# 1AC

### Adv 1—Preemption

#### Current doctrine allows the executive complete authority over when and where to conduct a cyber-attack. These standards aren’t transparent and justify pre-emption making cyber war inevitable

David HUSBAND, Electronic Privacy Information Center (EPIC) National Security Appellate Fellow, Harvard Law School graduate, Governor with the American Bar Association Law School Division, 3/5 [March 5, 2014, “Offensive Cyber Operations and America's Grand Strategy Mistake,” http://epic.org/blog/2014/03/offensive-cyber-operations-and-americas-grand-strategy-error.html]

The New York Times recently revealed a secret debate that has been taking place behind the scenes within the Obama Administration regarding whether or not to undertake cyber-attacks against the Assad regime in Syria. The Pentagon and the National Security Agency developed a plan in 2011 to "essentially turn the lights out for Assad," but President Obama rejected the cyber-strikes, as well as regular kinetic approaches, to the conflict. The Times speculates that some of the reasons for not attacking Syria include the doubtful utility of the strikes, the possibility of retaliation, and the larger debate about the use of cyber-weapons in general.¶ Another possible reason, which the NYT does not discuss, may be a lack of legal authority. Over at Lawfare, Jack Goldsmith provides a cogent analysis of the potential domestic legal basis for the strikes. Goldmsith first notes the relatively sparse legal authority for the President to undertake overt action without the support of Congress against an adversary that is unconnected to the war on terror (so the AUMF would not apply.) He also believes it is unlikely to fall within the Article II self-defense powers that may have justified action against Iran (as with Stuxnet), while concluding there might be statutory authority under § 954 of the National Defense Authorization Act for Fiscal Year 2012.¶ However, it is the larger debate over the use of cyber-weapons in general that is most fascinating. The Washington Post disclosed last August that America mounted 231 offensive cyber-operations in 2011 alone, noting that "the scope and scale of offensive operations represent an evolution in policy, which in the past sought to preserve an international norm against acts of aggression in cyberspace, in part because U.S. economic and military power depend so heavily on computers." A major question is why has this policy changed? Why is the American military so determined to engage in offensive cyber-warfare when America may be one of the most vulnerable countries in the world to cyber attack?¶ There should be a serious, public debate about the value of offensive cyber operations for American security versus the costs. There are indications that this debate has occurred behind the scenes, but if we have learned anything from the NSA surveillance scandal, it is that the American people should be involved in the debate. It is the American people who should be setting the terms of whether we should even engage in this war and, if we choose to do so, to what extent we should prosecute the war. This debate, quite frankly, should be far more public than it has been. It is high time that Americans are aware of what is being done in our name in the realm of national security, when the potential blowback and costs are so high.¶ The costs are manifold: they include giving increased prominence to cyber-warfare (thus increasing the likelihood that cyber-attacks will become a more broadly accepted military option), militarizing cyberspace and the internet, the publicity costs and reputational harm to American interests when these secret operations are inevitably revealed, and the threat of counter-attacks which can cause substantial economic damage when they occur. Finally, in a time of budget austerity, the increased cyber-arms race represents misdirected tax dollars that could be developing America rather than tearing down other countries.¶ In 1800, the submarine was first introduced to the Royal Navy, impressing Prime Minister William Pitt, but not the First Sea Lord at the time, Earl Vincent. Vincent exclaimed, "Pitt was the greatest fool that ever existed to encourage a mode of warfare, which those who command the sea did not want, and which, if successful, would deprive them of it." Obviously, the answer to the submarine problem was not simply to ignore submarines. From the Royal Navy's perspective, the answer was to focus on devising effective responses to them in order to maintain control of the ocean.¶ Yet, there is wisdom in Vincent's words. Why encourage and lead the way in developing an asymmetric technology that can dangerously harm your position, which you have expended great blood and treasure to build up? Even if this technology were developed, why would you do so while your existing defenses were woefully inadequate?¶ This, in short, is the dilemma the American military is facing with regards to cyber-warfare. According to security experts, "Cyberwar is the greatest threat facing the United States--outstripping even terrorism." Former Secretary of Defense Leon Pannetta publicly proclaimed, "such a destructive cyber attack could virtually paralyze the nation." Yet currently, the "most kinetic cyberattack to date was probably the Stuxnet worm that attacked Iran's Natanz nuclear enrichment facility in 2010," which the U.S. is widely believed to be responsible for. Previously, the Pentagon seemed to understand these shortcomings, believing that cyber-deterrence would be exceptionally difficult.¶ However, the current strategic thinking seems to be that engaging in offensive cyber operations will have a deterrent effect on other countries, making them less likely to engage in cyber-conflict with us if they see how strong they are. It is difficult to be sure this is the exact strategic thinking because the relevant documents are highly classified, despite EPIC's attempt to secure public access to them through the Freedom of Information Act. However, this idea is flawed, because cyber-warfare seems an ideal asymmetric tool for terrorists, non-attributable state actors, or attributable state actors who are too powerful for us to directly confront (China and Russia spring to mind). It seems a clear error of grand strategy to escalate a cyber arms race that could leave American infrastructure in shambles, with stunned Americans cast into sudden darkness, if we are attacked¶ The risk of a "cyber Pearl Harbor" to our critical infrastructure that we are frequently warned about is only exacerbated when we are constantly striking at the infrastructure of other countries. The politics of secret destruction in the name of national security are always easy--it is the politics of informed debate and creation in the name of democracy that are truly challenging.

#### Our policy has created a cyber-Cold War

Stephen BENAVIDES, policy analyst and union organizer, Truthout, 13 [July 30, 2013, “The Coming Cyber-Cold War: US Pioneering Online Attacks,” http://truth-out.org/news/item/17714-the-coming-cyber-cold-war]

The US government is openly and actively engaged in a reincarnation of the Cold War. Physical assets such as spies and informants have been replaced with zero-day software exploits and network security analysts. Old-school intelligence gathering, while effective to some degree, pales in comparison with the scope of big-data firms such as Endgame and Palantir. Instead of war-ravaged proximity states in Eastern Europe or the Middle East, we have shadowy “actors in cyberspace” and network backdoors on the Internet. The development and expansion of cyber-security, and hence cyber-warfare - equivalent to an arms race - has been in the works for decades and is now a prime objective for the executive branch and the Department of Defense. As the US prepares to deploy weaponized malware and viruses against its enemies, it is forcing those enemies to respond in kind. We are witnessing the first stage of an America-led arms race that undoubtedly will result in a cyber cold war.¶ Before Edward Snowden released details about foreign and domestic spying program PRISM, low-level and continuous cyber espionage was well underway. As far back as 2002, a three-year attack accessed and downloaded 10 to 20 terabytes of sensitive information from the Department of Defense in an operation titled "Titan Rain." The culprit - whether an individual or a state - was never identified. In 2009, there were cyber attacks on the US water and sewage systems, as well as the national electrical grid. China and Russia are alleged to have accessed secure systems and mapped out the entire infrastructure of the country. More recently, the Obama administration was forced to admit that it had deployed Stuxnet against Iranian nuclear centrifuges and that the NSA attacked Tsinghua University, a research facility in China. ¶ “Cyber warfare attacks” are the new terrorism, with risk to economic and national security elevated to Orwellian heights found post-9/11. At least that's what US military commanders want the public to believe.¶

#### Un-regulated offensive postures are bound to escalate—complexity and inter-connected infrastructures

Stephen BENAVIDES, policy analyst and union organizer, Truthout, 13 [July 30, 2013, “The Coming Cyber-Cold War: US Pioneering Online Attacks,” http://truth-out.org/news/item/17714-the-coming-cyber-cold-war]

The unregulated nature of the cyber arms trade not only leaves open the possibility of technology falling into an opposition organization's possession, but guarantees it. Once again, the US is leading weapons proliferation. Political inconvenience of a militarized conventional war also may play a part in the burgeoning cyber war. It is much more difficult for military commanders to justify the death of a sister or brother in combat operations widely understood to be about maintaining access to energy resources than a "victimless" attack on a foreign government to protect internal bank documents or dam vulnerabilities.¶ The government does acknowledge that the directive may raise unique national security and foreign policy concerns, and it states, "DCEO (Defensive Cyber Effects Operations) and OCEO (Offensive Cyber Effects Operations), even for subtle or clandestine operations, may generate cyber effects in locations other than the intended target, with potential unintended or collateral consequences that may affect U.S. national interests in many locations." One issue with waging war in an unknown environment, often against unknown enemies, is that an actor is unable to predict with any accuracy how weaponized software may interact with different systems. Even the most professional attacks have been known to spiral out of control, which leaves open the risk that an attack on an enemy ultimately will affect those it was designed to "protect."¶ Governments have not moved to apply international laws of war to cyberspace, although they call it warfare nonetheless. The Pentagon says the same rules of engagement apply, which is patently false because the US is under constant attack and also is attacking every day. Where is the open declaration of war? There is none. Instead the Internet is a militarized proxy, a theater for a new cold war. And anyone who wants to participate can. It took only 20 years for the parent of the Internet, the US military, to exercise overwhelming influence on its once-free and forlorn child. The Internet is now, or maybe has always been, an agent of the state.

#### U.S. cyber-attacks inevitably escalate to kinetic war

Trefor MOSS, journalist covering Asian politics, 13 [April 19, 2013, “Is Cyber War the New Cold War?” The Diplomat, http://thediplomat.com/2013/04/is-cyber-war-the-new-cold-war/?allpages=yes]

Cyberspace matters. We know this because governments and militaries around the world are scrambling to control the digital space even as they slash defense spending in other areas, rapidly building up cyber forces with which to defend their own virtual territories and attack those of their rivals.¶ But we do not yet know how much cyberspace matters, at least in security terms. Is it merely warfare’s new periphery, the theatre for a 21st century Cold War that will be waged unseen, and with practically no real-world consequences? Or is it emerging as the most important battle-space of the information age, the critical domain in which future wars will be won and lost?¶ For the time being, some states appear quite content to err on the side of boldness when it comes to cyber. This brazen approach to cyber operations—repeated attacks followed by often flimsy denials—almost suggests a view of cyberspace as a parallel universe in which actions do not carry real-world consequences. This would be a risky assumption. The victims of cyber attacks are becoming increasingly sensitive about what they perceive as acts of aggression, and are growing more inclined to retaliate, either legally, virtually, or perhaps even kinetically.¶ The United States, in particular, appears to have run out of patience with the stream of cyber attacks targeting it from China—Google and The New York Times being just two of the most high-profile victims—and which President Obama has now insisted are at least partly state-sponsored.¶ 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 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 21st century 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.

#### Kinetic attacks causes nuclear war

Zanvyl KRIEGER, School of Arts and Sciences at Johns Hopkins University, AND Ariel Ilan ROTH, Department of Political Science and IR at Goucher College, 7 [Autumn 2007, “Nuclear Weapons in Neo-Realist Theory,” *International Studies Review*, Vol. 9, No. 3, pp. 369-384, Accessed through JSTOR]

Critical, though not explicit, in Waltz is the belief that a war between nuclear powers will be hard to maintain at the conventional level. Waltz (Waltz and Sagan 2003:9) allows that such a sub-nuclear war may be fought but considers the risk of it escalating to the nuclear level with its accompanying certain destruction as too high for the risk tolerance of most leaders. The strategic studies literature has played host to this debate for decades. Some, like Snyder (1965), have argued that nuclear weapons are, in a sense, mutually negating, creating what has been called the stability-instability paradox, wherein stability at the nuclear level breeds instability at the conventional level. It is, in this conception, as if two duelists stand with guns loaded and cocked at each other’s heads yet proceed to have their fight with daggers instead (Jervis 1989:19-20). Others, like Barry Posen (1982), have argued that even though nuclear states may wish to limit their conflict to conventional weapons, actions that occur during wartime can lead to what he calls “inadvertent escalation.” In his “Cold War Turned Hot” example, NATO attacks near Soviet ballistic submarine bases could draw a nuclear response even though the aim of NATO is not to harm the strategically stabilizing Soviet submarine-based missile arsenal (Posen 1982:29-30). Such an interaction would then escalate further as American targets were hit with nuclear weapons and a war that was supposed to be both limited and sub-nuclear is now an apocalyptic doomsday. The prospects for inadvertent escalation are recognized by Jervis (1989:21) as well who comments that “because escalation can occur although no one wants it to, mutual second-strike capability does not make the world safe for major provocations and limited wars.” This conclusion leads to the first of Jervis’ (1989:23-24) expected outcomes from what he calls the “nuclear revolution,” namely, that there will be peace among the great powers.

#### Uniquely true because of misperceptions

Edited by Kristin M. LORD, Vice President and Director of Studies at the Center for a New American Security AND Travis SHARP, Bacevich Fellow at the Center for a New American Security, 11

Contributors: Robert E. Kahn, Mike McConnell, Joseph S. Nye, Jr. and Peter Schwartz (co-chairs); Nova J. Daly, Nathaniel Fick, Martha Finnemore, Richard Fontaine, Daniel E. Geer Jr., David A. Gross, Jason Healey, James A. Lewis, Kristin M. Lord, M. Ethan Lucarelli, Thomas G. Mahnken, Gary McGraw, Roger H. Miksad, Gregory J. Rattray, Will Rogers, Christopher M. Schroeder and Travis Sharp [June 2011, “America’s Cyber Future Security and Prosperity in the Information Age,” Volume I, Center for a New American Security, http://www.cnas.org/files/documents/publications/CNAS\_Cyber\_Volume%20I.pdf]

Offensive dominance creates a great risk of cyber arms races. State and non-state actors are likely to view the prevalence of offensive cyber threats as a legitimate rationale for bolstering their own capabilities, both defensive and offensive, thus fueling an action-reaction dynamic of iterative arming. Experts believe that at least 20 nations are engaged in a cyber arms competition and possess the type of advanced capabilities needed to wage cyber war against the United States.121 As Michael Nacht, Former Assistant Secretary of Defense for Global Strategic Affairs, told us, “An arms race is already going on in cyberspace and it is very intense.”122¶ Conflict in cyberspace is uniquely predisposed to escalation given uncertainties about what constitutes an act of war and the growing number of state and non-state actors seeking offensive capabilities. Actors are more likely to misperceive or miscalculate actions in cyberspace, where there is no widely understood strategic language for signaling intent, capability and resolve.123 Uncertainty will encourage states to prepare for worst-case contingencies, a condition that could fuel escalation. Furthermore, “false flag” attacks, in which an actor purposefully makes an attack look like it came from a third party, could also ignite a conflict.124

#### Independently—cyber-attacks breaks down command and control—causes nuclear response. The bureaucratic decision to react without information is a result of situating offensive cyber ops with the president

Stephen CIMBALA, Professor of Political Science at Penn State, 11 [Spring 2011 “Nuclear Crisis Management and "Cyberwar" Phishing for Trouble?” *Strategic Studies Quarterly*, 5.1, p. 117-131, Accessed through ProQuest]

