# Open Source Round 7 UMKC

# 1NC

### 1NC

#### Text – The United States Department of Defense should maintain sole control of offensive cyber operations in lieu of congressional notification or authorization. The United States Department of Defense should adopt a cyber-strategy of only mitigative counter-strikes and retributive counterstriking.

#### Legal measures fail – only shifting squo deterrence posture solves the aff

Kesan and Hayes 12 Jay Kesan, Professor, H. Ross & Helen Workman Research Scholar, and Director of the Program in Intellectual Property & Technology Law, University of Illinois College of Law, and Carol Hayes, Research Fellow, University of Illinois College of Law, served as a Christine Mirzayan Science and Technology Policy Graduate Fellow at the National Academy of Sciences, “MITIGATIVE COUNTERSTRIKING: SELF-DEFENSE AND DETERRENCE IN CYBERSPACE”, Harvard Journal of Law & Technology 25 Harv. J. Law & Tec 415, Spring 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1805163

The weaknesses of the current reliance on employing passive defense methods and seeking help from the authorities -- who are both technologically and legally ill-equipped to seek justice for victims -- present a difficult situation. Considering how modern society relies on the Internet and networked services, there is an urgent need for proactive policy to help insulate critical services from damage as well as mitigate harm from potential attacks. For a number of reasons explored below, we argue that, in some circumstances, permitting mitigative counterstrikes in response to cyberattacks would be more optimal. There is an urgent need for dialog on this topic as the development of technology has outpaced the law in this area. n15 While progress has been made in the form of executive orders addressing cybersecurity, n16 the proposed Cyber Intelligence Sharing and Protection Act ("CISPA"), n17 and cybersecurity provisions of the National Defense Authorization Act ("NDAA"), n18 these measures do not go far enough. New discussions and analyses are needed to ensure that responsive actions can be grounded in sound policy.¶ Because of the inadequacy in current means to address cyber threats, this Article examines other possible methods to deter cyberattacks, specifically the use of cyber counterstrikes as part of a model of active defense. Active defense involves (1) detecting an intrusion, (2) tracing the intruder, and (3) some form of cyber counterstrike. n19¶ [\*420] Though intrusion detection and tracing are essential, counterstriking is key to enhancing the deterrent effects of active defense. At its core, cyber counterstriking is about two things: (1) deterring attackers and (2) ensuring that attacked parties are not deprived of the inherent right to defend themselves and their property. There are many views of deterrence, but deterrence is generally accomplished by the threat of some combination of the following elements: (1) punishing attackers by inflicting unacceptable costs, or (2) preventing attackers from succeeding in their attacks. n20 These two elements of deterrence have led us to apply the terms "retributive counterstriking" and "mitigative counterstriking," respectively, to the counterstriking component of active defense.¶ In the cyber context, a "counterstrike" can involve any number of actions. As discussed in Part III.B, a counterstrike can involve the target executing its own Denial of Service ("DoS") attack against the attacker (for example, by redirecting the attacker's packets back at the attacker to knock the attacker's systems offline), n21 infecting the attacker's system with a virus or worm to permit the victim to take control, or a number of other options. The technologies available to execute counterstrikes are generally the same ones used in initial attacks; as we examine in more detail below, some of these currently available technologies permit an attack to be traced back to its origin -- with varying degrees of accuracy. Furthermore, there is now evidence that "cyber contractors" exist as part of what some have termed the new "military digital complex," whose work involves creating offensive cyber technologies that can have applications in the context of counterstriking. n22¶ The goal of a counterstrike can vary, from punishing the attacker to simply mitigating the harm to the target. We call the former "retributive counterstriking"; this type should remain under the sole control [\*421] of the military, as a national security matter relating to sensitive domestic and international legal issues. We define "mitigative counterstriking" as taking active efforts to mitigate harm to a targeted system, in a manner strictly limited to the amount of force necessary to protect the victim from further damage. We recognize there may be overlap between retributive and mitigative counterstriking, as the latter could potentially result in damage to the attacker's system. How-ever, the goal of mitigative counterstriking must be to mitigate damage from a current and immediate threat. We argue that whatever measures are deployed must be justifiable under a mitigation frame-work.

#### Passive defensive measures are ineffective – invites adversaries to attack until successful – only active counterstriking solves deterrence

Kesan and Hayes 12 Jay Kesan, Professor, H. Ross & Helen Workman Research Scholar, and Director of the Program in Intellectual Property & Technology Law, University of Illinois College of Law, and Carol Hayes, Research Fellow, University of Illinois College of Law, served as a Christine Mirzayan Science and Technology Policy Graduate Fellow at the National Academy of Sciences, “MITIGATIVE COUNTERSTRIKING: SELF-DEFENSE AND DETERRENCE IN CYBERSPACE”, Harvard Journal of Law & Technology 25 Harv. J. Law & Tec 415, Spring 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1805163

In Part II, we described the extent of the threat posed by modern cyberattack techniques and examined the currently available methods for addressing cyberattacks. Even if criminal and civil enforcement methods were consistently effective, using these methods is inherently ex post facto, addressing an injury after harm has already occurred. If a power grid is under siege from a cyberterrorist, the satisfaction of knowing that a future prosecution will be successful will not allay the immediate concerns of protecting public safety. There needs to be some method of addressing an attack that the operator of the system can control. Passive defense, including firewalls and antivirus software, is generally viewed as the primary method for a user to avoid being harmed by an attack attempt.¶ However, passive defense is all but useless against zero-day exploits. There are indications that it is more profitable to hoard lists of zero-day exploits for future offensive use than it is to report those exploits to the software manufacturers to fix the holes in their software code. n300 This makes it more difficult to close the holes that could lead to botnets being used in DDoS attacks. Similarly, passive options like dropping incoming packets are likely to be less effective with modern DDoS attacks than they would be with DoS attacks, where the repeated requests come from the same IP address.¶ In today's era of zero-day exploits and DDoS attacks, "scan, firewall, and patch" has become similar to "duck and cover." Cyberattack victims, particularly operators of CNI, should be empowered to repel as well as block attacks. This notion of actively repelling a cyberattack to mitigate harm to the victim system is what we have termed "mitigative counterstriking," which is at the core of the broad concept of active defense.

### 1NC

#### The political winds in America are changing. A revolution is emerging. Reject this revolution at your peril.

Farrell 11 – marketwatch, the burning platform (“A new Lost Decade is leading to revolution.” <http://www.theburningplatform.com/?p=22549>

