the block

#### 2. There is no coherent link to this argument – the impact claims of the 1AC are against nuclear war. Two arguments

A. Their link argument is survivalism, survival is not a 1AC argument, we just think that mass death is bad

B. Nuclear war would kill other species as well, the fact that we didn’t say humans in the 1AC means the link of omission makes no sense

#### 3. Reject systematic or all-encompassing “root cause” claims for human action

Bleiker, 3 (Roland, 2003, “Discourse and Human Agency,” Contemporary Political Theory, No. 2, Professor at School of Political Science, University of Queensland, pg. 25, JPL)

A conceptualization of human agency cannot be based on a parsimonious proposition, a one-sentence statement that captures something like an authentic nature of human agency. There is no essence to human agency, no core that can be brought down to a lowest common denominator, that will crystallize one day in a long sought after magic formula. A search for such an elusive centre would freeze a specific image of human agency to the detriment of all others. The dangers of such a totalizing position have been well rehearsed. Foucault (1982, 209), for instance, believes that a theory of power is unable to provide the basis for analytical work, for it assumes a prior objectification of the very power dynamics the theory is trying to assess. Bourdieu (1998, 25) speaks of the ‘imperialism of the universal’ and List (1993, 11) warns us of an approach that ‘subsumes, or, rather, pretends to be able to subsume everything into one concept, one theory, one position.’ Such a master discourse, she claims, inevitably oppresses everything that does not fit into its particular view of the world. What, then, is the alternative to anchoring an understanding of human agency in a foundationalist master narrative? How to ground critique, actions, norms and life itself if there are no universal values that can enable such a process of grounding? Various authors have advanced convincing suggestions. Consider the following three examples: (1) de Certeau (1990, 51) attempts to avoid totalitarian thought by grounding his position not in a systematic theory, but in ‘operational schemes.’ A theory is a method of delineation. It freezes what should be understood in its fluidity. An understanding of operational schemes, by contrast, recognizes that events should be assessed in their changing dimensions. Rather than trying to determine what an event is, such an approach maps the contours within which events are incessantly constituted and reconstituted. Or, expressed in de Certeau’s terminology, one must comprehend forms of action in the context of their regulatory environment. (2) Butler (1992, 3–7) speaks of contingent foundations. Like de Certeau, she too believes that the Foucaultean recognition that power pervades all aspects of society, including the position of the critic, does not necessarily lead into a nihilistic abyss. It merely shows that political closure occurs through attempts to establish foundational norms that lie beyond power. Likewise, to reopen this political domain is not to do away with foundations as such, but to acknowledge their contingent character, to illuminate what they authorize, exclude and foreclose. One must come to terms with how the subject and its agency are constituted and framed by specific regimes of power. However, this is not the end of human agency. Quite to the contrary. Butler (1992, 12–14) argues persuasively that ‘the constituted character of the subject is the very precondition of its agency.’ To appreciate the practical relevance of this claim, one must investigate the possibilities for agency that arise out of existing webs of power and discourse. One must scrutinize how social change can be brought about by a reworking of the power regimes that constitute our subjectivity (Butler, 1992, 13). (3) Deleuze and Guattari (1996, 3–25, 377) go a step further. Opting for the rhizome, they reject all forms of foundations, structures, roots or trees. The latter three, they say, has dominated much of the Western thought. A tree is a hierarchical system in which ones becomes two, in which everything can be traced back to the same origin. Roots and radicles may shatter the linear unity of knowledge, but they hold on to a contrived system of thought, to an image of the world in which the multiple always goes back to a centred and higher unity. The brain, by contrast, is not rooted, does not strive for a central point. It functions like a subterranean rhizome. It grows sideways, has multiple entryways and exits. It has no beginning or end, only a middle, from where it expands and overspills. Any point of the rhizome, Deleuze and Guattari emphasize, is connected to any other. It is a multiplicity without hierarchies, units or fix points to anchor thought. There are only lines, magnitudes, dimensions, plateaus, and they are always in motion. To travel along these lines and dimensions is to engage in nomad thought, to travel along axis of difference, rather than identity. Nomad thought, says one of Deleuze’s feminist interpreters, ‘combines coherence with mobility,’ it is ‘a creative sort of becoming, a performative metaphor that allows for otherwise unlikely encounters and unsuspected sources of interaction of experience and of knowledge’ (Braidotti, 1994, 21). The extent to which this form of thinking constitutes a grounding process may be left open to question. Judging from Deleuze’s own work it is clear, however, that the exploration of difference and multiplicities does not prevent him from taking positions for or against specific political issues. What he does forgo, however, is a central authorial voice F to the benefit of a polyphonic array of whispers and shouts.