This section discusses how cyberwar might adversely affect nuclear crisis management. Readers are advised, however, that history is indeterminate. It might turn out that, in some fortuitous cases, the United States could use nuclear deterrence and cyberwar as joint multipliers toward a successful outcome in crisis or war. For example, in facing down an opponent with a comparatively small or no nuclear arsenal and inferior conventional strike capabilities, the United States or another power could employ information warfare aggressively "up front" while forgoing explicit mention of its available nuclear capability. Russia's five-day war against Georgia in August 2008 involved obvious cyber attacks as well as land and air operations, but no explicit nuclear threats. On the other hand, had Georgia already been taken into membership by NATO prior to August 2008 or had Russo-Georgian fighting spread into NATO member-state territory, the visibility of Russia's nuclear arsenal as a latent and potentially explicit threat would have been much greater.¶ Notwithstanding the preceding disclaimers, information warfare has the potential to attack or disrupt successful crisis management on each of four dimensions. First, it can muddy the signals being sent from one side to the other in a crisis. This can be done deliberately or inadvertently. Suppose one side plants a virus or worm in the other's communications networks.19 The virus or worm becomes activated during the crisis and destroys or alters information. The missing or altered information may make it more difficult for the cyber victim to arrange a military attack. But destroyed or altered information may mislead either side into thinking that its signal has been correctly interpreted when it has not. Thus, side A may intend to signal "resolve" instead of "yield" to its opponent on a particular issue. Side B, misperceiving a "yield" message, may decide to continue its aggression, meeting unexpected resistance and causing a much more dangerous situation to develop.¶ Infowar can also destroy or disrupt communication channels necessary for successful crisis management. One way it can do this is to disrupt communication links between policymakers and military commanders during a period of high threat and severe time pressure. Two kinds of unanticipated problems, from the standpoint of civil-military relations, are possible under these conditions. First, political leaders may have predelegated limited authority for nuclear release or launch under restrictive conditions; only when these few conditions obtain, according to the protocols of predelegation, would military commanders be authorized to employ nuclear weapons distributed within their command. Clogged, destroyed, or disrupted communications could prevent top leaders from knowing that military commanders perceived a situation to be far more desperate, and thus permissive of nuclear initiative, than it really was. During the Cold War, for example, disrupted communications between the US National Command Authority and ballistic missile submarines, once the latter came under attack, could have resulted in a joint decision by submarine officers to launch in the absence of contrary instructions.¶ Second, information warfare during a crisis will almost certainly increase the time pressure under which political leaders operate. It may do this literally, or it may affect the perceived timelines within which the policymaking process can make its decisions. Once either side sees parts of its command, control, and communications (C3) system being subverted by phony information or extraneous cyber noise, its sense of panic at the possible loss of military options will be enormous. In the case of US Cold War nuclear war plans, for example, disruption of even portions of the strategic C3 system could have prevented competent execution of parts of the SIOP (the strategic nuclear war plan). The SIOP depended upon finely orchestrated time-on-target estimates and precise damage expectancies against various classes of targets. Partially misinformed or disinformed networks and communications centers would have led to redundant attacks against the same target sets and, quite possibly, unplanned attacks on friendly military or civilian installations.¶ A third potentially disruptive effect of infowar on nuclear crisis management is that it may reduce the search for available alternatives to the few and desperate. Policymakers searching for escapes from crisis denouements need flexible options and creative problem solving. Victims of information warfare may have a diminished ability to solve problems routinely, let alone creatively, once information networks are filled with flotsam and jetsam. Questions to operators will be poorly posed, and responses (if available at all) will be driven toward the least common denominator of previously programmed standard operating procedures. Retaliatory systems that depend on launch-on-warning instead of survival after riding out an attack are especially vulnerable to reduced time cycles and restricted alternatives:¶ A well-designed warning system cannot save commanders from misjudging the situation under the constraints of time and information imposed by a posture of launch on warning. Such a posture truncates the decision process too early for iterative estimates to converge on reality. Rapid reaction is inherently unstable because it cuts short the learning time needed to match perception with reality.20¶ The propensity to search for the first available alternative that meets minimum satisfactory conditions of goal attainment is strong enough under normal conditions in nonmilitary bureaucratic organizations.21 In civilmilitary command and control systems under the stress of nuclear crisis decision making, the first available alternative may quite literally be the last; or so policymakers and their military advisors may persuade themselves. Accordingly, the bias toward prompt and adequate solutions is strong. During the Cuban missile crisis, a number of members of the presidential advisory group continued to propound an air strike and invasion of Cuba during the entire 13 days of crisis deliberation. Had less time been available for debate and had President Kennedy not deliberately structured the discussion in a way that forced alternatives to the surface, the air strike and invasion might well have been the chosen alternative.22¶ Fourth and finally on the issue of crisis management, infowar can cause flawed images of each side's intentions and capabilities to be conveyed to the other, with potentially disastrous results. Another example from the Cuban crisis demonstrates the possible side effects of simple misunderstanding and noncommunication on US crisis management. At the most tense period of the crisis, a U-2 reconnaissance aircraft got off course and strayed into Soviet airspace. US and Soviet fighters scrambled, and a possible Arctic confrontation of air forces loomed. Khrushchev later told Kennedy that Soviet air defenses might have interpreted the U-2 flight as a prestrike reconnaissance mission or as a bomber, calling for a compensatory response by Moscow.23 Fortunately Moscow chose to give the United States the benefit of the doubt in this instance and to permit US fighters to escort the wayward U-2 back to Alaska. Why this scheduled U-2 mission was not scrubbed once the crisis began has never been fully revealed; the answer may be as simple as bureaucratic inertia compounded by noncommunication down the chain of command by policymakers who failed to appreciate the risk of "normal" reconnaissance under these extraordinary conditions.

#### The plan solves—

#### Ruling on the Third Amendment shifts authorization power for OCOs from the President to Congress since only Congress can authorize a quartering. This makes U.S. practice transparent and results in military attribution

Alan BUTLER, Appellate Advocacy Counsel, Electronic Privacy Information Center (EPIC); J.D. UCLA School of Law, 13 [June, 2013, “When Cyberweapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy,” American University Law Review, 62 Am. U.L. Rev. 1203, Lexis]

IV. Designing a National Cybersecurity Policy Informed by Third Amendment Principles¶ The preceding analysis of cyberoperations under the Third Amendment is focused primarily on the potential privacy impact of U.S. military intrusions into private networks. Given that the Third Amendment embodies the core value of protecting private property from military intrusion, its principles should inform the broader debate over cybersecurity policy.¶ The President, the DoD, the Department of Homeland Security (DHS), and Congress are all currently involved in developing a comprehensive cybersecurity strategy. n215 The DoD established USCYBERCOM in 2009 to advance the technical and operational capabilities necessary to implement a comprehensive cybersecurity strategy. n216 Congress considered competing proposals in 2012 - both of which focused on creating a new "information sharing' environment between private companies and government. n217 The President has issued a directive establishing "principles and processes for the use of cyber operations," n218 and conducted an internal legal analysis of his authority vis-a-vis cyberwarfare. n219¶ Yet, so far, none of these efforts have adequately addressed the civil liberties impact of cyberoperations. Even though the White House issued a "Cyberspace Policy Review" stressing the need to "conduct a national dialogue on cybersecurity" and reaffirming "the national commitment to privacy rights and civil liberties guaranteed by the Constitution and law," n220 the administration has not yet engaged in such a dialogue. Some within the DoD have acknowledged that there will be difficult questions in applying traditional legal rules to cyberspace, but so far, the DoD has not [\*1235] provided solutions. n221 Congress has focused on eliminating privacy rules that it claims would hamper corporate information sharing with the DHS and NSA. n222¶ The Third Amendment implications of military cyberoperations raise three important questions that should guide the development of cybersecurity policy going forward: (1) Can the President alone authorize military actions that have the potential to intrude upon civilian networks? (2) How can "consent" be granted for such cyberspace operations? (3) Would the United States be forced to admit attribution for a given attack if it intruded upon an innocent third-party network? These questions address the three key elements of a comprehensive cybersecurity strategy: authority, cooperation, and transparency.¶ A. Authority: Congress Must Be Involved in Establishing Any Framework for the Authorization of Cyberoperations¶ Given that the Third Amendment requires war-time quartering be conducted "in a manner to be prescribed by law," n223 Congress must have a role in establishing the framework used to authorize any offensive cyberoperation. This legislative involvement would not only ensure that all cyberoperations have adequate legal authorization but it would also promote the broader goals of transparency and cooperation that the President has emphasized throughout this process.¶ So far Congress has focused its energy on perceived problems rather than real solutions. n224 A debate raged in the 112th Congress over whether to let DHS or NSA take the lead on a proposed information-sharing environment. n225 This turf war was quite tangential from the problems of substandard security for critical systems and a lack of legal clarity as to the role of each government [\*1236] agency in responding to an external threat or strategic opportunity. n226 The only congressional involvement in developing a cybersecurity framework so far has been its brief affirmance in the 2012 National Defense Authorization Act n227 that the President may conduct "operations in cyberspace" subject to the traditional legal regimes applicable to kinetic warfare. n228 Congress's active role in setting our nation's military actions in cyberspace is the only way to have a national dialogue and to avoid relying on secret legal interpretations about important national security matters.¶ The President took steps to begin a national dialogue when he issued an Executive Order on the same day as the 2013 State of the Union Address. n229 The Executive Order focused on improving critical infrastructure cybersecurity while promoting privacy, civil liberties, and the economy. n230 The Order also provided for sharing of "cyber threat information" from executive branch agencies to private sector entities, n231 and the development of a framework by the National Institute of Standards and Technology (NIST) to establish baseline security standards for government agencies and critical infrastructure companies. n232 The Order also required that privacy and civil liberties protections be incorporated into the cybersecurity program and that the Chief Privacy Officer of DHS assess the privacy risks and publish a report. n233¶ [\*1237] The Executive Order did not address the "information sharing environment" proposed in Congress during 2012 and again in 2013. n234 The Order also did not address the legal determination of when and how cyberoperations can be authorized, which has apparently already been made in an internal executive-branch memorandum. n235 The President's Executive Order is a step in the right direction but it does not provide sufficient authority for cyberoperations that could intrude upon civilian systems; only Congress can authorize such quartering.

#### Strong civilian oversight is necessary to check strategic instability in cyber space. Absent the plan, nuclear war is inevitable

Dr. Greg AUSTIN, director of policy innovation at the EastWest Institute and Visiting Senior Fellow in the Department of War Studies in King’s College London, 13 [August 6, 2013, “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.¶

### tAdv 2—PC

#### Advantage Two is Posse Comitatus—

#### Current cyber policy is eroding the Posse Comitatus. The military is usurping control from civilian enforcement. That’s a slippery slope

Tim MAURER, Program Associate at the New America Foundation’s Open Technology Institute, 12 [December 5, 2012, “Is it Legal for the Military to Patrol American Networks?” http://www.foreignpolicy.com/articles/2012/12/05/is\_it\_legal\_for\_the\_military\_to\_patrol\_american\_networks]

Over the past couple months, the Pentagon has assumed an increasing role in defending American networks. In October, Secretary of Defense Leon Panetta announced new rules of engagement for the Pentagon's cyber operations. "The new rules will make clear that the department has a responsibility, not only to defend DOD networks, but also to be prepared to defend the nation and our national interests against an attack in or through cyberspace." Panetta insisted that the Pentagon would play only a "supporting role," but as James Lewis at the Center for Strategic and International Studies pointed out, "When it comes to cybersecurity, the center of action just shifted." And, indeed, a few weeks ago, the Washington Post revealed that President Obama had signed a secret directive expanding the U.S. military's authority in cyberspace to include defense of non-military networks.¶ It is a sign that efforts to develop the capacity of the Department of Homeland Security (DHS) to defend cyberspace have not kept pace with the perception of increasing threats. But it's also a sign that the United States is struggling to adapt to a world of transnational threats -- and risks eroding the fundamental distinction between the traditional roles of civilian and military forces in providing security. The Posse Comitatus Act of 1878 has restricted the deployment of federal troops in the homeland since the end of Reconstruction. It enshrined the idea that police forces are responsible for security within U.S. borders, while the military protects against threats beyond the country's borders. That is why only in extreme circumstances -- a natural or man-made crisis -- do we see troops in the streets.¶ The new policy is essentially the result of a trade-off between authority and capacity: The Department of Homeland Security has the authority, but not sufficient capacity to effectively defend the nation's networks. In contrast, the Department of Defense has better capacity, but not the authority. The choice then is to build up DHS's capacity, leaving the nation less protected in the interim, or expand DOD's authority. (This publication by National Defense University provides a more comprehensive analysis of the various policy options.)¶ Apparently, DHS has not been coming on fast enough. Lewis notes that "Iran has discovered a new way to harass much sooner than expected, and the United States is ill-prepared to deal with it," referencing the cyberattacks against the Saudi Aramco and RasGas companies. Secretary Panetta points out, "We know that foreign cyber-actors are probing America's critical infrastructure networks.... We know of specific instances where intruders have successfully gained access to these control systems. We also know they are seeking to create advanced tools to attack these systems and cause panic, destruction, and even the loss of life."¶ So does that mean the Posse Comitatus Act doesn't apply in cyberspace? Or if it does apply, how so? While cyberspace is bound by physical infrastructure located on territory with national borders, cyberspace as a domain is very different from any of the four other territorial domains -- land, sea, air, and space. There is no physical border in cyberspace that an attacker must cross to hit at his or her target, as there was for the British ships in 1777, the Japanese planes in 1941, or the terrorists on 9/11. An attack can happen anywhere within the United States, and in the case of zero-day exploits -- a cyberattack using a previously unknown vulnerability -- without prior warning. How will the government know whether suspicious activity is a criminal matter most appropriate for law enforcement, or a security matter falling within the Department of Defense's mission to protect the nation against threats from abroad in light of the continued challenges to attribute the source of an attack?¶ Expanding the Pentagon's role is a slippery slope. Not only is the military ill-suited for many civilian tasks -- witness police training in Afghanistan -- it can also easily bump up against civil liberties. For example, the warrantless wiretapping scandal during the last decade included the National Security Agency -- whose director also leads U.S. Cyber Command -- which was authorized by an executive order to conduct domestic surveillance. If the military is taking over cybersecurity simply because it has greater capacity, what will prevent it from being asked to assume ever greater homeland responsibilities in the future? After all, the Pentagon is the largest organization in the world -- it has more capacity when it comes to any number of problems. But capability is not a sufficient argument for policy. It highlights how reactive our current approach to cybersecurity is. It is borne out of immediate necessity to fill the current gap, but we need an effective longer-term plan -- and an exit strategy for the Pentagon's involvement in domestic security.

#### That undermines military readiness

Gene HEALY, senior editor at the Cato Institute, 5 [September 27, 2005, “Domestic Militarization: A Disaster in the Making,” http://www.cato.org/publications/commentary/domestic-militarization-disaster-making]

Having already wrecked a legendary American city, Hurricane Katrina may now be invoked to undermine a fundamental principle of American law; that principle, enshrined in the Posse Comitatus Act, is that when it comes to domestic policing, the military should be a last resort, not a first responder.¶ In his televised address on September 15, President Bush declared that “It is now clear that a challenge on this scale requires greater federal authority and a broader role for the armed forces—the institution of our government most capable of massive logistical operations on a moment’s notice.” Senator John Warner (R-Va.), chair of the Armed Services Committee, goes further. In the wake of Katrina, he’s suggested weakening Posse Comitatus, the longstanding federal law that restricts the government’s ability to use the U.S. military as a police force. Pentagon spokesman Lawrence Di Rita called Posse Comitatus a “very archaic” law that hampers the president’s ability to respond to a crisis.¶ Not so. The Posse Comitatus Act is no barrier to federal troops providing logistical support during natural disasters. Nor does it prohibit the president from using the army to restore order in extraordinary circumstances—even over the objection of a state governor.¶ What it does is set a high bar for the use of federal troops in a policing role. That reflects America’s traditional distrust of using standing armies to enforce order at home, a distrust that’s well-justified.¶ There are very good reasons to resist any push toward domestic militarization. As one federal court has explained, “military personnel must be trained to operate under circumstances where the protection of constitutional freedoms cannot receive the consideration needed in order to assure their preservation. The Posse Comitatus statute is intended to meet that danger.” Army Lt. Gen. Russell Honore, commander of the federal troops helping out in New Orleans, seemed to recognize that danger when he ordered his soldiers to keep their guns pointed down: “This isn’t Iraq,” he growled.¶ Soldiers are trained to be warriors, not peace officers—which is as it should be. But putting full-time warriors into a civilian policing situation can result in serious collateral damage to American life and liberty.¶ It can also undermine military readiness, because when soldiers are forced into the role of police officers, their war-fighting skills degrade. That’s what the General Accounting Office concluded in a 2003 report looking at some of the homeland security missions the military was required to carry out after September 11, 2001. According to the report, “While on domestic military missions, combat units are unable to maintain proficiency because these missions provide less opportunity to practice the varied skills required for combat and consequently offer little training value.” GAO also concluded that such missions put a serious strain on a military already heavily committed abroad.¶ American law calls for civilian peace officers to keep the peace, or, failing that, National Guardsmen under the command of their state governors. So perhaps we should stop treating the National Guard as if it’s no different than the Army Reserve. As Katrina made landfall, there were 7,000 guardsmen from Louisiana and Mississippi deployed in Iraq. Among them were 3,700 members of Louisiana’s 256th Mechanized Infantry Brigade, who took with them high-water vehicles and other equipment that could have been put to better use in New Orleans. The guardsmen here at home had only one satellite phone for the entire Mississippi coast, when Katrina initially hit—because the others were in Iraq. Lt. Gen. Steven Blum, chief of the National Guard Bureau, noted that had the Louisiana Guardsmen “been at home and not in Iraq, their expertise and capabilities could have been brought to bear.” Disaster relief and responding to civil disturbances are core missions for the Guard; attempting to establish democracy in the Middle East is not.¶ The Katrina tragedy ought to be an occasion for rethinking a number of federal policies, including our promiscuous use of the Guard abroad. Instead, Washington seems poised to embrace further centralization and militarization at home. That has the makings of a policy disaster that would dwarf Hurricane Katrina.