Unfortunately, the new one gets worse: Why? The coming Lost Decade is a backdrop for a wave of class warfare destined to trigger a historic revolution in American politics, bigger than the ‘29 Crash and Great Depression. Initially inspired by the Arab Spring, Occupy Wall Street is a virus spreading rapidly as Occupy Everything, a reform movement that will overshadow the GOP/Tea Party as the voice of the people, leading to an Occupy America. Investors, listen closely: First, we’ll summarize five major signs of America’s new Lost Decade 2011-2021. Then, we summarize seven diverse examples of rebellions across the world adding fuel to America’s accelerating Occupy Wall Street revolution. Why is this crucial for investors? Because these class wars are guaranteed to deepen America’s market and economic problems during the coming Lost Decade. So listen closely investors: 1. Decade of debt stagnation till 2021 Barron’s Gene Epstein warns that Obama’s latest is “Too Little, Too Late.” Even if the president “gets everything he asked for in his new proposals, it won’t reduce our growing public debt. And he won’t get it all.” So America’s debt will remain around 80% of GDP for a decade, levels not seen since the 1940s. That’s right, debt will remain dangerously high at least through 2021. And it won’t matter who is president. Class warfare will accelerate this job-killing debt cycle. 2. Investors lose faith, bailing out Over at the Wall Street Journal Tom Lauricella warns “Investors lose faith in stocks … in a historic retreat, investors world-wide during the three months through August pulled some $92 billion out of stock funds in the developed markets,” more than reversing the total “put into those funds since stocks bottomed in 2009.” Worse, there’s a “widening belief that the mess left behind by the housing bubble and financial crisis will be a morass to contend with for years.” Yes, many years. 3. Fed surrenders, cannot fix economy In a Cleveland speech last week Fed Chairman Ben Bernanke warned that with 45% of the unemployed out more than six months, long-term unemployment is now a “national crisis” the Fed cannot fix. “Unheard of … this has never happened in the post-war period.” They’re “losing the skills they had, they are losing their connections, their attachment to the labor force.” But a job-killing Congress won’t act. 4. Wall Street still doesn’t get it In a recent Foreign Policy article, William Cohan, a former J. P. Morgan Chase managing director and author of “Money and Power: How Goldman Sachs Came to Rule the World,” warns Wall Street not only learned nothing after the 2008 meltdown, they’re aggressively lobbying to kill all reforms that might “break this dangerous cycle in which bankers and traders get very rich while the rest of us suffer from their mistakes.” Wall Street is deaf, blind and myopic, wants no limits on “all manner of bets on the market,” even at the “risk of a U.S. recession.” Only a catastrophe will wake Wall Street. 5. Yes, America’s second Lost Decade just began In a Money interview, “Are We the Next Japan?” Nomura Research economist Richard Koo sees “striking similarities between our current malaise” and Japan’s Lost Decade. Their stimulus did work, but then “the Japanese made a horrendous mistake in 1997.” The IMF told Japan “you’re running a huge fiscal deficit with an aging population … reduce your deficit.” So Japan “cut spending and raised taxes” and “the whole economy came crashing down.” Sure sounds familiar. Wall Street protest spread. Inspired by the Occupy Wall Street demonstrations in New York, some 100 people gathered Sunday outside the Federal Reserve Bank in Chicago to protest inequities in the nation’s financial system. Warning: to Wall Street CEOs, the Super Rich, the top 1% who think they own our government … the party’s over. No matter who gets elected in 2012 and 2016, the new Lost Decade 2011-2021 will make life miserable for the president and Congress, as with Japan earlier. Worse, this Lost Decade will make life miserable for everybody: corporations, investors, consumers, workers, small businesses and all our families, with the kind of economic suffering experienced in the painfully long Great Depression era. Yes, big shock dead ahead. The class wars like Arab Spring are accelerating across America. “Occupy Wall Street” is going viral, spreading through “Occupy Together,” expanding in dozens of cities across America and the world, growing bigger — in commitment, in mission, in boldness — a resistance movement waging war against our democracy-killing Super Rich. Next, expect many more class wars, regional rebellions, uprisings against the wealthy — yes, this is the second American Revolution.

#### **Cyber prolif is the result of global inequities that force arms races as an expansion of capital accumulation**

Callinicos, Director of the Centre for European Studies at King’s College, in ’04 [Alex, The Revolutionary Ideas of Karl Marx, 2004 pg. 196-197]

**Capitalism** has not changed its spots. It **is still based on the exploitation of the working class,** and liable to constant crises. The conclusion that Marx drew from this analysis, that the working class must overthrow the system and replace it with a classless society, is even more urgent now than in his day. **For the military rivalries which are the form increasingly assumed by competition between capitals now threaten the very survival of the planet**. As Marx’s centenary approached, the fires of war flickered across the globe—in Lebanon, Iran and Iraq, Kampuchea, southern Africa, the Horn of Africa, Afghanistan and the South Atlantic. **The accumulation of vast armouries of nuclear destruction by the superpowers**, missilerattling in the Kremlin, talk of ‘limited’ and ‘protracted’ nuclear war in Washington—these **cast a shadow over the whole of humanity**. Socialist revolution is an imperative if we are to change a world in the grip of economic depression and war fever, a world where 30 million rot on Western dole queues and 800 million go hungry in the Third World. To that extent, Marx’s ideas are more relevant today than they were 100 years ago. Capitalism has tightened its grip of iron on every portion of the planet since 1883, and is rotten-ripe for destruction, whether at its own hands through nuclear war, or at the hands of the working class. The choice is between workers’ power or the ‘common ruination of the contending classes’—between socialism or barbarism. Many people who genuinely wish to do something to remedy the present state of the world believe that this stress on the working class is much too narrow. The existence of nuclear weapons threatens everyone, whether workers or capitalists or whatever. Should not all classes be involved in remedying a problem which affects them all? What this ignores is that what Edward Thompson has called ‘exterminism’— **the vast and competing military apparatuses which control the arms race—is an essential part of the working of capitalism today. No sane capitalist desires a nuclear war** (although some insane ones who believe that such a war would be the prelude to the Second Coming now hold positions of influence in Washington). **But sane or insane, every capitalist is part of an economic system which is bound up with military competition between nation-states. Only a class with the interest and power to do away with capitalism can halt the march to Armageddon**. Marx always conceived of the working class as the class whose own selfemancipation would also be the liberation of the rest of humanity. The socialist revolution to whose cause he devoted his life can only be, at one and the same time, the emancipation of the working class and the liberation of all the oppressed and exploited sections of society.

#### **Capitalism makes elitist authoritarianism inevitable that uses mass violence to suppress all dissent**

Meszaros 95 (Istavan, Prof. Emeritus @ U of Sussex, Beyond Capital: Towards a Theory of Transition, p 146)

In view of the fact that the most intractable of the global capital system’s contradictions is the one between the internal unrestrainability of its economic constituents and the now inescapable necessity of introducing major restraints, any hope for finding a way out of this vicious circle under the circumstances marked by the activation of capital’s absolute limits must be vested in the political dimension of the system. Thus, in the light of recent legislative measures which already point in this direction, **there** **can be no doubt that the full power of the state will be activated to serve the end of squaring capital’s vicious circle**, **even if it means subjecting all potential dissent to extreme authoritarian constraints**. Equally there can be no doubt that whether or not such a remedial action (in conformity to the global capital system’s structural limits) will be successfully pursued, despite its obvious authoritarian character and destructiveness, will depend on the working class’s ability or failure to radically rearticulate the socialist movement as a truly international enterprise. In any event, **what makes matters** particularly **serious is the fact that the far-reaching issues themselves which confront humankind at the present stage of historical development cannot be avoided either by the ruling capital system or by any alternative to it**. Although, as a matter of historical contingency, **they have arisen from the activation of capital’s absolute limits, they cannot be conveniently bypassed, nor their gravity wished out of existence**. On the contrary, **they remain the overriding requirement of all-embracing remedial action in the reproductive practices of humankind for as long as the vicious circle of capital’s present-day historical contingency is not irretrievably consigned to the past.** Indeed, paradoxically, the ability to meet in a sustainable way the absolute historical challenge that had arisen from the perverse historical contingencies and contradictions of the capital system constitutes the measure of viability of any social metabolic alternative to the ruling order. Consequently, **the struggle to overcome the threatening absolute limits of the capital system is bound to determine the historical agenda for the foreseeable future.**