#### 4. Perm– Do both. At best their link is one of omission, the permutation resolves it

#### 5. The critique is anthropocentric – it assumes knowledge for nature

Bobertz 97 Bobertz Ass’t Prof of Law, Nebraska College of Law, 1997, Bradley Columbia Journal of Environmental Law,Lexis

 Apart from the political dangers Ferry associates with deep ecology, he believes the philosophy suffers from a fundamental self-contradiction. The argument that natural objects can possess their own interests strikes Ferry as "one of the mostabsurd forms of anthropomorphism." n100 We cannot "think like a mountain," to use Aldo Leopold's famous phrase, n101 because, quite obviously, we are not mountains. Recalling Sierra Club v. Morton, n102 the famous standing case involving a proposal to construct a ski resort in California's Mineral King valley, Ferry claims that environmentalists "always suppose that the interests of objects (mountains, lakes and other natural things) are opposed to development. But how do we know? After all, isn't it possible that Mineral King would be inclined to welcome a ski slope after having remained idlefor millions of years?" n103 Yet few people, including the writers Ferry labels as deep ecologists, would disagree with the fact that recognizing value in natural objects is an act of human cognition. Perhaps a person suffering from profound psychosis might claim the ability to understand how a mountain "thinks," but the writers Ferry criticizes do not advance such bizarre claims. n104 For deep ecologists and environmental ethicists, phrases such as "think like a mountain" are metaphorical and heuristic, not literal and agenda-setting.

#### 6. Their impact claims are anthropocentric – belief that humans can cause such harm replicates the problem

Fox, 5 (Russel, 11/22/5, “The Real Anthropocentrism,” In Medias Res, Ph.D, Assistant Professor of Political Science Division of Social and Behavioral Sciences Friends University, JPL)

In the end, I think the attempt to purge the human, to reduce the everyday productive place of actual human beings from one's picture of the natural world (an attempt that can lead ultimately to rather bizarre conclusions), rests on a perverse kind of anthropocentrism. Isn't anthropocentrism exactly what deep ecologists have long said is the root of our problem--the way in which our economies and societies assume that human beings are the center of creation? Yes. But isn't the belief that human beings are utterly and uniquely destructive of the natural world, that in our ordinary consumptive lives we cannot help but be a "foreign" presence on the earth, equally anthropocentric? In fact, it might be an even worse anthropocentrism: in the real world, farmers and gardeners and all those who care about the earth take seriously their stewardship of it, a stewardship which makes them, in my experience at least, humble and careful, aware of the fragility of their relationship with nature. Whereas radical environmentalism too often allows for no such complexity; there is humanity and there is nature, and the further the two are kept tightly separate from each other (close enough for the former to look at and "commune with" the latter, but nothing more), the better for both. For any who find themselves agreeing with this position, I strongly recommend 1491--a wonderful, provocative new book which argues that "pristine" New World which European explorers "discovered" and invaded in the from 15th to the 17th centuries, and which many today consider today to have been a kind of paradise lost, was to a great extent the creation of prolonged human interaction. The Amazon basin, the buffalo herds--all a result of generations of indigenous "species maintenance" and "land planning" (though tragic accidents played a part as well). Real environmentalists know that human technology and society, for better and for worse, are as much a part of the geography of the planet as the life patterns of any other species. Only a truly anthropocentric thinker would think that you can take humans--like either the Gwich'in or the Inupiat--out of the equation, and call what remains to be conserved truly "natural."