#### Readiness is key to hegemony and overall deterrence

Jack SPENCER, Policy Analyst for Defense and National Security at Heritage, 2K [September 15, 2000, “The Facts About Military Readiness,” http://www.heritage.org/research/reports/2000/09/bg1394-the-facts-about-military-readiness]

While there are clear signs that readiness is a problem for the U.S. military, Al Gore is factually correct when he contends that the U.S. armed forces stand far above any other military force. He is missing a more important point, however. The United States, as the most powerful nation in the world, has responsibilities and national security concerns far beyond those of any other nation.¶ U.S. military readiness cannot be gauged by comparing America's armed forces with other nations' militaries. Instead, the capability of U.S. forces to support America's national security requirements should be the measure of U.S. military readiness. Such a standard is necessary because America may confront threats from many different nations at once.¶ America's national security requirements dictate that the armed forces must be prepared to defeat groups of adversaries in a given war. America, as the sole remaining superpower, has many enemies. Because attacking America or its interests alone would surely end in defeat for a single nation, these enemies are likely to form alliances. Therefore, basing readiness on American military superiority over any single nation has little saliency.¶ The evidence indicates that the U.S. armed forces are not ready to support America's national security requirements. Moreover, regarding the broader capability to defeat groups of enemies, military readiness has been declining. The National Security Strategy, the U.S. official statement of national security objectives,3 concludes that the United States "must have the capability to deter and, if deterrence fails, defeat large-scale, cross-border aggression in two distant theaters in overlapping time frames."4 According to some of the military's highest-ranking officials, however, the United States cannot achieve this goal. Commandant of the Marine Corps General James Jones, former Chief of Naval Operations Admiral Jay Johnson, and Air Force Chief of Staff General Michael Ryan have all expressed serious concerns about their respective services' ability to carry out a two major theater war strategy.5 Recently retired Generals Anthony Zinni of the U.S. Marine Corps and George Joulwan of the U.S. Army have even questioned America's ability to conduct one major theater war the size of the 1991 Gulf War.6¶ Military readiness is vital because declines in America's military readiness signal to the rest of the world that the United States is not prepared to defend its interests. Therefore, potentially hostile nations will be more likely to lash out against American allies and interests, inevitably leading to U.S. involvement in combat. A high state of military readiness is more likely to deter potentially hostile nations from acting aggressively in regions of vital national interest, thereby preserving peace.

#### And blurring the lines between civil and military roles results in sweeping distrust of the military

Dan BENNETT, Student, Lewis & Clark Law School, J.D. expected 2007, 6 [Winter 2006, “Comment: The Domestic Role of the Military in America: Why Modifying or Repealing the Posse Comitatus Act Would Be a Mistake,” Lewis & Clark Law Review, 10 Lewis & Clark L. Rev. 935, Lexis]

Another concern about blurring the line between the realms of the military and the civilian government that controls it is the need to maintain a universal trust in the military as a non-political body. While polls suggest that only 22% of the American people trust Congress, and only 44% trust the president, an impressive 74% of people in this country trust the military. n41 If the military were seen to be doing the bidding of Congress in the domestic arena, it is likely that Americans' distrust of the government would lead to them, correctly or incorrectly, perceiving that the military was abandoning its crucial political neutrality. If the American people made that leap, institutional trust and confidence in the military would be undermined.¶ Finally, there is something inherently repugnant to most Americans at the thought of the military patrolling the streets of our cities and towns. One commentator imagines a future where the PCA has been repealed, and envisions "gray armored vehicles staffed by officers in black SWAT uniforms" patrolling neighborhoods and carelessly opening fire on peaceful protestors. n42 An inarguably chilling image that should cause PCA opponents to hesitate.¶

#### Lack of military legitimacy undermines CMR and hegemony

Rudy BARNES, Jr, retired colonel in the Army JAGC, 11 [January 28, 2011, “An Isolated Military as a Threat to Military Legitimacy,” http://militarylegitimacyreview.com/?page\_id=159]

The legitimacy of the US military depends upon civil-military relations. In Iraq and Afghanistan conflicting religions and cultures have presented daunting challenges for the US military since mission success in counterinsurgency (COIN) operations depends upon public support in those hostile cultural environments; and even in the US, civil-military relations are fragile since the military is an authoritarian regime within a democratic society. This cultural dichotomy within our society creates the continuing potential for conflict between authoritarian military values and more libertarian civilian values that can undermine military legitimacy, especially when there are fewer bridges between the military and the civilian population it serves.¶ The US military is a shield that protects our national security, but it can also be a sword that threatens our national security. After all, the US military controls the world’s most destructive weaponry. Our Founding Fathers understood this danger and provided for a separation of powers to prevent a concentration of power in the military. Still, if the US military were ever to become isolated from the civilian population it serves, then civil-military relations would deteriorate and US security would be at risk.¶ Richard Cohen has opined that we are slowly but inexorably moving toward an isolated military:¶ The military of today is removed from society in general. It is a majority white and, according to a Heritage Foundation study, disproportionately Southern. New England is underrepresented, and so are big cities, but the poor are no longer cannon fodder – if they ever were – and neither are blacks. We all fight and die just about in proportion to our numbers in the population.¶ The all-volunteer military has enabled America to fight two wars while many of its citizens do not know of a single fatality or even of anyone who has fought overseas. This is a military conscripted by culture and class – induced, not coerced, indoctrinated in all the proper cliches about serving one’s country, honored and romanticized by those of us who would not, for a moment, think of doing the same. You get the picture.¶ Talking about the picture, what exactly is wrong with it? A couple of things. First, this distant Army enables us to fight wars about which the general public is largely indifferent. Had there been a draft, the war in Iraq might never have been fought – or would have produced the civil protests of the Vietnam War era. The Iraq debacle was made possible by a professional military and by going into debt. George W. Bush didn’t need your body or, in the short run, your money. Southerners would fight, and foreigners would buy the bonds. For understandable reasons, no great songs have come out of the war in Iraq.¶ The other problem is that the military has become something of a priesthood. It is virtually worshipped for its admirable qualities while its less admirable ones are hardly mentioned or known. It has such standing that it is awfully hard for mere civilians – including the commander in chief – to question it. Dwight Eisenhower could because he had stars on his shoulders, and when he warned of the military-industrial complex, people paid some attention. Harry Truman had fought in one World War and John Kennedy and Gerald Ford in another, but now the political cupboard of combat vets is bare and there are few civilian leaders who have the experience, the standing, to question the military. This is yet another reason to mourn the death of Richard Holbrooke. He learned in Vietnam that stars don’t make for infallibility, sometimes just for arrogance. (Cohen, How Little the US Knows of War, Washington Post, January 4, 2011)¶ The 2010 elections generated the usual volume of political debate, but conspicuously absent were the two wars in which US military forces have been engaged for ten years. It seems that dissatisfaction with the wars in Iraq and Afghanistan has caused the American public to forget them and those military forces left to fight them.¶ A forgotten military can become an isolated military with the expected erosion of civil-military relations. But the forgotten US military has not gone unnoticed: Tom Brokaw noted that there have been almost 5,000 Americans killed and 30,000 wounded, with over $1 trillion spent on the wars in Afghanistan and Iraq, with no end in sight. Yet most Americans have little connection with the all-volunteer military that is fighting these wars. It represents only one percent of Americans and is drawn mostly from the working class and middle class. The result is that military families are often isolated “…in their own war zone.” (See Brokaw, The Wars that America Forgot About, New York Times, October 17, 2010) Bob Herbert echoed Brokaw’s sentiments and advocated reinstating the draft to end the cultural isolation of the military. (Herbert, The Way We Treat Our Troops, New York Times, October 22, 2010)¶ In another commentary on the forgotten military, Michael Gerson cited Secretary of Defense Robert Gates who warned of a widening cultural gap between military and civilian cultures: “There is a risk over time of developing a cadre of military leaders that politically, culturally and geographically have less and less in common with the people they have sworn to defend.” Secretary Gates promoted ROTC programs as a hedge against such a cultural divide. Gerson concluded that the military was a professional class by virtue of its unique skills and experience: “They are not like the rest of America—thank God. They bear a disproportionate burden, and they seem proud to do so. And they don’t need the rest of society to join them, just to support them.” (Gerson, The Wars We Left Behind, Washington Post, October 28, 2010)¶ The Chairman of the Joint Chiefs of Staff, Admiral Mike Mullen, has seconded the observations of Secretary Gates and warned of an increasingly isolated military and “…a potentially dangerous gulf between the civilian world and men and women in uniform.” Mullen explained, “To the degree that we are out of touch I believe is a very dangerous force.” And he went on to observe that “Our audience, our underpinnings, our authority, everything we are, everything we do, comes from the American people…and we cannot afford to be out of touch with them.” (Charley Keyes, Joint Chiefs Chair Warns of Disconnect Between Military and Civilians, CNN.com, January 10, 2011)¶ Gerson’s observation that the military are not like the rest of Americans goes to the heart of the matter. An isolated military that exacerbates conflicting military and civilian values could undermine civil-military relations and threaten military legitimacy. The potential for conflicting values is evident in the article by Kevin Govern on Higher Standards of Honorable Conduct Reinforced: Lessons (Re) Learned from the Captain Honors Incident (see article posted under this section) which highlights the “exemplary conduct” standard for military personnel and the need to enforce the unique standards of exemplary conduct to maintain good order and discipline in the military.¶ The communal and authoritarian military values inherent in the standards of exemplary conduct often clash with more libertarian civilian values; but in the past that clash has been moderated by bridges between the military and civilian cultures, most notably provided by the draft, the National Guard and reserve components. The draft is gone and the National Guard and reserve components are losing ground in an all-volunteer military that is withdrawing from Iraq and Afghanistan.¶ The Reserve Officer Training Program (ROTC) has provided most civilian-soldier leaders for the US military in the past, but it is doubtful that will continue in the future. If Coleman McCarthy speaks for our best colleges and universities, then ROTC is in trouble and so are civil-military relations:¶ These days, the academic senates of the Ivies and other schools are no doubt pondering the return of military recruiters to their campuses. Meanwhile, the Pentagon, which oversees ROTC programs on more than 300 campuses, has to be asking if it wants to expand to the elite campuses, where old antipathies are remembered on both sides. It should not be forgotten that schools have legitimate and moral reasons for keeping the military at bay, regardless of the repeal of “don’t ask, don’t tell.” They can stand with those who for reasons of conscience reject military solutions to conflicts. ROTC and its warrior ethic taint the intellectual purity of a school, if by purity we mean trying to rise above the foul idea that nations can kill and destroy their way to peace. If a school such as Harvard does sell out to the military, let it at least be honest and add a sign at its Cambridge front portal: Harvard, a Pentagon Annex. (Coleman McCarthy, Don’t ask, don’t tell has been repealed. ROTC still shouldn’t be on campus, Washington Post, December 30, 2010)¶ McCarthy’s attitude toward ROTC reflects a dangerous intellectual elitism that threatens civil-military relations and military legitimacy. But there are also conservative voices that recognize the limitations of ROTC and offer alternatives. John Lehman, a former Secretary of the Navy, and Richard Kohn, a professor of military history at the University of North Carolina at Chapel Hill, don’t take issue with McCarthy. They suggest that ROTC be abandoned in favor of a combination of military scholarships and officer training during summers and after graduation:¶ Rather than expanding ROTC into elite institutions, it would be better to replace ROTC over time with a more efficient, more effective and less costly program to attract the best of America’s youth to the services and perhaps to military careers. Except from an economic perspective, ROTC isn’t efficient for students. They take courses from faculty almost invariably less prepared and experienced to teach college courses, many of which do not count for credit and cover material more akin to military training than undergraduate education. Weekly drills and other activities dilute the focus on academic education. ROTC was begun before World War I to create an officer corps for a large force of reservists to be mobilized in a national emergency. It has outgrown this purpose and evolved into just another source of officers for a military establishment that has integrated regulars and reservists into a “total force” in which the difference is between part-time and full-time soldiering. The armed services should consider a program modeled in part on the Marine Platoon Leaders Corps to attract the nation’s most promising young people. In a national competition similar to ROTC scholarships, students should be recruited for four years of active duty and four years of reserve service by means of all-expenses-paid scholarships to the college or university of their choice. Many would no doubt take these lucrative grants to the nation’s most distinguished schools, where they would get top-flight educations and could devote full attention on campus to their studies. Youths would gain their military training and education by serving in the reserve or National Guard during college (thus fulfilling their reserve obligation). Being enlisted would teach them basic military skills and give them experience in being led before becoming leaders themselves. As reservists during college, they would be obligated to deploy only once, which would not unduly delay their education or commissioned service. They could receive their officer education at Officer Candidate School summer camps or after graduation from college. This program could also be available to those who do not win scholarships but are qualified and wish to serve. Such a system would cost less while attracting more, and more outstanding, youth to military service, spare uniformed officers for a maxed-out military establishment, and reconnect the nation’s leadership to military service – a concern since the beginning of the all-volunteer armed force. (Lehman and Kohn, Don’t expand ROTC. Replace it. Washington Post, January 28, 2011)¶ The system proposed by Lehman and Kohn would preserve good civil-military relations only if it could attract as many reserve component (civilian-soldier) military officers as has ROTC over the years. Otherwise the demise of ROTC will only hasten the isolation of the US military.¶ As noted by Richard Cohen, Tom Brokaw, Bob Herbert, Michael Gerson, Secretary of Defense Bill Gates and Chairman of the Joint Chiefs Admiral Mike Mullen, the increasing isolation of the US military is a real danger to civil-military relations and military legitimacy. The trends are ominous: US military forces are drawing down as they withdraw from Iraq and Afghanistan and budget cuts are certain to reduce both active and reserve components, with fewer bridges to link a shrinking and forgotten all-volunteer military to the civilian society it serves.¶ The US has been blessed with good civil-military relations over the years, primarily due to the many civilian-soldiers who have served in the military. But with fewer civilian-soldiers to moderate cultural differences between an authoritarian military and a democratic society, the isolation of the US military becomes more likely.¶ Secretary Gates and Admiral Mullen were right to emphasize the danger of an isolated military, but that has not always been the prevailing view. In his classic 1957 work on civil-military relations, The Soldier and the State, Samuel Huntington advocated the isolation of the professional military to prevent its corruption by civilian politics. It is ironic that in his later years Huntington saw the geopolitical threat environment as a clash of civilizations which required military leaders to work closely with civilians to achieve strategic political objectives in hostile cultural environments such as Iraq and Afghanistan. (see discussion in Barnes, Military Legitimacy: Might and Right in the New Millennium, Frank Cass, 1996, at pp 111-115)¶ Today, the specter of an isolated military haunts the future of civil-military relations and military legitimacy. With fewer civilian-soldiers from the National Guard and Reserve components to bridge the gap between our military and civilian cultures, an all-volunteer professional military could revive Huntington’s model of an isolated military to preserve its integrity from what it perceives to be a morally corrupt civilian society. It is an idea that has been argued before. (see Robert L. Maginnis, A Chasm of Values, Military Review (February 1993), cited in Barnes, Military Legitimacy: Might and Right in the New Millennium, Frank Cass, 1996, at p 55, n 6, and p 113, n 20)¶ The military is a small part of our population—only 1 percent—but the Department of Defense is our largest bureaucracy and notorious for its resistance to change. Thomas Jefferson once observed the need for such institutions to change with the times: “Laws and institutions must go hand in hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths disclosed, and manners and opinions change with the change of circumstance, institutions must advance also, and keep pace with the times.”¶ Michael Gerson noted that the military remains a unique culture of warriors within a civilian culture, and that “it is not like the rest of America.” For that reason a forgotten and isolated military with values that do not keep pace with changing times and circumstances and conflict with civilian values would not only be a threat to military legitimacy but also be a threat to our individual freedom and democracy.¶ In summary, the US military is in danger of becoming isolated from the civilian society it must serve. Military legitimacy and good civil-military relations depend upon the military maintaining close bonds with civilian society. In contemporary military operations military leaders must be both diplomats as well as warriors. They must be effective working with civilians in domestic and foreign emergencies and in civil-military operations such as counterinsurgency and stability operations, and they must be combat leaders who can destroy enemy forces with overwhelming force. Diplomat-warriors can perform these diverse leadership roles and maintain the close bonds needed between the military and civilian society. Such military leaders can help avoid an isolated military and insure healthy civil-military relations.