#### **The alternative is to do nothing – this solves the inevitability of capitalism**

Zizek 08—Senior Research @ Institute for Social Studies-Ljubljana [Slavoj, Violence, p. 207-217

While the parallel holds, the concluding characterisation seems to fall short: the unsettling message of Seeing is not so much the indissolubility of both people and government as much the compulsive nature of democratic rituals of freedom. What happens is that by abstaining from voting, people effectively dissolve the government-not only in the limited sense of overthrowing the existing government, but more radically. Why is the government thrown into such a panic by the voters' abstention? It is compelled to confront the fact that it exists, that it exerts power, only insofar as it is accepted as such by its subjects-accepted even in the mode of rejection. The voters' abstention goes further than the intra-political negation, the vote of no confidence: it rejects the very frame of decision. In psychoanalytic terms, the voters' abstention is something like the psychotic Verwerfung (foreclosure, rejection/repudiation), which is a more radical move than repression (Verdrangung). According to Freud, the repressed is intellectually accepted by the subject, since it is named, and at the same time is negated because the subject refuses to recognise it, refuses to recognise him or herself in it. In contrast to this, foreclosure rejects the term from the symbolic tout court. To circumscribe the contours of this radical rejection, one is tempted to evoke Badiou's provocative thesis: "It is better to do nothing than to contribute to the invention of formal ways of rendering visible that which Empire already recognizes as existent.''6 Better to do nothing than to engage in localised acts the ultimate function of which is to make the system run more smoothly (acts such as providing space for the multitude of new subjectivities). The threat today is not passivity, but pseudoactivity, the urge to "be active," to "participate," to mask the nothingness of what goes on. People intervene all the time, "do something"; academics participate in meaningless debates, and so on. The truly difficult thing is to step back, to withdraw. Those in power often prefer even a "critical" participation, a dialogue, to silence-just to engage us in "dialogue," to make sure our ominous passivity is broken. The voters' abstention is thus a true political act: it forcefully confronts us with the vacuity of today's democracies.If one means by violence a radical upheaval of the basic social relations, then, crazy and tasteless as it may sound, the problem with historical monsters who slaughtered millions was that they were not violent enough. Sometimes doing nothing is the most violent thing to do.

### 1NC

#### Text: The President of the United States should issue an executive order enacting, via the appropriate administrative agencies, a prohibition on offensive cyber operations about which Congress has not been notified.

#### **CP solves the whole Aff – maintains executive flex – plan sets precedent for future constraint**

Brecher ’13 Cyberattacks and the Covert Action Statute:¶ Toward a Domestic Legal Framework for¶ Offensive Cyberoperations¶ Aaron P. Brecher\* J.D. Candidate, May 2013, University of Michigan Law School. I am grateful to all¶ of the editors of the Michigan Law Review <http://www.michiganlawreview.org/assets/pdfs/111/3/Brecher.pdf>

The executive might also issue the proposed order, even though it would¶ limit her freedom in some ways, because of the possible benefits of constraining¶ future administrations or preempting legislative intervention.149 For¶ example, in this context, an administration may choose to follow the finding¶ and reporting requirements in order to convince Congress that legislative¶ intervention is unnecessary for proper oversight. This is acceptable if the¶ covert action regime is in fact adequate on its own. Moreover, if greater¶ statutory control over cyberattacks is needed, the information shared with¶ Congress may give Congress the tools and knowledge of the issue necessary¶ to craft related legislation.150 Additionally, while executive orders are hardly¶ binding, the inertia following adoption of an order may help constrain future¶ administrations, which may be more or less trustworthy than the current¶ one. Creating a presumption through an executive order also establishes a¶ stable legal framework for cyberattacks that allows law to follow policy in¶ this new field, and permits decisionmakers to learn more about the nature of¶ cyberoperations before passing detailed statutes that may result in unintended¶ consequences

**That constraint crushes cyber warmaking**

**Lorber 13** (Eric, J.D. Candidate, University of Pennsylvania Law School, Ph.D Candidate, Duke University Department of Political Science.January, 2013, University of Pennsylvania Journal of Constitutional Law, Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?, gender paraphrased)

This Comment provides an initial answer to the question of whether current U.S. law can effectively govern the Executive's use of OCOs. n17 It explores the interaction between this new tool and the current statutory limits on presidential war-making authority, with a particular focus on whether the two current federal laws meant to restrict executive power in this field - the War Powers Resolution n18 and the Intelligence Authorization Act n19 - apply to a wide range of potential offensive cyber operations undertaken by the executive branch. Beyond suggesting that neither the War Powers Resolution nor the Intelligence Authorization Act can effectively regulate most types of offensive cyber operations, this Comment suggests that while marginally problematic for a proper balance of war-making power between the executive and legislative branches, this lack of oversight does not fundamentally shift the current alignment. It does argue, however, that - given this lack of regulatory oversight - the President now has another powerful war-making tool to use at his [or her] discretion. Finally, the Comment suggests that this lack of limitation may be positive in some ways, as laying down clear legal markers before having a developed understanding of these capabilities may problematically limit their effective use.

### 1NC

#### Terrorist capabilities are degraded- they still have operational intent though

McLaughlin 2013 [John McLaughlin was a CIA officer for 32 years and served as deputy director and acting director from 2000-2004. He currently teaches at the Johns Hopkins University's School of Advanced International Studies and is a Non-Resident Senior Fellow at the Brookings Institution July 12, 2013 “Terrorism at a moment of transition” http://security.blogs.cnn.com/2013/07/12/terrorism-at-a-moment-of-transition/]

On targets, jihadists are now pulled in many directions. Many experts contend they are less capable of a major attack on the U.S. homeland. But given the steady stream of surprises they’ve sprung – ranging from the 2009 “underwear bomber” to the more recent idea of a surgically implanted explosive – it is hard to believe they’ve given up trying to surprise us with innovations designed to penetrate our defenses.¶ We especially should remain alert that some of the smaller groups could surprise us by pointing an attacker toward the United States, as Pakistan’s Tehrik e Taliban did in preparing Faizal Shazad for his attempted bombing of Times Square in 2010.¶ At the same time, many of the groups are becoming intrigued by the possibility of scoring gains against regional governments that are now struggling to gain or keep their balance – opportunities that did not exist at the time of the 9/11 attacks.¶ Equally important, jihadists are now learning from their mistakes, especially the reasons for their past rejection by populations where they temporarily gained sway.¶ Documents from al Qaeda in the Islamic Maghreb, discovered after French forces chased them from Mali, reveal awareness that they were too harsh on local inhabitants, especially women. They also recognized that they need to move more gradually and provide tangible services to populations – a practice that has contributed to the success of Hezbollah in Lebanon.¶ We are now seeing a similar awareness among jihadists in Syria, Tunisia, Libya, and Yemen. If these “lessons learned” take hold and spread, it will become harder to separate terrorists from populations and root them out.¶ Taken together, these three trends are a cautionary tale for those seeking to gauge the future of the terrorist threat.¶ Al Qaeda today may be weakened, but its wounds are far from fatal. It is at a moment of transition, immersed in circumstances that could sow confusion and division in the movement or, more likely, extend its life and impart new momentum.¶ So if we are ever tempted to lower our guard in debating whether and when this war might end, we should take heed of these trends and of the wisdom J. R. R. Tolkien has Eowyn speak in “Lord of the Rings”: "It needs but one foe to breed a war, not two ..."