#### 7. Perm, do the plan and all non-mutually exclusive parts of the alt. We can recognize the need for environmentally sustainable practices without resorting to dangerous biocentrism

Hwang, 3 (Kyung-Sig, 2003, “Apology for Environmental Anthropocentrism,” Eubios Ethics Institute, Professor in Department of Philosophy at Seoul National University, JPL) \*Gender modified

While our ability to affect the future is immense, our ability to foresee the results of our environmental interventions is not. I think that our moral responsibility grows with foresight. And yet, paradoxically in some cases grave moral responsibility is entailed by the fact of one's ignorance. If the planetary life-support system appears to be complex and mysterious, humble ignorance should indicate respect and restraint. However, as many life scientists have complained, these virtues have not been apparent in these generations. Instead they point out, we have boldly marched ahead, shredding delicate ecosystems and obliterating countless species, and with them the unique genetic codes that evolved through millions of years; we have altered the climate and even the chemistry of the atmosphere, and as a result of all this-what?[18] A few results are immediately to our benefit; more energy, more mineral resources, more cropland, convenient waste disposal. Indeed, these short-term payoffs motivated us to alter our natural environment. But by far the larger and more significant results, the permanent results, are unknown and perhaps unknowable. Nature, says poet, Nancy Newhall, "holds answers to more questions than we know how to ask." And we have scarcely bothered to ask.[19] Year and year, the natural habitants diminish and the species disappear, and thus our planetary ecosystem (our household) is forever impoverished. It is awareness of ecological crisis that has led to the now common claim that we need transvaluation of value, new values, a new ethic, and an ethic that is essentially and not simply contingently new and ecological. Closer inspection usually reveals that the writer who states this does not really mean to advance such a radical thesis, that all they are arguing for is the application of old, recognized, ethical values of the kind noted under the characterization of respect for persons, justice, honesty, promotion of good, where pleasure and happiness are seen as goods. Thus, although W. T. Blackstone writes; "we do not need the kind of transvaluation that Nietzsche wanted, but we do need that for which ecologists are calling, that is, basic changes in man's attitude toward nature and man's place in nature, toward population growth, toward the use of technology, and toward the production and distribution of goods and services." We need to develop what I call the ecological attitude. The transvaluation of values, which is needed, will require fundamental changes in the social, legal, political and economic institutions that embody our values. He concludes his article by explicitly noting that he does not really demand a new ethic, or a transvaluation of values. A human being is a hierarchical system and a component of super-individual, hierarchical system of sets. What is needed is not the denial of anthropocentrism, the placing of the highest value on humans and their ends and the conceiving of the rest of the nature as an instrument for those ends. Rather what is needed is the explicit recognition of these hierarchical systems and an ecological approach to science and the accumulation of scientific knowledge in which the myriad casual relationships between different hierarchical systems are recognized and put to the use of humanity. The freedom to use the environment must be restricted to rational and human use. If there is irrational use - pollution, overpopulation, crowding, a growth in poverty, and so on - people may wipe out hierarchies of life related to their own survival and to the quality of their own lives. This sort of anthropocentrism is essential even to human survival and a radical biotic egalitarianism would undermine conditions for that survival.[20] Rational anthropocentrism, one that recognizes the value of human life "transcends our individual life" and one in which we form a collective bond of identity with the future generations is essential in the process of human evolution.