#### Loss of military effectiveness risks multiple nuclear wars—maintaining readiness is key

Frederick W. KAGAN, resident scholar at the American Enterprise Institute, AND Michael O’HANLON, senior fellow and Chair in foreign policy studies at Brookings, 7 [April 2007, “The Case for Larger Ground Forces,” http://www.aei.org/files/2007/04/24/20070424\_Kagan20070424.pdf]

We live at a time when wars not only rage in nearly every region but threaten to erupt in many places where the current relative calm is tenuous. To view this as a strategic military challenge for the United States is not to espouse a specific theory of America’s role in the world or a certain political philosophy. Such an assessment flows directly from the basic bipartisan view of American foreign policy makers since World War II that overseas threats must be countered before they can directly threaten this country’s shores, that the basic stability of the international system is essential to American peace and prosperity, and that no country besides the United States is in a position to lead the way in countering major challenges to the global order.¶ Let us highlight the threats and their consequences with a few concrete examples, emphasizing those that involve key strategic regions of the world such as the Persian Gulf and East Asia, or key potential threats to American security, such as the spread of nuclear weapons and the strengthening of the global Al Qaeda/jihadist movement. The Iranian government has rejected a series of international demands to halt its efforts at enriching uranium and submit to international inspections. What will happen if the US—or Israeli—government becomes convinced that Tehran is on the verge of fielding a nuclear weapon? North Korea, of course, has already done so, and the ripple effects are beginning to spread. Japan’s recent election to supreme power of a leader who has promised to rewrite that country’s constitution to support increased armed forces—and, possibly, even nuclear weapons— may well alter the delicate balance of fear in Northeast Asia fundamentally and rapidly. Also, in the background, at least for now, Sino Taiwanese tensions continue to flare, as do tensions between India and Pakistan, Pakistan and Afghanistan, Venezuela and the United States, and so on. Meanwhile, the world’s nonintervention in Darfur troubles consciences from Europe to America’s Bible Belt to its bastions of liberalism, yet with no serious international forces on offer, the bloodletting will probably, tragically, continue unabated.¶ And as bad as things are in Iraq today, they could get worse. What would happen if the key Shiite figure, Ali al Sistani, were to die? If another major attack on the scale of the Golden Mosque bombing hit either side (or, perhaps, both sides at the same time)? Such deterioration might convince many Americans that the war there truly was lost—but the costs of reaching such a conclusion would be enormous. Afghanistan is somewhat more stable for the moment, although a major Taliban offensive appears to be in the offing.¶ Sound US grand strategy must proceed from the recognition that, over the next few years and decades, the world is going to be a very unsettled and quite dangerous place, with Al Qaeda and its associated groups as a subset of a much larger set of worries. The only serious response to this international environment is to develop armed forces capable of protecting America’s vital interests throughout this dangerous time. Doing so requires a military capable of a wide range of missions—including not only deterrence of great power conflict in dealing with potential hotspots in Korea, the Taiwan Strait, and the Persian Gulf but also associated with a variety of Special Forces activities and stabilization operations. For today’s US military, which already excels at high technology and is increasingly focused on re-learning the lost art of counterinsurgency, this is first and foremost a question of finding the resources to field a large-enough standing Army and Marine Corps to handle personnel intensive missions such as the ones now under way in Iraq and Afghanistan.¶ Let us hope there will be no such large-scale missions for a while. But preparing for the possibility, while doing whatever we can at this late hour to relieve the pressure on our soldiers and Marines in ongoing operations, is prudent. At worst, the only potential downside to a major program to strengthen the military is the possibility of spending a bit too much money. Recent history shows no link between having a larger military and its overuse; indeed, Ronald Reagan’s time in office was characterized by higher defense budgets and yet much less use of the military, an outcome for which we can hope in the coming years, but hardly guarantee. While the authors disagree between ourselves about proper increases in the size and cost of the military (with O’Hanlon preferring to hold defense to roughly 4 percent of GDP and seeing ground forces increase by a total of perhaps 100,000, and Kagan willing to devote at least 5 percent of GDP to defense as in the Reagan years and increase the Army by at least 250,000), we agree on the need to start expanding ground force capabilities by at least 25,000 a year immediately. Such a measure is not only prudent, it is also badly overdue.

#### Military controls of all aspects of cyber security, from monitoring pranks, to crafting offensive operations. Separating out roles is key to effective policy

Interview with Emanuel Pastreich, director of the Asia Institute, and Peter W. SINGER, the director of the Center for 21st Century Security and Intelligence and a senior fellow in the Foreign Policy program at Brookings, 14 [January 13, 2014, “The State, the Internet and Cybersecurity,” http://www.brookings.edu/research/interviews/2014/01/13-the-state-the-internet-and-cybersecurity-singer]

Pastreich: “So, in cyberspace, is there a posse comitatus?” ¶ Singer: “Well, no, there is not. There remain a series of issues that we need to work out. When I say ‘we’ I am talking about communities at every level, from the global down to the national, regional, and individual. We need to think about how agencies and corporations can be made accountable and responsible, but also about what we can do as citizens. For example, what exactly do we mean as a community, as a nation, by ‘cyber war?’ And, in turn, who should we expect to fight it? ¶ “One challenge that we find in this debate that we want to unpack for readers is the wide variety of dissimilar threats that we often bundle together as cyber threats simply because they all take place in cyberspace. For example, one senior Pentagon official cited an enormous number of cyber attacks on the Pentagon when he testified to Congress. The problem was that what he spoke of an “attack” the congressmen listening imagined some existential ‘cyber Pearl Harbor’ or ‘cyber 9-11.’ After all, that is what the secretary of defense had been discussing in various closed hearings. Yet, what the Pentagon official was talking about with these numbers instead was a hodgepodge ranging from attempts at address scans or ‘knocks,’ defamation (i.e., pranks such as changing external user-face websites), espionage (i.e., stealing secrets), and some more aggressive attempts to compromise security. ¶ “That Pentagon official was bundling together everything from the equivalent of a teenage prankster with a firecracker, to a pistol-robber, a terrorist with a roadside bomb, a spy with a hidden gun, and a military armed with a cruise-missile. He was giving the impression that all these ‘attacks’ were basically similar because they all use the technology of cyberspace. But the only similarity between a firecracker and a cruise missile is the use of the technology of explosive materials. Such discussions are not a responsible way to keep the public informed about a critical issue. ¶ “What we need to do is to disentangle our thinking about the nature of the threats and in turn that will allow us to disentangle our thinking about appropriate responses. For example, the US Military Cyber Command and its partner the National Security Agency have taken on a wide range of roles largely because of an overwhelming fear of what cyber attacks could be and also the fact that other agencies lack skill and the budget capacity. They are handling issues, as a result, that frankly are not appropriate to their mandate. ‘Appropriate’ here means in a strategic and organizational sense, and also in a legal sense. ¶ “Think of it this way: Let’s imagine two banks were transferring money between them and one of their trucks was blocked in the street by a group of protesters. Well, no one would say, ‘call in the Army! It is the Army’s responsibility!’ And yet that is how we often react if the issue involves electronic transfers. We have to get over that kind of thinking. This is also huge to the concerns of IP theft and US-China tensions that result from it. It is critical that we disentangle certain subtle but important differences between a ‘9-11’ threat and a ‘death by a thousand cuts.’”

#### Limiting exceptions the Posse Comitatus renews separation between civilian and military enforcement

Matthew HAMMOND, attorney in the U.S. D.O.J., 1997 [“The Posse Comitatus Act: A Principle in Need of Renewal,” *Washington University Law Review*, Volume 75, Issue 2, 75 Wash. U. L. Q. 953, Lexis]

In response to the military presence in the Southern States during the Reconstruction Era, Congress passed the Posse Comitatus Act' ("PCA" or the "Act") to prohibit the use of the Army in civilian law enforcement. The Act embodies the traditional American principle of separating civilian and military authority and currently forbids the use of the Army and Air Force to enforce civilian laws.2 In the last fifteen years, Congress has deliberately eroded this principle by involving the military in drug interdiction at our borders This erosion will continue unless Congress renews the PCA's principle to preserve the necessary and traditional separation of civilian and military authority.¶ The need for reaffirmation of the PCA's principle is increasing because in recent years, Congress and the public have seen the military as a panacea for domestic problems.4 Within one week of the bombing of the federal building in Oklahoma City,' President Clinton proposed an exception to the PCA to allow the military to aid civilian authorities in investigations involving "weapons of mass destruction. ' In addition to this proposal Congress also considered legislation to directly involve federal troops in enforcing customs and immigration laws at the border.7 In the 1996 presidential campaign, candidate Bob Dole pledged to increase the role of the military in the drug war, and candidate Lamar Alexander even proposed replacing the Immigration and Naturalization Service and the Border Patrol with a new branch of the armed forces.'¶ The growing haste and ease with which the military is considered a panacea for domestic problems will quickly undermine the PCA if it remains unchecked. Minor exceptions to the PCA can quickly expand to become major exceptions. For example in 1981, Congress created an exception to the PCA to allow military involvement in drug interdiction at our borders.9 Then in 1989, Congress designated the Department of Defense as the "single lead agency" in drug interdiction efforts.'¶ The PCA criminalizes, effectively prohibiting, the use of the Army or the Air Force as a posse comitatus" to execute the laws of the United States. It reads:¶ Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.'2¶ Though a criminal law, the PCA has a more important role as a statement of policy that embodies "the traditional Anglo-American principle of separation of military and civilian spheres of authority, one of the fundamental precepts of our form of government."' 3¶ Major and minor exceptions to the PCA, which allow the use of the military in law enforcement roles, blur the line between military and civilian roles, undermine civilian control of the military, damage military readiness, and inefficiently solve the problems that they supposedly address.'4 Additionally, increasing the role of the military would strengthen the federal law enforcement apparatus that is currently under close scrutiny for overreaching its authority. 5 Although it seems benign, such an increase in military authority revives fears of past overreaching during the late 1960s.16¶ This Note argues that the principle embodied by the PCA should be renewed by rejecting exceptions to the Act and reaffirming the policy behind its inception. This renewal is necessary to preserve the historic division between civilian and military roles, to maintain civilian superiority over the military, to enhance military readiness, and to efficiently attack domestic problems. Part II reviews the historical traditional American fear of a standing army and the circumstances leading to the PCA's passage. Part III discusses the current scope of the PCA and the permissible roles of the military. Part IV explains how exceptions to the PCA endanger its underlying principle. The explanation covers the spectrum of possible exceptions to the PCA: drug interdiction, border duty, and biological and chemical weapons investigations. 7 Part V proposes legislative action to reaffirm the policy of the PCA and to limit to any further exceptions to it.¶

#### Third Amendment restrictions make unilateral offensive cyber operations unconstitutional. OCO’s “quarter” viruses in private networks and computers

Alan BUTLER, Appellate Advocacy Counsel, Electronic Privacy Information Center (EPIC); J.D. UCLA School of Law, 13 [June, 2013, “When Cyberweapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy,” American University Law Review, 62 Am. U.L. Rev. 1203, Lexis]