#### OCO are key to prevent terrorist recruiting and organization of large scale attacks- key to prevent CBW attacks

Brennan 2012 [Lieutenant Colonel John W. Brennan 15 March 2012 US Army War College “United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?” http://nsfp.web.unc.edu/files/2012/09/Brennan\_UNITED-STATES-COUNTER-TERRORISM-CYBER-LAW-AND-POLICY.pdf]

More disturbing than terror financing, is the implementation of a worldwide¶ recruiting drive, launched by al-Qa’ida in order to co-opt computer and electrical ¶ engineers who already possess advanced degrees from elite universities. Before their¶ demise, Al-Qa’ida in the Arabian Peninsula (AQAP) leaders Anwar al Awlaki and Inspire ¶ Magazine editor-in-chief Samir Kahn were posting high-tech want ads in their jihadi ¶ circular on the internet in order to elicit acts of terror by homegrown western Muslims. ¶ The two also posted numerous want-ads to recruit individuals who possessed high-tech ¶ degrees.¶ 15¶ As we shall learn, the lack of an effective U. S. CT Cyber policy prevented ¶ the timely interdiction and/or manipulation of the data on this website--action that could ¶ have been used to not only thwart AQAP’s cyber efforts, but could have been used to ¶ create physical vulnerabilities within the organization as well. The plots that could be hatched by heavily recruited techno-savvy terrorists are ¶ especially horrifying. Imagine if you will, the mayhem that could be unleashed by a ¶ terrorist, who using the internet, pilots multiple unmanned aircraft armed with explosive, ¶ chemical, or biological payloads. A hint of this frightening scenario came to pass when ¶ the FBI foiled a plot by Rezwan Ferdaus, a young Bangladeshi-American physicist, who ¶ was arrested while in the process of developing the means to fly remote-controlled ¶ aircraft packed with explosives into the U. S. Capitol and the Pentagon.(Valencia, Milton J. ¶ and Ballou, Brian R. 2011, A1) Another terrifying possibility consists of dozens, if not hundreds ¶ of improvised explosive devices igniting simultaneously through the instantaneity of the ¶ internet. The process of perfecting this method of terrorist attack was proven to be well ¶ on its way to fruition, as § Marked 16:31 § was evident after the capture of numerous Al-Qa’ida in Iraq ¶ (AQI) improvised explosive device (IED) cell members. These individuals were ¶ detained while in the possession of hundreds of digital tone multi-frequency (DTMF) ¶ boards that were purported to be used to simultaneously initiate multiple IEDs to destroy ¶ U. S. and Iraqi security forces.¶ 16¶ Today these potential threats may seem far-fetched to some, but so did the ¶ concept of crashing jet airliners into the World Trade Center and the Pentagon prior to ¶ September 11¶ th¶ , 2001. These and other cyber-enabled terror plots are unfortunately far ¶ from fiction, as their perpetrators were caught in the acts of planning or executing them. ¶ The cyber terror threats which emanate from the various international terrorist ¶ organizations around the globe are of a seminal concern to U. S. national decisionmakers. Though significant, the task of countering these terrorists’ threats within ¶ cyberspace is anything but insurmountable, provided that those who are charged with ¶ exposing and attacking these networks are given the latitude to act effectively. The ¶ concerns of national leaders and their desires to exploit terrorist organizations in ¶ cyberspace are clearly evident in the content of numerous past, and current national ¶ security strategy documents.

#### **Bioweapon use spreads globally and causes extinction – outweighs nuclear weapons**

John D. Steinbruner, Brookings senior fellow and chair in international security, vice chair of the committee on international security and arms control of the National Academy of Sciences, Winter 1997, Foreign Policy, “Biological weapons: a plague upon all houses,” n109 p85(12), infotrac

Although human pathogens are often lumped with nuclear explosives and lethal chemicals as potential weapons of mass destruction, there is an obvious, fundamentally important difference: Pathogens are alive, weapons are not. **Nuclear** and chemical **weapons do not reproduce** themselves **and** do not independently **engage in adaptive behavior; pathogens do** both of these things. That deceptively simple observation has immense implications. The use of **a manufactured weapon** is a singular event. Most of the damage occurs immediately. The **aftereffects**, whatever they may be, **decay rapidly over time** and distance **in a** reasonably **predictable manner.** Even before a nuclear warhead is detonated, for instance, it is possible to estimate the extent of the subsequent damage and the likely level of radioactive fallout. Such predictability is an essential component for tactical military planning. The use of **a pathogen**, by contrast, is an extended process whose scope and timing **cannot be** precisely **controlled.** For most potential biological agents, the predominant drawback is that they would not act swiftly or decisively enough to be an effective weapon. But for a few **pathogens** - ones **most likely to have a decisive effect and therefore** the ones **most likely to be contemplated for deliberately hostile use** - the § Marked 16:31 § risk runs in the other direction. A lethal pathogen **that could efficiently spread from one victim to another would be capable of initiating an intensifying cascade of disease that might ultimately threaten the entire world population. The 1918 influenza epidemic demonstrated the potential for a global contagion of this sort** but not necessarily its outer limit.

## Case

### Advantage 1

#### Past the tipping point – EVERYONE either has or is getting OCOs

Clayton 11 Mark Clayton, reporter for CSM, served as the Monitor's Toronto bureau chief from 1993-2007, reporting on Canadian culture and political affairs, including that nation's close call with Quebec secession, “The new cyber arms race”, Christian Science Monitor, March 7th, 2011, http://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race

Policy experts are just beginning to ask some of these questions as the cyberweapons buildup begins. And make no mistake, it is beginning. By one estimate, more than 100 nations are now amassing cybermilitary capabilities. This doesn't just mean erecting electronic defenses. It also means developing "offensive" weapons.¶ Shrouded in secrecy, the development of these weaponized new software programs is being done outside public view and with little debate about their impact on existing international treaties and on conventional theories of war, like deterrence, that have governed nations for decades.¶ "Here's the problem – it's 1946 in cyber," says James Mulvenon, a founding member of the Cyber Conflict Studies Association, a nonprofit group in Washington. "So we have these potent new weapons, but we don't have all the conceptual and doctrinal thinking that supports those weapons or any kind of deterrence. Worse, it's not just the US and Soviets that have the weapons – it's millions and millions of people around the world that have these weapons."¶ In the new cyber world order, the conventional big powers won't be the only ones carrying the cannons. Virtually any nation – or terrorist group or activist organization – with enough money and technical know-how will be able to develop or purchase software programs that could disrupt distant computer networks.¶ And the US, because it's so wired, is more vulnerable than most big powers to this new form of warfare. It's the price the country may one day pay for being an advanced and open society.

#### Countermeasures solve - air gapping and redundancy

Bailey, science correspondent – Reason Magazine, 1/18/’11

(Ronald, <http://reason.com/archives/2011/01/18/cyberwar-is-harder-than-it>)

Brown and Sommer observe that the Internet and the physical telecommunications infrastructure were designed to be robust and self-healing, so that failures in one part are routed around. “You have to be cautious when hearing from people engaging in fear-mongering about huge blackouts and collapses of critical infrastructures via the Internet,” says University of Toronto cyberwarfare expert Ronald Deibert in the January/February 2011 issue of the *Bulletin of the Atomic Scientists*. “There is a lot of redundancy in the networks; it’s not a simple thing to turn off the power grid.” In addition, our experience with current forms of malware is somewhat reassuring. Responses to new malware have generally been found and made available within days and few denial of service attacks have lasted more than a day. In addition, many critical networks such as those carrying financial transactions are not connected to the Internet requiring insider information to make them vulnerable.