#### 8. Preventing human extinction is necessary in an eco-centric framework

Baum 9 – PhD @ Penn State University Sean Baum, PhD @ Penn State University, 2009, “Costebenefit analysis of space exploration: Some ethical considerations,” Space Policy, Vol. 25, Science Direct

It is of note that the priority of reducing the risk of human extinction persists in forms of CBA which value nature in an ecocentric fashion, ////i.e. independently of any consideration of human interests. The basic reason is that without humanity leading long-term survival efforts (which would most likely include space colonization), the rest of Earth life would perish as a result of the astronomical processes described above. This point is elaborated by futurist Bruce Tonn, who argues on ecocentric grounds for reorienting society to focus on avoiding human extinction through both immediate avoidance of catastrophe and long-term space colonization [40]. Tonn dubs this process of surviving beyond Earth’s eventual demise ‘‘transcending oblivion’’ [41]. There is thus some convergence in the recommendations of the common anthropocentric, money-based CBA and the ecocentric CBA described here. This convergence results from the fact that (in all likelihood) only humans are capable of colonizing space, and thus human survival is necessary for Earth life to transcend oblivion.

# 1AR

### Chaloupka

#### Chaloupka’s theory lacks definition and has no practical application

Brians 92 (Paul, Prof Department of ENglish WSU, http://www.wsu.edu/~brians/ntc/NTC8.pdf, AD: 7/1/10) jl

The confusion underlying this apparent tangle has two closely related sources: Chaloupka plunges in, dismisses careful initial conceptualization, and defines by accretion. Of course this book’s audience is scholarly, but I do not believe anyone can say what Chaloupka means by “modernism,” without which “postmodernism” becomes a slippery term. In their anthology, Bradbury and McFarlane define modernism as a literary movement between 1890 and 1930. In the Preface to his anthology, Peter Brook describes postmodern as the capitalist world (television, mass production, and consumption) and its opponents. What is modernism to Chaloupka? We are provided a key summary of features near the end: liberal and Marxist commitment to scientific certainty (134). And he is still defining postmodern/postructural/deconstructive and liberal humanist discourse in the last chapter. I do not have space to describe all the reasons why this book makes difficult reading. (Is “nukespeak” criticism “a simple critique of euphemism,” when Hilgartner, et al.’s Nukespeak is a major analysis of secrecy and censorship in the United States?) But let me end mainly positively. By insisting upon the failure of the traditional Enlightenment liberal humanistic, scientific, opposition to nuclear war preparations (Chap. 4 on Star Wars and the Freeze), and by urging an alternative strategy of postmodern irony, he nudges all of us in the peace movement to rethink our assumptions and methods. Liberal humanist antinuclearist politics has offered (referring to Helen Caldicott) “a sober, anti-ironic terrorism of images” (133–34), but has it generally degenerated into finalities that resolve questions, reify value choices, and avoid realistic politics (137)? He too sweepingly dismisses the flexibility and the achievements of the liberal humanist antinuclearists. But of great value, postmodern politics seeks “to delegitimize the subtle, contemporary forms of authority” in both nuclearists and antinuclearists //////(128), and discards programs but offers ironic possibilities in the face of the paradoxes of power. However, the “discourse that would raise those discomforts in a critical manner has hardly begun to be identified” (138).

### Cap

**New zizek and daly card with new warrants justifies new answers, Capitalism is the most ethical system**

C. Bradley **Thompson. 1993**. BB&T Research Professor at Clemson University and the Executive Director of the Clemson Institute for the Study of Capitalism “Socialism vs. Capitalism: which is the moral system”On Principle, v1n3 October 1993