III. Applying the Third Amendment to Military Cyberoperations¶ The Third Amendment prohibitions govern military intrusions onto private property. Cyberoperations can affect private computers and networks, including innocent third-party systems. n169 As the U.S. military develops its strategy and begins to conduct cyberoperations, its actions affecting domestic systems must comply with Third Amendment principles.¶ Each category of cyberoperations has the potential to affect private systems in the United States. The use of a self-replicating virus or worm, such as Stuxnet, can result in widespread infection beyond the intended military target. Even more targeted cyberexploits, such as Flame or Red October, use intermediate networks and devices to gain access to their targets. Additionally, a retaliatory strike or hack-back may harm an innocent third-party system rather than the actual attacker. The Third Amendment governs all of these situations if the affected system belongs to someone under U.S. jurisdiction.¶ To determine whether the Third Amendment prohibits a given military cyberoperation, the relevant inquiry would be: (1) is the computer or network device property protected as part of "any house," and (2) does the military intrusion constitute "quartering" by a "Soldier"? If the network or device is protected, and the military intrusion constitutes quartering, then consent is required under the Third Amendment during times of peace and a formal legal enactment is required during times of war. [\*1228]¶ A. The Private Property Protected by the Third Amendment Includes Computer and Network Infrastructure¶ The first issue relevant to the Third Amendment analysis of military cyberoperations is whether civilian computers and networks are protected. The Third Amendment prohibits quartering "in any house." n170 This provision could be interpreted as protecting only residential buildings, as opposed to the "persons, houses, papers, and effects" protected by the Fourth Amendment. n171 However, the history of the Third Amendment indicates that it governs "quartering" on excludable private property generally, regardless of the specific structure or parcel used. n172 In respecting the "Owner['s]" right to exclude, the scope of the Third Amendment may in fact be broader than the Fourth Amendment. n173 The only federal court to fully analyze and apply the Third Amendment in a modern context took a similarly broad view of the protected property right. n174¶ The history surrounding the ratification of the Third Amendment also suggests that a broad view is appropriate. The English quartering statutes traditionally provided for quartering in "public houses" during wartime, n175 including the 1765 provision governing quartering in the Colonies. n176 These statutes specifically listed the types of structures that could be used for quartering. n177 This was even true of the Quartering Act of 1774, one of the "intolerable acts" that [\*1229] revolutionary colonists cited in the lead up to the war. n178 Notably, British soldiers "were not quartered in private colonial houses" during the pre-revolutionary period. n179 When the Third Amendment was enacted, however, Congress rejected an alternative proposal that would have allowed billeting of soldiers in public houses and inns. n180 Rather than provide specific rules based on the classification of property, Congress adopted a general prohibition governing "any house." n181¶ The Second Circuit adopted a broad view of the Third Amendment's property protections in Engblom. n182 There, the court analyzed the Third Amendment's application based on its role in assuring "a fundamental right to privacy," as noted by the Supreme Court in Griswold. n183 The Second Circuit rejected a rigid application of the term "Owner" because it "would be wholly anomalous when viewed, for example, alongside established Fourth Amendment doctrine" that protects tenants. n184 The court ultimately held that the Third Amendment's property-based privacy interests are not limited only to those "Owners" who possess a fee simple ownership of their residence but instead protect citizens who lawfully occupy or possess a residence. n185¶ In a more recent case, Custer County Action Ass'n v. Garvey, n186 the U.S. Court of Appeals for the Tenth Circuit rejected a claim under the Third Amendment based on the military use of airspace over a plaintiff's home. n187 The court reviewed the claim under the Engblom framework and found that the plaintiffs had no general right to exclude planes traversing the airspace over their property. n188 The Supreme Court had reached a similar conclusion under the Fifth [\*1230] Amendment Takings Clause years earlier in United States v. Causby. n189 Thus, the Tenth Circuit followed a similar analysis of the Third Amendment where "any home" was defined as a property area in which an individual has a right to exclude others. n190¶ When framed as a right to exclude the military from private property, it is clear that computers, networks, and other systems fall within the scope of the Third Amendment. The phrase "any house" encompasses all forms of property that fit within the typical paradigm. Rather than include or exclude certain types of property, the Framers opted for broad language. n191 Civilian networked devices will necessarily fall within this category because they are maintained within, and are a component of, private property. Hacking is analogous to a trespass, n192 and typical home and corporate systems can also rightfully be classified as private property. n193 Invasion of these systems is prohibited by comprehensive federal laws that recognize this general right to exclude. n194 [\*1231]¶ B. Military Software Placed on a Home or Business Network or Computer Device Is "Quartered" for Third Amendment Purposes¶ Having established that the Third Amendment protects private networks and computer systems, it is necessary to consider whether military cyberoperations can be "quartered" on these systems. While the conclusion that a military cyberoperation constitutes quartering in a system would be a novel application of the quartering provision, n195 it would be consistent with the purposes and principles underlying the Third Amendment. There are at least two interpretive hurdles relevant to this inquiry: (1) whether computer software and files can be "quartered" at all, and (2) whether these elements are indeed an extension of the regulated "Soldier" used in the Third Amendment. The language can be reasonably interpreted to apply to certain military cyberoperations, especially given the underlying concern of the Third Amendment: that military personnel will cause harm to civilians by imposing on their private property. n196¶ As it relates to the first hurdle, cyberoperations may constitute quartering because they involve trespassing into and placing files on a private system. The long history of quartering was focused primarily on the provision of lodging to members of the military. n197 The modern usage of the term "quarter," - to "lodge, or dwell," n198 - generally matches the traditional definition of "quarter" at the time [\*1232] of the framing - "to lodge; to fix on a temporary dwelling." n199 Furthermore, the modern definition of "to lodge" - "to provide temporary quarters for" or "to establish or settle in a place" n200 - also tracks the traditional definition of "to lodge" - "to place in a temporary habitation" or "to afford place to." n201 At a minimum, it is clear that the quartering concept encompasses "something less than a permanent occupation." n202 It is unclear whether any mere trespass would suffice, or whether there must be some extended use of the private property to constitute quartering. n203¶ Given the definition and purpose of the quartering provision, it is likely that cyberoperations could constitute quartering to the extent that they involve intruding into and placing files on a private system. These files can cause damage and impose costs on the "Owners" similar to the "Soldiers" quartered in a traditional Third Amendment case.¶ The second issue involves whether these cyberoperations fall within the Third Amendment because they are carried out by "Soldiers." The problem of applying the traditional legal principles of warfare to the cyberspace domain is not a new one. A great deal of recent scholarship has focused on the application of international law in cyberspace. n204 While the analysis of cyberattacks under customary international law and the law of war focus on the use of physical force, the military attribution of these operations is a baseline assumption of all the analysis. n205 The term cyberoperations is used throughout a forthcoming cyberwar manual to refer to the "employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace." n206 Cyberoperations are military operations to the extent that USCYBERCOM is executing or coordinating the operations. [\*1233] Consequently, the Third Amendment governs a cyberoperation's invasion of private property.¶ This view is consistent with both a broad reading of the anti-quartering right in English cases as well as the Second Circuit's holding in Engblom. n207 There is English common law, for example, related to the quartering of horses in "actual service." n208 The horses were merely an instrumentality of war used by the soldiers, but they were considered quartered at common law. n209 Similarly, in Engblom, the Second Circuit held that the National Guardsmen were considered "Soldiers" within the meaning of the Third Amendment because they were "state employees under the control of the Governor." n210 The degree of military "control" was key in both cases. n211¶ Under this analysis, quartering of "Soldiers" in private computer systems occurs when military operators directly or indirectly employ files or software that accesses and places itself upon a private system. Typically, a C&C server will direct cyberoperations that another group is responsible for configuring. n212 In the case of an active defense system, a remote or local system could also control the operation. n213 Regardless, USCYBERCOM closely controls and manages any cyberoperation that the United States currently undertakes. n214 [\*1234]¶

#### Erosion of posse comitatus erodes civilian control of the military which guarantees escalation of all minor conflicts

Matthew HAMMOND, attorney in the U.S. D.O.J., 1997 [“The Posse Comitatus Act: A Principle in Need of Renewal,” *Washington University Law Review*, Volume 75, Issue 2, 75 Wash. U. L. Q. 953, Lexis]

The differences in the role of civil law enforcement and the role of the military are blurred by the PCA's exceptions. Civilian law enforcement is traditionally local in character, responding to needs at the city, county, or state level. Civilian law enforcement trains for the law enforcement mission, which differs from the military mission. n151 Civilian law enforcement requires the cognizance of individual rights and seeks to protect those rights, even if the person being protected is a bad actor. Prior to the use of force, police officers attempt to de-escalate a situation. Police officers are trained to use lesser forms of force when possible to draw their weapons only when they are prepared to fire.¶ On the other hand, soldiers are trained when to use or not to use deadly force. n152 Escalation is the rule. The military exists to carry out the external mission of defending the nation. Thus, in an encounter with a person identified with the enemy, soldiers need not be cognizant of individual rights, and the use of deadly force is authorized without any aggressive or bad act by that person. n153 This difference between soldiers and police has been tragically illustrated in the recent shooting of a young man by marines patrolling near the Mexican border. n154¶ The exceptions of border duty, investigative support, and drug interdiction blur the traditional line between civilian law enforcement and the role of the [\*974] military. Border duty by soldiers under the Border Integrity Act has traditionally been the responsibility of civilian law enforcement. Drug interdiction has traditionally been a task for civilian law enforcement, and long-term military involvement comes close to subjecting civilians to all three types of military power - a fear of the Founding Fathers. n155 Investigative support by the military is very reminiscent of the military surveillance conducted in the 1960s, which was condemned by Congress and members of the Supreme Court as an improper use of the military. n156¶ B. Undermining Civilian Control of the Military¶ Civilian control of the military is undermined whenever military activities invade areas that "endanger liberties or the democratic process, even when that expansion is sanctioned by the civilian leadership." n157 The military should not gain "unwarranted influence" in civilian affairs. n158 The purpose of civilian control is "to ensure that defense policy and the agencies of defense policy are subordinated to other national traditions, values, customs, governmental policies, and economic and social institutions." n159 The civilian government must therefore consider the institutional characteristics of the military, including personnel, doctrine, training, equipment, and morale, when making policy decisions about the domestic use of the military. n160 A military with many nonmilitary functions is more "autonomous" and thus under less civilian control. n161¶ In the case of counter-drug activities, the government has disregarded all these considerations. The counter-drug mission is not a good fit for the military: the chronic nature of the drug problem requires the military's deep [\*975] involvement over time without any true success n162 because the high profitability of drug trafficking makes its complete deterrence impossible. n163 This involvement without success hurts morale, n164 and the long-term nature of the involvement cannot help but increase the "unwarranted influence" of the military in civilian affairs. n165¶ Both border duty and investigative support, if enacted, would create the same concerns as the counter-drug mission. Increasing the involvement of the military in civilian law enforcement will make it difficult to maintain the military's subordinate role over the long-term. Additionally, use of the military in civilian law enforcement damages its professionalism, which the PCA's enactment helped to develop. Many of these same concerns underlay the government's reluctance to send the military abroad without clear criteria and timelines for withdrawal, n166 yet those concerns have been ignored in [\*976] domestic military use.

#### The impact is global warfare

Eliot A. COHEN, Professor of Strategic Studies at the Paul H. Nitze School of Advanced International Studies at Johns Hopkins, 2 [“Civil-Military Relations,” *America the Vulnerable: Our Military Problems and How To Fix Them*, Edited by John Lehman and Harvey Sicherman, Foreign Policy Research Institute, http://www.fpri.org/americavulnerable/06.CivilMilitaryRelations.Cohen.pdf]

Left uncorrected, the trends in American civil-military relations could breed certain pathologies. The most serious possibility is that of a dramatic civil-military split during a crisis involving the use of force. In the recent past, such tensions did not result in open division. For example, Franklin Roosevelt insisted that the United States invade North Africa in 1942, though the chiefs of both the army and the navy vigorously opposed such a course, favoring instead a buildup in England and an invasion of the continent in 1943. Back then it was inconceivable that a senior military officer would leak word of such a split to the media, where it would have reverberated loudly and destructively. To be sure, from time to time individual officers broke the vow of professional silence to protest a course of action, but in these isolated cases the officers paid the accepted price of termination of their careers.¶ In the modern environment, such cases might no longer be isolated. Thus, presidents might try to shape U.S. strategy so that it complies with military opinion, and rarely in the annals of statecraft has military opinion alone been an adequate guide to sound foreign policy choices. Had Lincoln followed the advice of his senior military advisers there is a good chance that the Union would have fallen. Had Roosevelt deferred to General George C. Marshall and Admiral Ernest J. King there might well have been a gory debacle on the shores of France in 1943. Had Harry S. Truman heeded the advice of his theater commander in the Far East (and it should be remembered that the Joint Chiefs generally counseled support of the man on the spot) there might have been a third world war.¶ Throughout much of its history, the U.S. military was remarkably politicized by contemporary standards. One commander of the army, Winfield Scott, even ran for president while in uniform, and others (Leonard Wood, for example) have made no secret of their political views and aspirations. But until 1940, and with the exception of periods of outright warfare, the military was a negligible force in American life, and America was not a central force in international politics. That has changed. Despite the near halving of the defense budget from its high in the 1980s, it remains a significant portion of the federal budget, and the military continues to employ millions of Americans. More important, civil-military relations in the United States now no longer affect merely the closet-room politics of Washington, but the relations of countries around the world. American choices about the use of force, the shrewdness of American strategy, the soundness of American tactics, and the will of American leaders have global consequences. What might have been petty squabbles in bygone years are now magnified into quarrels of a far larger scale, and conceivably with far more grievous consequences. To ignore the problem would neglect one of the cardinal purposes of the federal government: “to provide for the common defense” in a world in which security cannot be taken for granted.¶

### Plan

#### The United States federal government should restrict the war powers authority of the President of the United States to conduct offensive cyber operations on the grounds that offensive cyber operations violate the Third Amendment.

# 2AC

## Solvency

### 2AC Circumvention

#### Congressional opposition to the authority curbs Presidential action—robust statistical and empirical proof

KRINER 10 Assistant professor of political science at Boston University [Douglas L. Kriner, “After the Rubicon: Congress, Presidents, and the Politics of Waging War”, page 228-231]

Conclusion

The sequence of events leading up to the sudden reversal of administration policy and the dramatic withdrawal of U.S. Marines from Lebanon clearly demonstrates that open congressional opposition to Reagan's conduct of the mission in Beirut was critically important in precipitating the change in course. By tracing the pathways of congressional in- fluence, the case study achieves two important objectives. First, it vividly illustrates Congress's capacity to influence the scope and duration of a use of force independent of major shifts in public opinion and changing conditions on the ground. The analysis makes clear that there was no dramatic shift in public opinion after the Beirut barracks bombing that compelled the Reagan administration to withdraw the Marines; in fact, in the wake of the attack the public rallied behind the president. As such, opponents of Reagan's policies in Congress initially fought against the tide of public opinion, and the modest decline in popular support for the president's handling of the Lebanon mission occurred only after a sustained campaign against the deployment on Capitol Hilt.89 Similarly, the administration's own internal analysis of the situation in early January 1984 makes clear that changing conditions on the ground did not necessitate a dramatic change in the nature of the Marine mission. Indeed, by the National Security Council's own estimate, some conditions in the region were actually improving. Instead, administration officials repeatedly emphasized domestic pressures to curtail the scope and duration of the Marine mission.90 Moreover, as the political and military situation in Lebanon worsened in late January and early February 1984, it is interesting that a number of key administration officials publicly and privately believed that there was a direct link between congressional opposition at home and the deterioration of the situation on the ground in the Middle East.

Second, the case study illustrates how the formal and informal congressional actions examined in the statistical analyses of chapter 4 affected presidential decision-making through the proposed theoretical mechanisms for congressional influence over presidential conduct of military affairs developed in chapter 2. Vocal opposition to the president in Congress-expressed through hearings and legislative initiatives to curtail presidential authority, and the visible defection from the White House of a number of prominent Republicans and erstwhile Democratic allies-raised the political stakes of staying the course in Lebanon. Nothing shook Reagan's basic belief in the benefits to be gained from a strong, defiant stand in Beirut. But the political pressure generated by congressional opposition to his policies on both sides of the aisle raised the likely political costs of obtaining these policy benefits. Congressional opposition also influenced the Reagan administration's decision-making indirectly by affecting its estimate of the military costs that would have to be paid to achieve American objectives. In the final analysis, through both the domestic political costs and signaling mechanisms discussed in chapter 2 , congressional opposition contributed to the administration's ultimate judgment that the benefits the United States might reap by continuing the Marine mission no longer outweighed the heightened political and military costs necessary to obtain them.

Finally, while the Marine mission in Lebanon is admittedly but one case, it is a case that many in the Reagan administration believed had important implications for subsequent military policymaking. In a postmortem review, Don Fortier of the National Security Council and Steve Sestanovich at the State Department warned that the debacle in Lebanon raised the possibility that, in the future, the decision to use force might be akin to an all-or-nothing decision. "If the public and Congress reject any prolonged U.S. role (even when the number of troops is small)," the administration analysts lamented, "we will always be under pressure to resolve problems through briefer, but more massive involvements-or to do nothing at all." Thus, from the administration's "conspicuously losing to the Congress" over Lebanon policy, Fortier and Sestanovich argued that the White House would have to anticipate costly congressional opposition if similar actions were launched in the future and adjust its conduct of military operations accordingly, with the end result being a "narrowing of options" on the table and more "limited flexibility" when deploying major contingents of American military might abroad.91 This last point echoes the first anticipatory mechanism posited in chapter 2, and reminds us that Congress need not overtly act to rein in a military action of which it disapproves for it to have an important influence on the scope and duration of a major military endeavor. Rather, presidents, having observed Congress's capacity to raise the political and tangible costs of a given course of military action, may anticipate the likelihood of congressional opposition and adjust their conduct of military operations accordingly.