#### **Cyber war infeasible**

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

An attack against the electrical grid is a reasonable threat scenario since power systems are "a high priority target for military and insurgents" and there has been a trend towards utilizing commercial software and integrating utilities into the public Internet that has "increased vulnerability across the board" (Lewis 2010). Yet the increased vulnerabilities are mitigated by an increased detection and deterrent capability that has been "honed over many years of practical application" now that power systems are using standard, rather than proprietary and specialized, applications and components (Leita and Dacier 2012). The security of the electrical grid is also enhanced by increased awareness after a smart-grid hacking demonstration in 2009 and the identification of the Stuxnet malware in 2010: as a result the public and private sector are working together in an "unprecedented effort" to establish robust security guidelines and cyber security measures (Gohn and Wheelock 2010).

#### **Multiple checks empirically check escalation – their evidence is alarmist**

Birch ‘12 (Douglas is a former foreign correspondent for the Associated Press and the Baltimore Sun who has written extensively on technology and public policy, Forget Revolution, 10/1/12, http://www.foreignpolicy.com/articles/2012/10/01/forget\_revolution?page=0,3)

First, the freak "derecho" storm that barreled across a heavily-populated swath of the eastern United States on the afternoon of June 29 knocked down trees that crushed cars, bashed holes in roofs, blocked roads, and sliced through power lines. According to an August report by the U.S. Department of Energy, 4.2 million homes and businesses lost power as a result of the storm, with the blackout stretching across 11 states and the District of Columbia. More than 1 million customers were still without power five days later, and in some areas power wasn't restored for 10 days. Reuters put the death toll at 23 people as of July 5, all killed by storms or heat stroke. The second incident occurred in late July, when 670 million people in northern India, or about 10 percent of the world's population, lost power in the largest blackout in history. The failure of this huge chunk of India's electric grid was attributed to higher-than-normal demand due to late monsoon rains, which led farmers to use more electricity in order to draw water from wells. Indian officials told the media there were no reports of deaths directly linked to the blackouts. But this cataclysmic event didn't cause widespread chaos in India -- indeed, for some, it didn't even interrupt their daily routine. "[M]any people in major cities barely noticed the disruption because localized blackouts are so common that many businesses, hospitals, offices and middle-class homes have backup diesel generators," the New York Times reported. The most important thing about both events is what didn't happen. Planes didn't fall out of the sky. Governments didn't collapse. Thousands of people weren't killed. Despite disruption and delay, harried public officials, emergency workers, and beleaguered publics mostly muddled through. The summer's blackouts strongly suggest that a cyber weapon that took down an electric grid even for several days could turn out to be little more than a weapon of mass inconvenience. "Reasonable people would have expected a lot of bad things to happen" in the storm's aftermath, said Neal A. Pollard, a terrorism expert who teaches at Georgetown University and has served on the United Nation's Expert Working Group on the use of the Internet for terrorist purposes. However, he said, emergency services, hospitals, and air traffic control towers have backup systems to handle short-term disruptions in power supplies. After the derecho, Pollard noted, a generator truck even showed up in the parking lot of his supermarket. The response wasn't perfect, judging by the heat-related deaths and lengthy delays in the United States in restoring power. But nor were the people without power as helpless or clueless as is sometimes assumed.

#### Militarized cyber revolution coming now – squo solves adaptation to a new domain of warfare

Singer and Wright 13 Peter Singer, Director, 21st Century Defense Initiative Senior Fellow, Foreign Policy, Thomas Wright, Fellow, Foreign Policy, Managing Global Order, “An Obama Doctrine on New Rules of War”, Brookings Institution, January 17th, 2013, http://www.brookings.edu/research/papers/2013/01/an-obama-doctrine-on-new-rules-of-war

There has been a game change in weaponry over the last several years, with a new generation of advanced technology that moves the point of critical human decision, both geographically off the battlefield and also, increasingly, chronologically away from the time of kinetic action. These encompass both physical systems, like unmanned aircraft (a.k.a. “drones”), and a new class of virtual weaponry, malware that can conduct a cyber attack with real world consequences.¶ The United States has been a leader in driving this revolution. Its military unmanned systems now number more than 8,000 in the air and 12,000 on the ground and are used daily in Afghanistan. The U.S. Cyber Command became operational in 2010 and military spending on cyber operations now measures in the billions of dollars.¶ At the same time, civilian intelligence agencies are increasingly using these technologies in a series of not-so-covert operations and so-called “secret wars” that have leaked into the press. There have been over 400 drone strikes into places like Pakistan and Yemen. The United States also deployed Stuxnet to sabotage Iranian nuclear development, the world’s first known use of a specially designed cyber weapon.¶ Such weapons seem advanced, but represent just the beginning. Technologies currently under development are far more effective and more autonomous, and capable of operating in a wider set of circumstances. We are at the onset of a decades-long technological revolution in warfare, comparable to the introduction of mechanization and airpower onto the battlefield or the advent of the atomic bomb.

#### Cyber-space warfare is distinct from other campaigns – allowing executive maneuverability and flexibility on OSO’s is k2 dealing with unique cyber threats

http://www.brookings.edu/~/media/events/2013/6/27%20cybersecurity%20dempsey/20130627\_dempsey\_cybersecurity\_transcript.pdf

Well, I didn't, I'm not making any ¶ assertions about Title 10 and Title 50. What I am suggesting is that it is our ¶ elected leaders, and notably the Congress of the United States, that ¶ generally decides whether the nation is under a condition of war, it's called ¶ the War Powers Act. And here's why that's important; there is an ¶ assumption out there, I think, and I would like to disabuse you of it, that a ¶ cyber attack that had destructive effects would be met by a cyber response ¶ with destructive attacks. That's not necessarily the case. 29 ¶ ¶ I mean, again, this is why I'm so adamant that we think of ¶ cyber as a domain not unique to all others, it has many common features of ¶ other domains, that is land, sea, air and space. And I think that what the ¶ President of the United States would insist upon, actually, is that he had ¶ the options and the freedom of movement to decide what kind of response ¶ we would employ. And § Marked 16:32 § that's why I say I don't want to have necessarily a ¶ narrow conversation about what constitutes war and cyber, because the ¶ response could actually be in one of the traditional, one of the other ¶ traditional domains.