The intellectuals’ mantra runs something like this: In theory socialism is the morally superior social system despite its dismal record of failure in the real world. Capitalism, by contrast, is a morally bankrupt system despite the extraordinary prosperity it has created. In other words, capitalism at best, can only be defended on pragmatic grounds. We tolerate it because it works. Under socialism a ruling class of intellectuals, bureaucrats and social planners decide what people want or what is good for society and then use the coercive power of the State to regulate, tax, and redistribute the wealth of those who work for a living. In other words, socialism is a form of legalized theft. The morality of socialism can be summed-up in two words: envy and self-sacrifice. Envy is the desire to not only possess another’s wealth but also the desire to see another’s wealth lowered to the level of one’s own. Socialism’s teaching on self-sacrifice was nicely summarized by two of its greatest defenders, Hermann Goering and Bennito Mussolini. The highest principle of Nazism (National Socialism), said Goering, is: "Common good comes before private good." Fascism, said Mussolini, is " a life in which the individual, through the sacrifice of his own private interests…realizes that completely spiritual existence in which his value as a man lies." Socialism is the social system which institutionalizes envy and self-sacrifice: It is the social system which uses compulsion and the organized violence of the State to expropriate wealth from the producer class for its redistribution to the parasitical class. Despite the intellectuals’ psychotic hatred of capitalism, it is the only moral and just social system. Capitalism is the only moral system because it requires human beings to deal with one another as traders--that is, as free moral agents trading and selling goods and services on the basis of mutual consent. Capitalism is the only just system because the sole criterion that determines the value of thing exchanged is the free, voluntary, universal judgement of the consumer. Coercion and fraud are anathema to the free-market system. It is both moral and just because the degree to which man rises or falls in society is determined by the degree to which he uses his mind. Capitalism is the only social system that rewards merit, ability and achievement, regardless of one’s birth or station in life. Yes, there are winners and losers in capitalism. The winners are those who are honest, industrious, thoughtful, prudent, frugal, responsible, disciplined, and efficient. The losers are those who are shiftless, lazy, imprudent, extravagant, negligent, impractical, and inefficient. Capitalism is the only social system that rewards virtue and punishes vice. This applies to both the business executive and the carpenter, the lawyer and the factory worker. But how does the entrepreneurial mind work? Have you ever wondered about the mental processes of the men and women who invented penicillin, the internal combustion engine, the airplane, the radio, the electric light, canned food, air conditioning, washing machines, dishwashers, computers, etc.? What are the characteristics of the entrepreneur? The entrepreneur is that man or woman with unlimited drive, initiative, insight, energy, daring creativity, optimism and ingenuity. The entrepreneur is the man who sees in every field a potential garden, in every seed an apple. Wealth starts with ideas in people’s heads. The entrepreneur is therefore above all else a man of the mind. The entrepreneur is the man who is constantly thinking of new ways to improve the material or spiritual lives of the greatest number of people. And what are the social and political conditions which encourage or inhibit the entrepreneurial mind? The free-enterprise system is not possible without the sanctity of private property, the freedom of contract, free trade and the rule of law. But the one thing that the entrepreneur values over all others is freedom--the freedom to experiment, invent and produce. The one thing that the entrepreneur dreads is government intervention. Government taxation and regulation are the means by which social planners punish and restrict the man or woman of ideas. Welfare, regulations, taxes, tariffs, minimum-wage laws are all immoral because they use the coercive power of the state to organize human choice and action; they’re immoral because they inhibit or deny the freedom to choose how we live our lives; they’re immoral because they deny our right to live as autonomous moral agents; and they’re immoral because they deny our essential humanity. If you think this is hyperbole, stop paying your taxes for a year or two and see what happens. The requirements for success in a free society demand that ordinary citizens order their lives in accordance with certain virtues--namely, rationality, independence, industriousness, prudence, frugality, etc. In a free capitalist society individuals must choose for themselves how they will order their lives and the values they will pursue. Under socialism, most of life’s decisions are made for you. Both socialism and capitalism have incentive programs. Under socialism there are built-in incentives to shirk responsibility. There is no reason to work harder than anyone else because the rewards are shared and therefore minimal to the hard-working individual; indeed, the incentive is to work less than others because the immediate loss is shared and therefore minimal to the slacker. Under capitalism, the incentive is to work harder because each producer will receive the total value of his production--the rewards are not shared. Simply put: socialism rewards sloth and penalizes hard work while capitalism rewards hard work and penalizes sloth..