## T

### 2AC T

#### OCO’s include spying and info-gathering

Alan BUTLER, Appellate Advocacy Counsel, Electronic Privacy Information Center (EPIC); J.D. UCLA School of Law, 13 [June, 2013, “When Cyberweapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy,” American University Law Review, 62 Am. U.L. Rev. 1203, Lexis]

Offensive cyberoperations include "actions taken against an adversary's computer systems or networks that harm the adversary's interests." n55 Many military cyberoperations are not intended to cause physical destruction. n56 For example, cyberexploitations are used to facilitate quiet and undetectable information-gathering. n57 These operations take advantage of the same vulnerabilities and access [\*1213] paths as targeted cyberattacks. n58 The viruses used in cyberexploits can infect computers and systems across the globe, and these viruses can remain dormant for years without detection. n59 Recently uncovered cyberexploitation attacks used sophisticated malware to gather troves of confidential data from a broad range of computers and devices. n60

#### Counter-interp---war powers authority is OVERALL power over war-making---we meet

Manget 91 Fred F, Assistant General Counsel with the CIA, "Presidential War Powers", 1991, media.nara.gov/dc-metro/rg-263/6922330/Box-10-114-7/263-a1-27-box-10-114-7.pdf

The President's war powers authority is actually a national defense power that exists at all times, whether or not there is a war declared by Congress, an armed conflict, or any other hostilities or fighting. In a recent case the Supreme Court upheld the revocation of the passport of a former CIA employee (Agee) and rejected his contention that certain statements of Executive Branch policy were entitled to diminished weight because they concerned the powers of the Executive in wartime. The Court stated: "History eloquently attests that grave problems of national security and foreign policy are by no means limited to times of formally declared war. " 3 ; Another court has said that the war power is not confined to actual engagements on fields of battle only but embraces every aspect of national defense and comprehends everything required to wage war successfully. 3 H A third court stated: "It is-and must be-true that the Executive should be accorded wide and normally unassailable discretion with respect to the conduct of the national defense and the prosecution of national objectives through military means . "39

Thus, the Executive Branch's constitutional war powers authority does not spring into existence when Congress declares war, nor is it dependent on there being hostilities. It empowers the President to prepare for war as well as wage it, in the broadest sense. It operates at all times.

#### Counter-interp---authority means legality

Ellen Taylor 96, 21 Del. J. Corp. L. 870 (1996), Hein Online

The term authority is commonly thought of in the context of the law of agency, and the Restatement (Second) of Agency defines both power and authority.'89 Power refers to an agent's ability or capacity to produce a change in a legal relation (whether or not the principal approves of the change), and authority refers to the power given (permission granted) to the agent by the principal to affect the legal relations of the principal; the distinction is between what the agent can do and what the agent may do.

#### Prefer our interpretation—

#### Aff ground—all OCOs the US does are pre-emptive. There is no distinction.

#### Plan says OCO—text determines topicality.

#### Good is good enough. Alternatives trade off with substance, trigger a race to the most limiting interpretation, and exceed the jurisdictional role of the judge.

#### Err aff on T

#### Very limited number of CYBER affs have been read means aff innovation outweighs. Anything that isn’t an aff read at GSU but is reasonably topical should be rewarded, not excluded.

#### We read a plan—given the status quo of debate, the threshold for T should be high because the alternative incentives LESS aff innovation and NOT reading a plan, which internal link turns all their T offense.

## Russ DA

#### Snowden

**Stokes 12/5**/13 - Director of global economic attitudes at the Pew Research Center [Bruce Stokes “NSA Spying: A Threat to US Interests?,” YaleGlobal, 5 December 2013, pg. http://yaleglobal.yale.edu/content/nsa-spying-threat-us-interests

WASHINGTON: Revelations by Edward Snowden of US National Security Agency spying have exposed both similarities and differences in public attitudes toward privacy among Europeans and Americans. Both publics value privacy, but Americans, more so than most Europeans, appear willing to sacrifice privacy in the name of security. These differences pose potential challenges to the ongoing free trade discussions between the European Union and the United States, the Transatlantic Trade and Investment Partnership, where new rules governing the digital economy could prove central to a final agreement. ¶ Americans have conflicting views about NSA activities done in their name. They suggest that the National Security Agency may have gone too far in spying on US allies. They also think that the NSA has intruded on Americans' personal privacy in scooping up massive amounts of private phone calls and emails. But, in the pursuit of terrorists, a majority will still trade their personal privacy for greater security.¶ Such differences have raised new doubts in Europe about the United States. German Chancellor Angela Merkel recently told members of the German parliament that US spying “must be explained and more importantly new trust must be built up for the future.” And, while it’s too early to know the lasting impact of the Snowden affair on transatlantic relations, Europeans’ perceptions of the United States, especially as a stalwart defender of individual freedom, may face new strains.¶ A recent survey by the Pew Research Center found that 56 percent of Americans said it is unacceptable for the United States to monitor the phone calls of the leaders of allied nations, including Merkel. Just 36 percent said it is a tolerable practice.¶ American wariness of NSA activities may, in part, reflect concern about a possible invasion of their own privacy. In a mid-July Washington Post-ABC News survey, 49 percent said they thought that the NSA surveillance program intruded on their personal privacy rights. And 74 percent said it infringed on some Americans' privacy, if not their own.¶ Nevertheless, when asked to balance security worries against privacy concerns, Americans opt for security. In that same Washington Post-ABC News poll, 57 percent felt that it was important for the federal government to investigate terrorist threats, even if it intrudes on personal freedom. Just 39 percent said that the government should not intrude on personal privacy, even if it limits the government’s ability to investigate possible terrorist threats.¶ There has been little cross-national polling of European views on the NSA affair. And the questions are often worded differently or conducted with differing methodologies, so that comparisons between polling findings are more illustrative than definitive. But what has been done suggests notable differences with American viewpoints and some broad similarities.¶ Like Americans, Europeans appear to be worried about personal privacy. They do not think that national security concerns warrant an invasion of their privacy. Majorities in Germany (70 percent), France (52 percent) and Sweden (52 percent) think that their own government would not be justified in collecting the telephone and internet data of its citizens as part an effort to protect national security, according to a survey done by TNS Opinion for the German Marshall Fund of the United States. A substantial minority, or 44 percent, of people in the United Kingdom agree. In this survey, 54 percent of Americans surveyed suggested that such activity would go too far in violating citizens' privacy and is therefore not justified.¶ Another difference emerged in this survey between American and European attitudes toward spying on one’s allies. Publics on both sides of the Atlantic think national security is no justification for action, but it’s a sentiment held more strongly by some Europeans than by Americans. A strong majority of Germans (72 percent) and more than half the French and the Swedes (each 55 percent) did not think that national governments are justified in collecting telephone and internet data of citizens in other allied countries even as part of an effort to protect national security, according to the TNS/GMF survey. More British, 43 percent, thought it was unjustified than saw it as justified, 30 percent. Notably, American attitudes resembled those of the British – 44 percent unjustified, 33 percent justified.¶ The exposure of NSA spying has had an impact on America's image abroad, especially in Europe.¶ In spring 2013, before extensive revelations of NSA activities, a median of 62 percent in five European Union nations – Britain, France, Germany, Poland and Spain – had a favorable view of the United States, according to a Pew Research Center survey. That included 76 percent for Italians, 64 percent for the French and 53 percent for Germans.¶ That median was already in decline, down from 67 percent in 2009. It’s unclear whether the NSA affair will accelerate that erosion or prove a minor bump in the road in transatlantic relations. But there are some early warning signs. A recent poll by the German public broadcaster, ARD and the German daily Die Welt, found that only 35 percent of Germans consider the US government to be trustworthy.¶ Moreover, the US government's respect for individual liberty has long been a strong suit of American public diplomacy. Even in many nations where opposition to US foreign policy is widespread and where overall ratings for the United States are low, majorities or pluralities maintained that the country respects individual rights.¶ In the 2013 Pew Research Center survey, a median of 70 percent of people in 39 nations thought the United States government respected the personal freedoms of its people. In contrast, a median of only 36 percent saw China protecting individual liberties.¶ This view of America as a resolute defender of civil rights was particularly strong in Europe: Italy (82 percent), Germany (81 percent), France (80 percent) and Spain (69 percent). Positive views of Uncle Sam's record had risen by 20 points in Spain, 15 in France and 11 in Germany since 2008. But these are now the countries where some of the public outcry against NSA spying has been loudest.¶ So Americans are of two minds about recent allegations of NSA surveillance of phone and email communications. They worry about its impact on international relations and their own privacy. But that concern continues to be trumped by an ongoing anxiety about terrorism. Europeans similarly share concerns about spying’s impact on privacy, but they generally do not think national security concerns are more important than privacy.¶ These differences are already playing out in the negotiations over the Transatlantic Trade and Investment Partnership. Some European officials have called for a pause in the talks in response to the Snowden revelations. That is unlikely. But NSA spying has revived European concerns about who owns data generated by individual consumers through their credit card purchases, internet searches and the like – and what private companies can and cannot do with that data. Some European privacy advocates would like to ban the cross-border transfer of such data. But many companies, especially data-intensive American firms like Google and Facebook, and even companies like General Electric, claim that the business model of the new digital economy is built on the ability to amass and analyze large sets of data. They argue that quarantining such information within national borders will deny future generations many of the economic benefits to be gained from big data.¶ The transatlantic disagreement over NSA intrusion into personal privacy is not simply a national security issue, it now has business implications.

#### One policy change will not reverse the course. This is a deep and fundamental rights issue for Europe

**UPI 12/20**/13 [United Press International, “Restoring lost trust may take many years: Germany,” Dec. 20, 2013 at 1:42 PM, pg. http://www.upi.com/Top\_News/Special/2013/12/20/Restoring-lost-trust-may-take-many-years-Germany/UPI-99901387564931/

BERLIN, Dec. 20 (UPI) -- Restoring trans-Atlantic trust lost as a result of spying controversies may take some time to repair, new German Foreign Minister Frank-Walter Steinmeier said as he took over from Guido Westerwelle.¶ "The Transatlantic Alliance is and remains the backbone of our security," Steinmeier said, addressing a Foreign Ministry gathering. But a lot has changed recently and much cannot be taken for granted, he added.¶ "Despite all placations citing the Western community of shared values, trust has been lost and it will require a great deal of joint effort to restore it," he added.¶ "Today we are confronted with the question of how we can reconcile freedom and security in a digitally connected world and in light of new threats that have indeed arisen. We must make it clear to our American friends that not everything that is technically possible is politically wise. And this goes far beyond the question of whether spying among friends is permissible or not.¶ "It also begs the question of how can we ensure that our citizens' fundamental right to privacy remains intact in the 21st century, against a fully transformed communications backdrop. How can we prevent the technical and legal fragmentation of the World Wide Web, on which a large part of our increasing prosperity is based?¶ "This trust will not be regained overnight, but we will work hard to restore it," Steinmeier said.¶ He said the transatlantic relationship "is currently under considerable strain -- Iraq war, Guantanamo, [U.S. secrets leaker Edward] Snowden, NSA [National Security Agency] are the words that come to mind in that context."

#### Obama has already lost all foreign and domestic credibility—saps pol cap

WALT 3—18—14 [Stephen Walt, The Solve-Everything, Do-Nothing White House, http://www.foreignpolicy.com/articles/2014/03/18/the\_solve\_everything\_do\_nothing\_obama\_white\_house]

At the moment, U.S. foreign policy is in considerable disarray, and the vultures are circling the White House. Hawkish critics such as John McCain, Condoleezza Rice, and Niall Ferguson are lambasting Obama for his alleged "weakness" on Ukraine, Syria, Benghazi, or whatever -- even though their main complaint seems to be that he isn't willing to repeat the same costly blunders they either made or supported in the past. Still, the New York Times's David Sanger wonders if Obama's more restrained approach to running the world has reached its limits, and he quotes one former Obama aide saying "we're seeing the 'light footprint' run out of gas." And Tom Friedman thinks Obama can't decide if he's Pollyanna, John Wayne, or Henry Kissinger (as if these are the only options). Contrary to the critical overreaction to Obama in the wake of events in Ukraine, what we are really seeing here is the classic problem of over-commitment -- in this case one that is more diplomatic than military in nature. U.S. officials like to claim they know how to walk and chew gum at the same time -- by which they mean they can handle more than one problem at once -- but trying to do too many things simultaneously leaves no bandwidth for dealing with the unexpected. It also forces top officials to rely heavily on subordinates who may not be good at their assigned tasks. Pursuing multiple objectives without a clear set of priorities also allows opponents to thwart your aims merely by dragging their feet and waiting until Washington is distracted by the next problem. This tactic also forces U.S. leaders to spend more political capital, which in turn leaves them weaker when other issues arise. And when you try to do too many things at once, steps taken to advance your aims in one area may undermine your efforts somewhere else.¶ To see how Obama got here, let's start with a quick look back to the start of his second term. As regular readers know, I didn't think the administration would accomplish much on the foreign-policy front, given the dearth of low-hanging fruit and an unfinished domestic agenda. I thought foreign policy would be a holding action: they'd concentrate on getting Obamacare to work, nurture the economic recovery, try to ease out of Afghanistan, and then hand all those other pesky problems off to Hillary in 2016. ¶ But then John Kerry became secretary of state in January 2013 and decided to get ambitious. He picked up a favorable tailwind when Iran elected a reformist president, and for a time it looked like my original forecast was dead wrong. Suddenly we had a genuine diplomatic process with Iran, active work on a "framework" agreement for Israeli-Palestinian peace, a renewed push for big transatlantic and transpacific trade deals, and Kerry even stumbled his way to a face-saving agreement to destroy Syria's chemical weapons stockpile. If a couple of those initiatives came to fruition, Obama and Kerry would end the second term in a blaze of foreign policy glory. But look what happened instead. The Iran negotiations produced an interim agreement and the administration stared down the predictable opposition from AIPAC and other hardliners, but the process has been slow, the fight has already used up a lot of political capital, and the opponents of a deal haven't gone away. In fact, they've made it clear that any final agreement has to go a very long way to eliminating Iran's enrichment program. (Can you say, "that's a deal-breaker?")¶ And the latest developments in Ukraine won't help. There are a number of serious issues still left to resolve with Iran, our regional allies are deeply wary, and Moscow (which is part of the P5+1) isn't going to do us any favors at this point. By reducing confidence in Obama's judgment, the Ukraine fiasco will also make it harder for him to sell whatever deal the negotiators eventually reach. Capping Iran's nuclear program still makes good strategic sense, but getting to the finish line ain't going to be easy.¶ Similarly, Kerry's energetic shuttle-diplomacy breathed new life into the moribund Israeli-Palestinian peace process, but then the United States quickly repeated the same familiar mistakes, no doubt leading to the same unhappy outcome. Instead of bringing in a fresh team with new ideas, Kerry recycled former AIPAC, WINEP, and Brookings Saban Center honcho Martin Indyk, a man with a proven track record of not reaching a Middle East peace deal. Instead of building on the 2000 Clinton parameters, the 2007 Abbas-Olmert talks, and the 2002/2007 Arab League peace offer, the still-undisclosed framework agreement is rumored to lean heavily in favor of Israel's preferences, most notably on the status of East Jerusalem and the Jordan River Valley. In short, the United States is once again acting as "Israel's lawyer," thereby insuring that this latest effort goes nowhere.¶ To be fair, Kerry has questioned Israel's demand that it be recognized as a "Jewish state," (a new condition that was not part of the previous negotiations), but there is no sign Kerry or Obama are willing to put meaningful pressure on Israeli Prime Minister Benjamin Netanyahu in order to get a workable deal. Furthermore, trying to get a deal with Iran and a two-state deal on Israel-Palestine at the same time was a bridge too far, because it requires taking on the Netanyahu government and the Israel lobby simultaneously -- on two separate issues. Even if you believe AIPAC has less clout than it used to, this would be a daunting task for any American president, even in a second term. And it is not as though these issues are trivial ones for Israel either in light of the turmoil in the rest of the region; any Israeli leader would be certain to work hard to make sure its concerns were satisfied. So why did Obama or Kerry think they could pull off a miracle on both?¶ And all this took time. Meanwhile, the Syrian meat grinder has ground on, repeatedly threatening to drag in the United States. Although Obama wisely chose not to intervene last summer (a position that the American people clearly supported) it was still a major distraction and gave critics something to latch onto whenever they got tired of talking about Benghazi. Then there's Afghanistan, which used to be Bush's failure but which Obama has owned ever since he chose to escalate the war in 2009. Although Afghan President Hamid Karzai's petulant refusal to sign a security agreement has given Obama an easy out, so far the president has refused to take it. Why? Because if the Afghan government collapses too quickly, Obama's entire approach to the war will be discredited.¶ Finally, Obama was blindsided by events in Ukraine, but why the administration didn't see this coming remains a mystery. No matter what Putin says, Yanukovych's ouster was not the result of some deep Western plot, and in many ways Yanukovych deserved to go. But the United States as far from a neutral party in this process, as top U.S. officials -- including Assistant Secretary of State Victoria Nuland and U.S. Ambassador Geoffrey Pyatt -- either took actions or made statements that showed clear support for the demonstrators and a clear U.S. preference for interim Prime Minister Arseniy Yatsenyuk. Unfortunately, they intervened without considering how it might look to Russia, especially after 20 years of NATO expansion, the deployment of missile defenses near the Soviet border, and George W. Bush's 2008 proposal to bring Ukraine and Georgia into NATO. This was geostrategic incompetence of the highest order, but that is what happens when presidents and secretaries of state are too busy with a zillion other things and stop paying attention to what their ideologically driven subordinates are up to. ¶ So now the United States and Europe are in a giant kerfuffle with Moscow, which will burn up even more time and make it even harder to get Russian cooperation on Iran, in Syria, or against a rising China. It might all have been avoided had the Clinton, Bush, and Obama administrations not decided that it was America's mission to try to guide as many countries as possible toward some sort of democracy (no matter how flawed) and some sort of pro-Western political alignment, even when other powers had reason to view this as a threat. In the meantime, movement towards the two big-trade deals has stalled, Congress and the CIA are mud-wrestling over the torture report, and I haven't said anything about territorial disputes in Asia, that missing Malaysian airliner, or the troubling¶