#### 4GW is the most accurate description of modern war- escalation is likely if uncontained- executive authority is key to counter these threats

Li 2009 [Zheyoa Li Winter, 2009 The Georgetown Journal of Law Public Policy 7 Geo. J.L. & Pub. Pol'y 373 “War Powers for the Fourth Generation: Constitutional Interpretation in the Age of Asymmetric Warfare” lexis]

Even as the quantity of nation-states in the world has increased dramatically since the end of World War II, the institution of the nation-state has been in decline over the past few decades. Much of this decline is the direct result of the waning of major interstate war, which primarily resulted from the introduction of nuclear weapons. 122 The proliferation of nuclear weapons, and their immense capacity for absolute destruction, has ensured that conventional wars remain limited in scope and duration. Hence, "both the size of the armed forces and the quantity of weapons at their disposal has declined quite sharply" since 1945. 123 At the same time, concurrent with the decline of the nation-state in the second half of the twentieth century, non-state actors have increasingly been willing and able to use force to advance their causes. In contrast to nation-states, who adhere to the Clausewitzian distinction between the ends of policy and the means of war to achieve those ends, non-state actors do not necessarily fight as a mere means of advancing any coherent policy. Rather, they see their fight as a life-and-death struggle, wherein the ordinary terminology of war as an instrument of policy breaks down because of this blending of means and ends. 124¶ It is the existential nature of this struggle and the disappearance of the Clausewitzian distinction between war and policy that has given rise to a new generation of warfare. The concept of fourth-generational warfare was first articulated in an influential article in the Marine Corps Gazette in 1989, which has proven highly prescient. In describing what they saw as the modern trend toward a new phase of warfighting, the authors argued that:¶ [\*395] In broad terms, fourth generation warfare seems likely to be widely dispersed and largely undefined; the distinction between war and peace will be blurred to the vanishing point. It will be nonlinear, possibly to the point of having no definable battlefields or fronts. The distinction between "civilian" and "military" may disappear. Actions will occur concurrently throughout all participants' depth, including their society as a cultural, not just a physical, entity. Major military facilities, such as airfields, fixed communications sites, and large headquarters will become rarities because of their vulnerability; the same may be true of civilian equivalents, such as seats of government, power plants, and industrial sites (including knowledge as well as manufacturing industries). 125 It is precisely this blurring of peace and war and the demise of traditionally definable battlefields that provides the impetus for the formulation of a new theory of war powers. As evidenced § Marked 16:33 § by Part III, supra, the constitutional allocation of war powers, and the Framers' commitment of the war power to two co-equal branches, was not designed to cope with the current international system, one that is characterized by the persistent machinations of international terrorist organizations, the rise of multilateral alliances, the emergence of rogue states, and the potentially wide proliferation of easily deployable weapons of mass destruction, nuclear and otherwise.

#### Most likely nuclear escalation

Richards 2005 (Dr. Chet Richards, J. Addams & Partners July 12, 2005, “Dear Mr. & Ms. 1RP: Welcome to the 21st Century” http://www.zmetro.com/pdf/2005/07/welcome\_21st\_century\_v4.pdf)

Beginning with Mao Tse-Tung, and continuing to the present day, insurgency and other forms of non-state warfare have become more potent and much more dangerous in at least two ways: Groups other than states – that is, multinational organizations ranging from alQa’ida to the narcotrafficking cartels – are beginning to acquire high levels of sophistication in organization and in the information technologies that allow them to plan and conduct operations while widely dispersed.4 These same groups increasingly have the financial wherewithal to acquire virtually any type of weapon, from small arms to chemical and biological to nuclear, that they need to carry out operations. The only exceptions are conventional weapons such as tanks, combat aircraft, and fighting ships that require large facilities to support them, but are primarily of use only against other military forces armed with the same types of weapons. They are using their new capabilities not only to fight local governments, as was the case with traditional insurgencies, but to attack distant superpowers as well. Because they can’t field sizable amounts of conventional military hardware, fourth generation (4GW) forces will never try to achieve victory by defeating the military forces of a state in stand-up battles. Instead, they will try to convince their state opponent that it is simply not worth it to continue the fight. Successful 4GWcampaigns in modern times would include those against the French in Algeria, the US in Vietnam and the Soviet Union in Afghanistan, where the insurgents never defeated the foreign armies in any major battle, but eventually persuaded the governments back home to withdraw them. In a well run 4GW campaign, everything the 4GW forces do – including fighting and usually losing the occasional major battle – will support this goal. Persuading governments to withdraw forces, rather than defeating them on the battlefield, is an “information age” goal.6 To achieve the necessary level of persuasion, practitioners of 4GWwill use every information tool they can find to spread their messages to the enemy population and decision makers: Our cause is just and no threat to you There’s nothing here worth your effort and sacrifice Your troops are becoming brutal and your tactics ineffective If you keep it up, you’re going to bleed for a very long time So why not just leave now? As we enter the 21st Century, 4GWorganizations are becoming adept at spreading such messages through new channels, such as global news services (CNN, Al Jazeerah) and of course, web sites, blogs, and mass e-mailings. What you may not be aware of is that 4GWorganizations are also using the latest information tools to communicate with each other and to share information, particularly about what is and is not working (what the military calls “lessons learned.”)7Messages may be encrypted, or sent using code phrases, or even hidden in web site images, a practice called steganography. As with so many information age techniques, instructions for encryption and steganography are floating all over the Internet. Information age techniques are ideal for loose networks of highly motivated individuals, which is a typical form of organization for 4GW groups. Modern information warfare places a higher premium on creativity and innovation than it does on things 4GW organizations typically don’t have, like massive forces, volumes of regulations, and expensive hardware.8 By emphasizing speed and innovation, 4GWgroups can often invent new techniques faster than more structured and bureaucratic organizations such as the Pentagon.9 First responder organizations themselves may be targets of information warfare operations. The information systems of 1RP organizations, including operational systems as well as payroll and administrative, might make attractive targets in coordination with a physical attack. This is a real threat: Many members of al-Qa’ida and affiliated groups are from the educated classes in their countries, were technically trained (Osama bin Laden is a civil engineer), studied and lived in the West, and are capable of conceiving and managing such attacks. There are other advantages to the non-state player from operating in a loose social network. Obviously a social network is harder to find than an organization that requires a fixed infrastructure and wears uniforms. But perhaps most significant in wars of the weak against the strong, networks are highly resilient, so killing their leaders and destroying portions of the network can leave the rest to regenerate under new leadership in different locations.1112 So long as enough of the network survives to pass along the ideology and culture, along with lessons learned, the new network will likely be more dangerous and more resilient than its predecessor, much like the more resistant forms of bacteria that can emerge as a result of mis-use of antibiotics. In fact, the European resistance movements during World War II exhibited just this kind of toughness and survivability. In addition to its networked structure, there are other attributes of 4GW that should concern the 1RP (editor’s note: First Responder) community. The first is its transnational nature. An operation can be approved in Afghanistan, planned in Germany, funded in the Middle East, and carried out in the United States, as was the 9/11 attack. There is no one state we can retaliate against, nor one nationality we can profile against. Further, because it is transnational, it can involve networks of networks, such as alQa’ida attempting to cooperate with narco-trafficking organizations in Latin America to trade access to potential base areas and help in infiltrating the US for assistance in distributing narcotics.13 The upshot is that the lack of identifiable 4GW activity may not be an indication that an attack is not in the works, if the su4rveillance is being conducted by someone else. One of the more unpleasant aspects of insurgencies that will likely carry over to 4GWis their use of disguise, camouflage, and the other tools of deception. Because they are militarily weak, 4GW groups survive not by confronting superior firepower but by staying out of its sights. Those that have survived have become masters of concealment and deception, making it even more difficult to pick up early warning signals. This is why simple ethnic or national profiling will not work – 4GWteams will go to great lengths not to be identified as members of the groups in question. Skin color, eye color, and hair color are trivially easy to change, and the criminal infrastructure that already exists in most developed countries makes it simple to get drivers licenses or other means of identification (as any victim of identity theft can attest.) In a pinch, one can always recruit a member of a non-targeted group, such as the “shoe bomber,” Richard Reid, and it would be a mistake to assume the next batch will be as poorly trained. If we’re going to let Icelanders (or grandmothers or parents with toddlers, or whoever) through with less security screening than Saudis or Pakistanis or Jordanians, see if you can guess what the next aircraft hijacker will look like. Another unpleasant fact of 4GW is that like insurgency from whence it sprang, 4GW will be a protracted struggle.14 As Henry Kissinger once noted, if the guerillas don’t lose, they win, so they have all the motivation they need to keep going for as long as they think it will take.15 First responders should not draw comfort from what seems like a pause in attacks – operational cycles can stretch over several years, and a fourth generation war can span decades.16 But the most unpleasant fact of 4GW is that in it, we have finally reached the level of total war.17 In the eyes of the 4GW attacker, there are no civilians and no noncombatants. A concern for public relations offers the only reason for limiting the scope or violence of the attacks. What seems like “terrorism” to us, or senseless, random violence, may appear to the 4GW network as a legitimate way to persuade the foreign state government to withdraw, that is to stop the war. Such a strategy is nothing new. It was what Sherman had in mind during his marches through the South after the fall of Vicksburg (July 1863).18 In its local areas, the 4GW organization will spread the message that the foreign state has killed many civilians, which in a war of an advanced state versus a Third World country will often be true and will always be believed. What this means is that when a 4GW group decides to directly attack the United States or another state involved in “their” struggle, no level of violence, even nuclear, is ruled out. They may calculate that the message they are sending to the state government, to the state’s population, to undecided elements in other parts of the world, and to their own members is worth any backlash from the scenes of horror and brutality that ensue.

#### Congressional notifications destroys the ability to carry out offensive cyber operations

Brennan 2012 [Lieutenant Colonel John W. Brennan 15 March 2012 US Army War College “United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?” http://nsfp.web.unc.edu/files/2012/09/Brennan\_UNITED-STATES-COUNTER-TERRORISM-CYBER-LAW-AND-POLICY.pdf]

As a matter of current U. S. policy, the decision to label a computer network ¶ operation (CNO) as a traditional military activity (TMA), thereby falling under the purview ¶ of Title 10 of the United States Code (USC), or as a covert action under Title 50 of the ¶ USC, has spurred a great deal of discussion at the highest levels of the U. S. ¶ Government.¶ 47¶ Although cyber warfare is only one aspect of the overall current Title ¶ 10/50 debate that is raging within Congress and the various departments within the ¶ executive branch, one cannot legitimately discuss the policies that govern the approvals ¶ to conduct CNOs without touching upon this current source of friction.¶ 48¶ Much of the¶ policy concerning the details of computer network operations is classified, but is gaining ¶ in importance such that many policy experts are speaking about it, some albeit from ¶ under the cloak of anonymity.¶ 49¶ As Andru E. Wall suggests, the confusion over Title 10 ¶ and Title 50 authorities appears to have, “…more to do with congressional oversight ¶ and its attendant internecine power struggles than with operational or statutory ¶ authorities,” despite the fact that by design, Title 10 and 50 authorities are mutually ¶ supporting and were not intended to be competing.¶ 50¶ Retired Admiral Dennis C. Blair ¶ (former ODNI) proclaimed that, “This infuriating business about who’s in charge and ¶ who gets to call the shots is just making us look muscle-bound.” ADM Blair went on to ¶ bemoan the “over-legalistic” approach to CT cyber--despite the fact that current cyber ¶ laws are woefully inadequate to address the, …”complexity of the global information ¶ network.”¶ 51¶ (Wall 2011101)

#### **No Risk of Miscalc over cyber space-US sends the signal that it is a key asset of defense. Future international agreements regulate norms.**

Lewis ’10 The Cyber War Has Not Begun ¶ James Andrew Lewis ¶ Center for Strategic and International Studies ¶ March 2010 http://csis.org/files/publication/100311\_TheCyberWarHasNotBegun.pdf

The problem of defense, involving as it does questions of ideology, domestic regulation, self-interest and painful issues like identity management, will not see rapid progress. There are, however international measures that the Executive Branch can take to reduce risk. First, the United States needs to establish thresholds, signals, and public doctrine on cyber warfare. This will let our opponents better judge the risk of attack and may perhaps have some deterrent effect. The President‟s statement on May 29, 2009 that cyberspace was a critical national asset that the United States would use all means to defend was an important first step, but there has been no following action. It is time to consider moving further. For example, the United States could announce that it sees a distinction between a cyber attack on a deployed military force and an attack on civilian targets in the American homeland and would treat the latter as a strategic threat. Exchanges of information on doctrine and national sensitivities with potential opponents (such as occurred in the Cold War) would reduce the risk for miscalculation in the use of cyber attack. ¶ The risk of miscalculation could also be reduced by international agreement on norms for cyber conflict. Common understandings on how the existing laws of war applied, on the nature of escalation in cyber conflict, and on the responsibilities of states before and during conflict would help to create an international framework to constrain cyber conflict and define the potential consequences for differing levels of hostile action. Some norms would need to be tailored to fit a specific threat; others could apply generally. Norms will not appear magically (although there 4 ¶ are implicit thresholds that could be expanded and made explicit) and cyberspace will continue to be a Hobbesian environment until nations engage to cooperatively define what is responsible behavior in this new domain.

#### **No Cyber war- only agency posturing and fear mongering**

Rid ’13 Cyber War Will Not Take Place¶ by THOMAS RID on 10 MARCH 2013 <http://thomasrid.org/cyber-war-will-not-take-place/> Thomas Rid, reader in war studies at King's College London, is author of "[Cyber War Will Not Take Place](http://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.608939)" and co-author of "[Cyber-Weapons](http://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354)."

‘This book will be welcomed by all those who have struggled to get the measure of the “cyber war” threat. As Thomas Rid takes on the digital doomsters he also provides a comprehensive, authoritative and sophisticated analysis of the strategic quandaries created by new technologies.’ Sir Lawrence Freedman, Professor of War Studies, King’s College London and author of Strategy: A History¶ ‘Thomas Rid provides an unusually level-headed view of where we are in the cyber arms race. This book nips in the bud the loose talk of cyber war and illustrates what’s really happening. Anyone involved in building defences against future attacks should read this book first.’ Mikko Hypponen, virus analyst and Chief Research Officer, F-Secure ¶ ‘We’re in the early years of a cyber war arms race, one fuelled both by fear and ignorance. This book is a cogent counterpoint to both the doomsayers and profiteers, and should be required reading for anyone concerned about our national security policy in cyberspace.’ Bruce Schneier, security guru and author of Liars and Outliers: Enabling the Trust Society Needs to Thrive¶ ‘With news of cyber war, terrorism and espionage seemingly everywhere, separating hype from reality is not always easy. Many agencies and companies stand to gain by inflating cyber security fears. Thomas Rid takes a razor to the evidence and carefully dissects the evolution of conflict and espionage in the cyber age. The result is a compelling and authoritative take on war and strategy in cyberspace, one that will surely be seminal in this area for years to come.’ Ronald J. Deibert, Citizen Lab Director, Professor of Political Science, University of Toronto and author of Black Code: Inside the Battle for Cyberspace ‘Cyber war is coming,’ announced a landmark RAND report in 1993. In 2005, the U.S. Air Force boasted it would now fly, fight, and win in cyberspace, the ‘fifth domain’ of warfare. This book takes stock, twenty years on: is cyber war really coming? Has war indeed entered the fifth domain?¶ Cyber War Will Not Take Place cuts through the hype and takes a fresh look at cyber security. Thomas Rid argues that the focus on war and winning distracts from the real challenge of cyberspace: non-violent confrontation that may rival or even replace violence in surprising ways.