#### Hegemony solves your economy scenario

Mandelbaum 5 (Michael, Professor and Director of the American Foreign Policy Program at Johns Hopkins, The Case for Goliath: How America Acts As the World’s Government in the Twenty-First Century, p. 192-195)

Although the spread of nuclear weapons, with the corresponding increase in the likelihood that a nuclear shot would be fired in anger somewhere in the world, counted as the most serious potential consequence of the abandonment by the United States of its role as the world's government, it was not the only one. In the previous period of American international reticence, the 1920s and 1930s, the global economy suffered serious damage that a more active American role might have mitigated. A twenty-first-century American retreat could have similarly adverse international economic consequences. The economic collapse of the 1930s caused extensive hardship throughout the world and led indirectly to World War II by paving the way for the people who started it to gain power in Germany and Japan. In retrospect, the Great Depression is widely believed to have been caused by a series of errors in public policy that made an economic downturn far worse than it would have been had governments responded to it in appropriate fashion. Since the 1930s, acting on the lessons drawn from that experience by professional economists, governments have taken steps that have helped to prevent a recurrence of the disasters of that decade.' In the face of reduced demand, for example, governments have increased rather than cut spending. Fiscal and monetary crises have evoked rescue efforts rather than a studied indifference based on the assumption that market forces will readily reestablish a desirable economic equilibrium. In contrast to the widespread practice of the 1930s, political authorities now understand that putting up barriers to imports in an attempt to revive domestic production will in fact worsen economic conditions everywhere. Still, a serious, prolonged failure of the international economy, inflicting the kind of hardship the world experienced in the 1930s (which some Asian countries also suffered as a result of their fiscal crises in the 1990s) does not lie beyond the realm of possibility. Market economies remain subject to cyclical downturns, which public policy can limit but has not found a way to eliminate entirely. Markets also have an inherent tendency to form bubbles, excessive values for particular assets, whether seventeenth century Dutch tulips or twentieth century Japanese real estate and Thai currency, that cause economic harm when the bubble bursts and prices plunge. In responding to these events, governments can make errors. They can act too slowly, or fail to implement the proper policies, or implement improper ones. Moreover, the global economy and the national economies that comprise it, like a living organism, change constantly and sometimes rapidly: Capital flows across sovereign borders, for instance, far more rapidly and in much greater volume in the early twenty-first century than ever before. This means that measures that successfully address economic malfunctions at one time may have less effect at another, just as medical science must cope with the appearance of new strains of influenza against which existing vaccines are not effective. Most importantly, since the Great Depression, an active American international economic role has been crucial both in fortifying the conditions for global economic well-being and in coping with the problems that have occurred, especially periodic recessions and currency crises, by applying the lessons of the past. The absence of such a role could weaken those conditions and aggravate those problems. The overall American role in the world since World War II therefore has something in common with the theme of the Frank Capra film It's a Wonderful Life, in which the angel Clarence, played by Henry Travers, shows James Stewart, playing the bank clerk George Bailey, who believes his existence to have been worthless, how life in his small town of Bedford Falls would have unfolded had he never been born. George Bailey learns that people he knows and loves turn out to be far worse off without him. So it is with the United States and its role as the world's government. Without that role, the world very likely would have been in the past, and would become in the future, a less secure and less prosperous place. The abdication by the United States of some or all of the responsibilities for international security that it had come to bear in the first decade of the twenty-first century would deprive the international system of one of its principal safety features, which keeps countries from smashing into each other, as they are historically prone to do. In this sense, a world without America would be the equivalent of a freeway full of cars without brakes. Similarly, should the American government abandon some or all of the ways in which it had, at the dawn of the new century, come to support global economic activity, the world economy would function less effectively and might even suffer a severe and costly breakdown. A world without the United States would in this way resemble a fleet of cars without gasoline.

#### Empirics prove no war.

Miller 1—Morris Miller is an adjunct economics professor at the University of Ottawa [Jan.-Mar, 2001, “Poverty: A Cause of War?” *Peace Magazine*, http://peacemagazine.org/archive/v17n1p08.htm]

Economic Crises?¶ Some scholars have argued that it is not poverty, as such, that contributes to the support for armed conflict, but rather some catalyst, such as an economic crisis. However, a study by Minxin Pei and Ariel Adesnik shows that this hypothesis lacks merit. After studying 93 episodes of economic crisis in 22 countries in Latin American and Asia since World War II, they concluded that much of the conventional thinking about the political impact of economic crisis is wrong:¶ "The severity of economic crisis—as measured in terms of inflation and negative growth—bore no relationship to the collapse of regimes ... or (in democratic states, rarely) to an outbreak of violence... In the cases of dictatorships and semi-democracies, the ruling elites responded to crises by increasing repression (thereby using one form of violence to abort another)."

#### The recession disproves war predictions.

Zakaria 9—Fareed Zakaria is editor of Newsweek. He writes a regular column for Newsweek. He also hosts an international affairs program, which airs Sundays worldwide on CNN. Zakaria was the managing editor of *Foreign Affairs*. He serves on the board of Yale University, The Council on Foreign Relations, The Trilateral Commission, and Shakespeare and Company. He received a B.A. from Yale and a Ph.D. in political science from Harvard. [December 11, 2009, “The Secrets of Stability,” The Daily Beast, http://www.thedailybeast.com/newsweek/2009/12/11/the-secrets-of-stability.html]

One year ago, the world seemed as if it might be coming apart. The global financial system, which had fueled a great expansion of capitalism and trade across the world, was crumbling. All the certainties of the age of globalization—about the virtues of free markets, trade, and technology—were being called into question. Faith in the American model had collapsed. The financial industry had crumbled. Once-roaring emerging markets like China, India, and Brazil were sinking. Worldwide trade was shrinking to a degree not seen since the 1930s.¶ Pundits whose bearishness had been vindicated predicted we were doomed to a long, painful bust, with cascading failures in sector after sector, country after country. In a widely cited essay that appeared in The Atlantic this May, Simon Johnson, former chief economist of the International Monetary Fund, wrote: "The conventional wisdom among the elite is still that the current slump 'cannot be as bad as the Great Depression.' This view is wrong. What we face now could, in fact, be worse than the Great Depression."¶ Others predicted that these economic shocks would lead to political instability and violence in the worst-hit countries. At his confirmation hearing in February, the new U.S. director of national intelligence, Adm. Dennis Blair, cautioned the Senate that "the financial crisis and global recession are likely to produce a wave of economic crises in emerging-market nations over the next year." Hillary Clinton endorsed this grim view. And she was hardly alone. *Foreign Policy* ran a cover story predicting serious unrest in several emerging markets.¶ Of one thing everyone was sure: nothing would ever be the same again. Not the financial industry, not capitalism, not globalization.¶ One year later, how much has the world really changed? Well, Wall Street is home to two fewer investment banks (three, if you count Merrill Lynch). Some regional banks have gone bust. There was some turmoil in Moldova and (entirely unrelated to the financial crisis) in Iran. Severe problems remain, like high unemployment in the West, and we face new problems caused by responses to the crisis—soaring debt and fears of inflation. But overall, things look nothing like they did in the 1930s. The predictions of economic and political collapse have not materialized at all.¶

## K

#### Plan is the focus of the debate. Decide whether the plan is superior to a competitive policy option or the squo. Any other interpretation moots 9 minutes of the 1ac and shifts the focus to unpredictable question begging

#### Prior questions will never be fully settled---must take action even under conditions of uncertainty

Molly Cochran 99, Assistant Professor of International Affairs at Georgia Institute for Technology, “Normative Theory in International Relations”, 1999, pg. 272

To conclude this chapter, while modernist and postmodernist debates continue, while we are still unsure as to what we can legitimately identify as a feminist ethical/political concern, while we still are unclear about the relationship between discourse and experience, it is particularly important for feminists that we proceed with analysis of both the material (institutional and structural) as well as the discursive. This holds not only for feminists, but for all theorists oriented towards the goal of extending further moral inclusion in the present social sciences climate of epistemological uncertainty. Important ethical/political concerns hang in the balance. We cannot afford to wait for the meta-theoretical questions to be conclusively answered. Those answers may be unavailable. Nor can we wait for a credible vision of an alternative institutional order to appear before an emancipatory agenda can be kicked into gear. Nor do we have before us a chicken and egg question of which comes first: sorting out the metatheoretical issues or working out which practices contribute to a credible institutional vision. The two questions can and should be pursued together, and can be via moral imagination. Imagination can help us think beyond discursive and material conditions which limit us, by pushing the boundaries of those limitations in thought and examining what yields. In this respect, I believe international ethics as pragmatic critique can be a useful ally to feminist and normative theorists generally.¶

#### Perm do the plan and adopt a pacifist analysis that injects moral and epistemic doubt into our decisionmaking about war

#### Link ev is about drones—high tech violence now w/ cyber preemption—aff link turns impact

#### We don’t make certain calculations about war—say US irrationality now is unrestrained violence—that’s the whole preemption advantage

### Cyber war real

#### Even if our solution isn't perfect, the 1ac is a step in the right direction—individual acknowledgement of our agency in cyber security discussions is a critical pre-requisite the re-shaping the terrain of cyber policy

Ronald J. DEIBERT, professor of political science and director of the Canada Centre for Global Security Studies at the Munk School of Global Affairs, University of Toronto, 13 [“Bounding Cyber Power: Escalation and Restraint in Global Cyberspace,” Internet Government Papers, Paper No. 6, October 2013]

Looking toward the near term in cyberspace governance, there are many possible scenarios, with unforeseen contingencies taking us down any number of paths. At the same time, politics and society are not entirely chaotic: social order is shaped by underlying forces that set the tempo and framework within which life unfolds. Today, these forces appear to be driving securitization processes in cyberspace, processes that may end up subverting the domain entirely, possibly leading to system wide instability and perhaps even international violence. It is imperative that we use our agency to check and constrain the least desirable elements of these trends and shape those structures that provide the framework for what is seen as legitimate or not. Doing so will require a clear vision and a strategy to implement it, which in turn will require coordinated work at multiple levels and involve a wide variety of stakeholders. The obstacles standing in the way of realizing this vision are certainly formidable, but the alternatives to doing nothing are dire. The securitization of cyberspace may be inevitable, but what form that security takes is not. As the securing of cyberspace unfolds, ensuring basic principles of transparency, accountability and mutual restraint will be critical.

#### Securitizing cyber space is the ONLY way to prevent large scale cyber war – the alt can’t solve fast enough or change US doctrine – vulnerability creates a Unique need for it

Pickin 12 (Matthew, MA War Stuides – Kings College, “What is the securitization of cyberspace? Is it a problem?”, http://www.academia.edu/3100313/What\_is\_the\_securitization\_of\_cyberspace\_Is\_it\_a\_problem)

In evaluating whether securitization of cyberspace is a problem, it is very clear that securitization is a growing concern with many complications. There are many issues including privacy, regulation, surveillance, internet regulation and the growing tension in the international system. However, because the United States is a superpower contesting with other cyber-heavyweights such as Iran, Russia and China the issue will not be de-securitized in the short term. With the discovery and use of cyber-weapons, many states are in the process of making their own for defensive and offensive purposes. The government of the United States will not de-securitize the issue of cyberspace while there are rival states and groups which prove a threat to the national security agenda. These problems will continue to exist until there is no defensive agenda and the issue is de-securitized, for now securitization is a necessary evil.

#### Cyber threats are real—their dismissal marginalizes civic discussions

Ronald J. DEIBERT, professor of political science and director of the Canada Centre for Global Security Studies at the Munk School of Global Affairs, University of Toronto, 13 [“Bounding Cyber Power: Escalation and Restraint in Global Cyberspace,” Internet Government Papers, Paper No. 6, October 2013]

There is an urgent need for the articulation of an alternative cyber-security strategy for civic networks and from the perspective of liberal democracy. For many who would characterize themselves as part of global civil society, “security” is seen as anathema. In today’s world of exaggerated threats and self-serving hyperbole, it is easy to dismiss security as a myth to be demolished, rather than engaged.28 Securitization is generally associated with the defence industry, Pentagon strategists, intelligence agencies and many others question whether employing the language of security only plays into this complex. But the vulnerabilities of cyberspace are very real, the underbelly of cybercrime is undeniably huge (and growing), an arms race in cyberspace is escalating and major governments are poised to set the rules of the road that may impose top-down solutions that subvert the domain as we know it. Dismissing these vulnerabilities as manufactured myths propagated by power elites will only marginalize civic networks from the conversations where policies are being forged.

### Impact O/W

#### Cyber-attacks come first—they're a form of structural violence. Questions of containing threats in cyberspace come first

Jarno LIMNÉLL, Director of Cyber Security at Stonesoft, a McAfee Group company, 2/12 [“Is cyber war real?" foreignaffairs.com, February 12, 2014, http://www.foreignaffairs.com/articles/140762/jarno-limnell-thomas-rid/is-cyberwar-real]

Cyberwar, in fact, is part of the evolution of conventional warfare, which itself is linked to broader social and political change. It is no longer easy to imagine a confrontation that does not include some element of cyber-activity, such as surveillance or sabotage. Asking whether cyberwar is real, then, is less important than concentrating on how to contain the threats posed by some uses of computer technology. After all, a cyberattack need not kill someone or cause major material damage to still be considered dangerous.¶ Moreover, understanding war as solely physical contestation is an unnecessarily limited view. Consider, for example, nonlethal military tactics that fall under the broad category of strategic communication, which include psychological operations. States and militaries seeking to avoid unnecessary or disproportionate killing need to find other ways to influence potential adversaries and strengthen ties with allies. Strategic communication seeks to coerce enemies and sway allies and includes operations in peace as well as war, blurring the line between the two.¶ The concept of violence is also ambiguous. In addition to causing physical injury or death, violence can refer to mental abuse and different forms of deprivation. The academic discipline of peace studies has for decades advanced the concept of structural violence, such as racism and sexism. In its widest sense, then, violence can be found in almost any coercive situation. And the various attacks and activities associated with cyberwar, from stealing data to disrupting other governments’ computer systems, clearly fall within this broad category.

### Util

#### VTL is inevitable and subjective

#### Maximizing all lives is the only way to affirm equality

Cummiskey 90—David, Professor of Philosophy, Bates [Kantian Consequentialism, Ethics 100.3, p 601-2, p 606, JSTOR]

We must not obscure the issue by characterizing this type of case as the sacrifice of individuals for some abstract "social entity." It is not a question of some persons having to bear the cost for some elusive "overall social good." Instead, the question is whether some persons must bear the inescapable cost for the sake of other persons. Nozick, for example, argues that "to use a person in this way does not sufficiently respect and take account of the fact that he is a separate person, that his is the only life he has."30 Why, however, is this not equally true of all those that we do not save through our failure to act? By emphasizing solely the one who must bear the cost if we act, one fails to sufficiently respect and take account of the many other separate persons, each with only one life, who will bear the cost of our inaction. In such a situation, what would a conscientious Kantian agent, an agent motivated by the unconditional value of rational beings, choose? We have a duty to promote the conditions necessary for the existence of rational beings, but both choosing to act and choosing not to act will cost the life of a rational being. Since the basis of Kant's principle is "rational nature exists as an end-in-itself' (GMM, p. 429), the reasonable solution to such a dilemma involves promoting, insofar as one can, the conditions necessary for rational beings. If I sacrifice some for the sake of other rational beings, I do not use them arbitrarily and I do not deny the unconditional value of rational beings. Persons may have "dignity, an unconditional and incomparable value" that transcends any market value (GMM, p. 436), but, as rational beings, persons also have a fundamental equality which dictates that some must sometimes give way for the sake of others. The formula of the end-in-itself thus does not support the view that we may never force another to bear some cost in order to benefit others. If one focuses on the equal value of all rational beings, then equal consideration dictates that one sacrifice some to save many. [continues] According to Kant, the objective end of moral action is the existence of rational beings. Respect for rational beings requires that, in deciding what to do, one give appropriate practical consideration to the unconditional value of rational beings and to the conditional value of happiness. Since agent-centered constraints require a non-value-based rationale, the most natural interpretation of the demand that one give equal respect to all rational beings lead to a consequentialist normative theory. We have seen that there is no sound Kantian reason for abandoning this natural consequentialist interpretation. In particular, a consequentialist interpretation does not require sacrifices which a Kantian ought to consider unreasonable, and it does not involve doing evil so that good may come of it. It simply requires an uncompromising commitment to the equal value and equal claims of all rational beings and a recognition that, in the moral consideration of conduct, one's own subjective concerns do not have overriding importance.¶

### AT: Security K

#### Our scenarios are part of the liberalism of fear—fearing the consequences of concentration of power in the executive challenges securitization.

Michael **WILLIAMS** Graduate School of Public and International Affairs, University of Ottawa **’11** “Securitization and the liberalism of fear” *Security Dialogue* 42 p. 453-456

¶ Fear is not a concept (or indeed a word) often found in securitization theory. Instead, the Copenhagen School speaks of security as an existential threat, as emergency measures or as a ‘breaking free of rules’. Security is not an objective condition, but emerges through particular social processes or ‘speech acts’ that elevate an issue above the normal political logic: ‘if we do not tackle this problem, everything else will be irrelevant because we will not be here or will not be free to handle it in our own way’ (Buzan et al., 1998: 24). Yet, even this formulation indicates an intimate relationship between existential threat and fear—the fear of annihilation, loss and alienation. Threats imply the loss of or damage to something (physical survival or well-being, an object, a social order, an identity) that is valued—that is, a fear for its continued possession or existence. People can fear other individuals, other groups, other states (or their own); they can fear economic calamity or environmental degradation. Even exceptional violence or fearless killing—an existential or heroic self-sacrifice, for instance—is tied in complex ways to fear: fear for someone or something else that is being defended, fear of failing to achieve glory or salvation. Fear’s negativity always has positive value. This article seeks to extend securitization theory conceptually and, to a lesser degree, empirically by further developing the relationship between securitization and the politics of fear. My suggestion is that by so doing it is possible to enlarge the theoretical framework of the Copenhagen School and to expand its application in understanding the politics of security in liberal societies. At first glance, fear might seem straightforwardly related to securitization: an increase in fear equals an increase in securitization, or at the very least facilitates successful securitization. However, rather than looking at the ways in which fear can facilitate securitization, or adding to the widespread claims about the connections between the politics of fear and the extension of security logics throughout society,1 I want to explore a rather different possibility: that focusing on fear also allows us to see how fear can operate in ways that can actually inhibit processes of securitization, constraining the logic of extremity, making actors reluctant to use securitizing moves and providing resources for opposing such moves. To make this argument, I turn to an examination of the relationship between liberalism and fear. As Jef Huysmans (1998) pointed out in one of the earliest and most perceptive appraisals of the Copenhagen School, liberalism provides an important backdrop to the theory, with a narrowly technocratic liberalism and superficial pluralism serving both as a foil for the idea of securitization as radically creative and socially constructed and as a link to theories of enmity, emergency, and the political identified with Carl Schmitt and with classical political realism more broadly. Fear within liberalism is thus often closely associated with a politics of extremity and enmity, and is seen as having close—and perhaps even constitutive—connections to securitization. Liberal societies, such positions often imply, either need a politics of security and fear in order to overcome the weaknesses of their pluralist foundations or, conversely, are congenitally ill-equipped to respond effectively to the challenges of a politics of extremity and securitization. This understanding of liberalism has in turn become a staple (sometimes an almost unquestioned assumption) for some of the most vibrant controversies over the theoretical and political entailments of securitization theory.2 There is little doubt that these analyses point to crucial issues in the relationship between liberalism and security, and in the politics of securitization in liberal states. Yet, this ‘Schmittian’ or classical ‘realist’ (or, for that matter, Straussian) representation and critique of liberalism is not the only version of liberalism available, and to take it as a given model for liberal thought or practice as a whole—and as an assumed foundation for analysing how ‘security’ operates in liberal societies—may in fact risk being seriously misleading. At least, this is the suspicion I want to explore here, and for help in doing so it is particularly revealing to turn one of the most nuanced and influential expressions of an alternative vision, a vision that Judith Shklar aptly christened the ‘liberalism of fear’.3 Shklar’s conception of liberal politics, I suggest, can help provide a more rounded appreciation of the politics of security in liberal polities, and of how a better understanding of the liberalism of fear can extend the reach of securitization theory both conceptually and empirically, and may—perhaps paradoxically—even provide support for the Copenhagen School’s political project of desecuritization. I In contrast to the narrowly rationalistic liberalism that is the focus of the critiques alluded to above, the liberalism of fear has a number of affinities with securitization theory.4 It is resolutely anti-utopian. It is, in a philosophical sense, non-foundationalist. It is sceptical, seeing a world where violence (actual or potential) is and will remain an ineradicable part of political life. It sides with what Emerson once called the ‘party of memory’ in contrast to the ‘party of hope’ (see Shklar, 1998: 8), insisting on facing up to the worst things that human beings have shown themselves capable of doing to one another, and trying to avoid them. It is suspicious of and generally eschews grand moral visions and philosophical or theo-political schemas, which it tends to see as sources of obscurantism and conflict rather than emancipation and progress. It has no ‘strong’ ontology, in either a rationalist or a social constructivist (self–other) sense.5 It rejects the identification of liberalism with an abstract rationalism, a narrow utilitarianism, Kantian formalism, a programme of indisputable natural rights or a flat proceduralism.6 In sum, it is a vision of liberalism that contrasts sharply with the thin version often put forth by both proponents and critics of liberalism in international relations7—and in many debates over securitization theory. Yet, if the liberalism of fear is sceptical, it is not cynical. Nor is it without a place to stand. In place of essentialist visions of individuals or schemes of indisputable rights, it advocates a focus on cruelty and fear. It is, in Stanley Hoffmann’s (1998: xxii) nice phrase, a vision based on the ‘existential experience of fear and cruelty’, concentrating on humanity’s shared capacity to feel fearand to be victims of cruelty.8 Perhaps most importantly in this context, it turns this focus on fear into a positive principle of liberal politics. As Shklar (1998: 10–11) argues, the liberalism of fear does not, to be sure, offer a summum bonum toward which all political agents should strive, but it certainly does begin with a summum malum which all of us know and would avoid if only we could. That evil is cruelty and the fear that it inspires, and the very fear of fear itself. To that extent, the liberalism of fear makes a universal and especially a cosmopolitan claim, as it historically has always done. In this vision, fear is central to liberal politics, but in a way very different from those visions that see fear, emergency and ‘security’ as the defining ‘outside’ of liberal societies, as the antithesis of normal politics, or, as suggested in other analyses, as the constitutive realm or radical otherness or enmity that stabilizes and/or energizes otherwise decadent or depoliticized liberal orders.9 For the liberalism of fear, fear cannot and should not be always and in every way avoided. For one thing, it is an inescapable part of life, something that often helps preserve us from danger. More complexly, fear can also be a crucial element in preserving as well as constructing a liberal order, for one of the major things to be feared in social life is the fear of fear itself. As Shklar (1998: 11) puts it in one of her most evocative phrasings: To be alive is to be afraid, and much to our advantage in many cases, since alarm often preserves us from danger. The fear we fear is of pain inflicted by others to kill and maim us, not the natural and healthy fear that merely warns us of avoidable pain. And, when we think politically, we are afraid not only for ourselves but for our fellow citizens as well. We fear a society of fearful people. This vision of liberal politics fears the politics of fear. It fears above all collective concentrations of powerthat make possible ‘institutionalized cruelty’, particularly when they are abetted or accompanied by a politics of fear. Thus, while the liberalism of fear fears all concentrations of power, it fears most the concentration of power in that most fearsome of institutions in the modern world—the state; for while cruelty can reflect sadistic urges, ‘public cruelty is not an occasional personal inclination. It is made possible by differences in public power’ (Shklar, 1998: 11). A degree of fear and coercion is doubtless a condition of the operation of all social orders; but, as its first order of concern, the liberalism of fear focuses on restraining fear’s excesses. As Shklar (1998: 11) puts it: A minimal level of fear is implied in any system of law, and the liberalism of fear does not dream of an end to public, coercive government. The fear it does want to prevent is that which is created by arbitrary, unexpected, unnecessary, and unlicensed acts of force and by habitual and pervasive acts of cruelty and torture performed by military, paramilitary and police agents in any regime. The liberalism of fear is far from rejecting the state’s role in the provision of social goods, including security. Indeed, these may be essential in overcoming socially derived cruelties of many kinds.10 But, it is **continually alert** to the state’s potential to do the opposite.11 Here, then, is a vision of politics where fear is not confined to the realm of security; nor is fear wholly negative. Such a vision shares with the Copenhagen School the fear that fear in politics is dangerous. But, Shklar’s multidimensional analysis of fear allows us to see how fear can work as a counter-practice against processes of securitization. Fear operates in normal politics, and the fear of fear—that is, the fear of the power of the politics of security and its consequences—is a core part of liberal theory and practice. Fear is not a one-way street to extremity, nor does it operate only in emergency situations. Instead, the fear of fear can act as a bulwark against such processes. In other words, the fear of fear can within ‘normal’ or even ‘securitized’ politics act to prevent or oppose a movement toward a more intense politics of fear—countering a shift toward ‘security’ in its more extreme manifestations.12

### 1ar

**Structural violence is reductive and vague – default to extinction impacts**

**Boulding 77**Twelve Friendly Quarrels with Johan Galtung Author(s): Kenneth E. BouldingReviewed work(s):Source: Journal of Peace Research, Vol. 14, No. 1 (1977), pp. 75-86Published Kenneth Ewart Boulding (January 18, 1910 – March 18, 1993) was an economist, educator, peace activist, poet, religious mystic, devoted Quaker, systems scientist, and interdisciplinary philosopher.[1][2] He was cofounder of General Systems Theory and founder of numerous ongoing intellectual projects in economics and social science. He graduated from Oxford University, and was granted United States citizenship in 1948. During the years 1949 to 1967, he was a faculty member of the University of Michigan. In 1967, he joined the faculty of the University of Colorado at Boulder, where he remained until his retirement.

 Finally, we come to the great Galtung metaphors of 'structural violence' 'and 'positive peace'. They are metaphors rather than models, and for that very reason are suspect. Metaphors always imply models and metaphors have much more persuasive power than models do, for models tend to be the preserve of the specialist. But when a metaphor implies a bad model it can be very dangerous, for it is both persuasive and wrong. The metaphor of structural violence I would argue falls right into this category. The metaphor is that poverty, deprivation, ill health, low expectations of life, a condition in which more than half the human race lives, is 'like' a thug beating up the victim and 'taking his money away from him in the street, or it is 'like' a conqueror stealing the land of the people and reducing them to slavery. The implication is that poverty and its associated ills are the fault of the thug or the conqueror and the solution is to do away with thugs and conquerors. While there is some truth in the metaphor, in the modern world at least there is not very much. Violence, whether of the streets and the home, or of the guerilla, of the police, or of the armed forces, is avery different phenomenon from poverty. The processes which create and sustain poverty are not at all like the processes which create and sustain violence, although like everything else in 'the world, everything is somewhat related to everything else. There is a very real problem of the structures which lead to violence, but unfortunately Galitung's metaphor of structural violence as he has used it has diverted attention from this problem.Violence in the behavioral sense, that is, somebody actually doing damage to somebody else and trying to make them worse off, is a 'threshold' phenomenon, rather like the boiling over of a pot. The temperature under a pot can rise for a long time without its boiling over, but at some 'threshold boiling over will take place. The study of the structures which underlie violence are a very important and much neglected part of peace research and indeed of social science in general. Threshold phenomena like violence are difficult to   study because they represent 'breaks' in the systenm rather than uniformities. Violence, whether between persons or organizations, occurs when the 'strain' on a system is too great for its 'strength'. The metaphor here is that violence is like what happens when we break a piece of chalk. Strength and strain, however, especially in social systems, are so interwoven historically that it is very difficult to separate them. The diminution of violence involves two possible strategies, or a mixture of the two; one is Ithe increase in the strength of the system, 'the other is the diminution of the strain. The strength of systems involves habit, culture, taboos, and sanctions, all these 'things which enable a system to stand lincreasing strain without breaking down into violence. The strains on the system 'are largely dynamic in character, such as arms races, mutually stimulated hostility, changes in relative economic position or political power, which are often hard to identify. Conflicts of interest 'are only part 'of the strain on a system, and not always the most important part. It is very hard for people ito know their interests, and misperceptions of 'interest take place mainly through the dynamic processes, not through the structural ones. It is only perceptions of interest which affect people's behavior, not the 'real' interests, whatever these may be, and the gap between percepti'on and reality can be very large and resistant to change. However, what Galitung callsstructural violence (which has been defined 'by one unkind commenltator as anything that Galitung doesn't like) wasoriginally defined as any unnecessarily low expectation of life, on that assumption that anybody who diesbefore the allotted span has been killed, however unintentionally and unknowingly, by somebody else. The concept has been expanded to include all 'the problems of poverty, destitution, deprivation, and misery. These are enormously real and are a very high priority for research and action, but they belong to systems which are only peripherally related to 'the structures whi'ch produce violence. This is not rto say that the cultures of violence and the cultures of poverty are not sometimes related, though not all poverty cultures are cultures of violence, and certainly not all cultures of violence are poverty cultures. But the dynamics lof poverty and the success or failure to rise out of it are of a complexity far beyond anything which the metaphor of structural violence can offer. While the metaphor of structural violence performed a service in calling attention to a problem, it may have d'one a disservice in preventing us from finding the answer.