### Advantage 2

#### **Congressional oversight fails cyber operations are labeled as covert.**

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

Under the 1991 law, “covert actions,” those with respect to which “it is¶ intended that the role of the United States Government will not be apparent¶ or acknowledged publicly,”33 need only be reported to a small group of¶ legislators known as the “Gang of Eight,”34 and then only in a “timely¶ fashion,” a term not defined by statute.35 Characterization of U.S. planning¶ and execution of electronic warfare as “covert” could enable reporting to¶ the smaller group, making it more difficult for Congress to play a¶ significant role.36 Moreover, any reporting might be delayed indefinitely Another potential obstacle to congressional involvement is the¶ reportedly common but statutorily unauthorized practice of informal¶ reporting to an even smaller “Gang of Four” – the leaders of the¶ intelligence committees – generally for sensitive non-covert intelligence¶ activities.38

#### International norms won’t solve- definitions, verification, and attribution fail

Rid ’12 [Think Again: Cyberwar](http://www.foreignpolicy.com/articles/2012/02/27/cyberwar)¶ Don't fear the digital bogeyman. Virtual conflict is still more hype than reality.¶ BY THOMAS RID | [MARCH/APRIL 2012](http://www.foreignpolicy.com/issues/192/contents/) Thomas Rid, reader in war studies at King's College London, is author of "[Cyber War Will Not Take Place](http://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.608939)" and co-author of "[Cyber-Weapons](http://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354)

We Need a Cyberarms Control Agreement."¶ We don't. Cyberwar alarmists want the United States to see cybersecurity as a new challenge on a geopolitical scale. They see cyberspace becoming a new area for military competition with rivals such as Russia and China, and they believe new cyberarms limitation agreements are needed to prevent this. There are some rumblings to establish international norms on this topic: The British government convened a conference in London in late 2011, originally intended to make the Internet more secure by agreeing on new rules of the road, and Russia and China proposed at the U.N. General Assembly last September the establishment of an "[international code of conduct for information security](http://blog.internetgovernance.org/pdf/UN-infosec-code.pdf)." Now, diplomats are debating whether the United Nations should try to forge the equivalent of nuclear arms control in cyberspace.¶ So, should it? The answer is no. Attempts to limit cyberweapons through international agreements have three principal problems. The first difficulty is drawing the line between cybercrime and potentially political activity in cyberspace. In January, for instance, a Saudi hacker stole about 20,000 Israeli credit card numbers from a shopping website and leaked the information to the public. In retaliation, a group of Israeli hackers broke into Saudi shopping sites and threatened to release private credit card information.¶ Where is the dividing line? Even if it were possible to distinguish criminal from state-sponsored political activity, they often use the same means. A second hitch is practical: Verification would be impossible. Accurately counting the size of nuclear arsenals and monitoring enrichment activities is already a huge challenge; installing cameras to film programmers and "verify" they don't design malicious software is a pipe dream.¶ The third problem is political, and even more fundamental: Cyberaggressors may act politically, but in sharp contrast with warfare, they are likely to have a strong interest in avoiding attribution. Subversion has always thrived in cyberspace because preserving one's anonymity is easier to achieve than ironclad attribution. That's the root of the political problem: Having a few states agree on cyberarms limitation is about as realistic as a treaty to outlaw espionage and about as practical as outlawing the general subversion of established order.

#### Global polarization prevents agreement, especially with China

Segal and Waxman ’11 Why a Cybersecurity Treaty Is a Pipe DreamAuthors: [Adam Segal](http://www.cfr.org/experts/china-innovation-cybersecurity/adam-segal/b8863), Maurice R. Greenberg Senior Fellow for China Studies, and [Matthew C. Waxman](http://www.cfr.org/experts/cybersecurity-courts-and-tribunals-international-law/matthew-c-waxman/b8695), Adjunct Senior Fellow for Law and Foreign Policy October 27, 2011 Adam Segal is the Ira A. Lipman Senior Fellow for Counterterrorism and National Security Studies at the [Council on Foreign Relations](http://www.cfr.org/). Matthew Waxman, also a fellow at the Council on Foreign Relations, is Associate Professor at Columbia Law School and member of the Hoover Institution Task Force on National Security and Law <http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325>

As a step in that direction, the British government is convening next week the London Conference on Cyberspace to promote new norms of cybersecurity and the free flow of information via digital networks. International diplomacy like this among states and private stakeholders is important and will bring needed attention to these issues. But the London summit is also likely to expose major fault lines, not consensus, on the hardest and most significant problems. The idea of ultimately negotiating a worldwide, comprehensive cybersecurity treaty is a pipe dream.¶ Different interests among powerful states – stemming from different strategic priorities, internal politics, public-private relationships and vulnerabilities – will continue to pull them apart on how cyberspace should be used, regulated, and secured. With the United States and European democracies at one end and China and Russia at another, states disagree sharply over such issues as whether international laws of war and self-defense should apply to cyber attacks, the right to block information from citizens, and the roles that private or quasi-private actors should play in Internet governance. Many emerging Internet powers and developing states lie between these poles, while others are choosing sides.

#### No China offensive capabilies—only focused on preventing domestic hackers

Rid ’12 [Think Again: Cyberwar](http://www.foreignpolicy.com/articles/2012/02/27/cyberwar)¶ Don't fear the digital bogeyman. Virtual conflict is still more hype than reality.¶ BY THOMAS RID | [MARCH/APRIL 2012](http://www.foreignpolicy.com/issues/192/contents/) Thomas Rid, reader in war studies at King's College London, is author of "[Cyber War Will Not Take Place](http://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.608939)" and co-author of "[Cyber-Weapons](http://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354)."

Or so the alarmists tell us. Reality looks quite different. Stuxnet, by far the most sophisticated cyberattack on record, was most likely a U.S.-Israeli operation. Yes, Russia and China have demonstrated significant skills in cyberespionage, but the fierceness of Eastern cyberwarriors and their coded weaponry is almost certainly overrated. When it comes to military-grade offensive attacks, America and Israel seem to be well ahead of the curve.¶ Ironically, it's a different kind of cybersecurity that Russia and China may be more worried about. Why is it that those countries, along with such beacons of liberal democracy as Uzbekistan, have suggested that the United Nations establish an "international code of conduct" for cybersecurity? Cyberespionage was elegantly ignored in the suggested wording for the convention, as virtual break-ins at the Pentagon and Google remain a favorite official and corporate pastime of both countries. But what Western democracies see as constitutionally protected free speech in cyberspace, Moscow and Beijing regard as a new threat to their ability to control their citizens. Cybersecurity has a broader meaning in non-democracies: For them, the worst-case scenario is not collapsing power plants, but collapsing political power.¶ The social media-fueled Arab Spring has provided dictators with a case study in the need to patrol cyberspace not only for subversive code, but also for subversive ideas. The fall of Egypt's Hosni Mubarak and Libya's Muammar al-Qaddafi surely sent shivers down the spines of officials in Russia and China. No wonder the two countries asked for a code of conduct that helps combat activities that use communications technologies -- "including networks" (read: social networks) -- to undermine "political, economic and social stability."¶ § Marked 16:34 § So Russia and China are ahead of the United States, but mostly in defining cybersecurity as the fight against subversive behavior. This is the true cyberwar they are fighting

#### No SCS conflict—economics and deterrence

Creehan 12 – Senior Editor of the SAIS (school of advanced international studies, johns Hopkins) Review of International Affairs (Sean, “Assessing the Risks of Conflict in the South China Sea,” Winter/Spring, SAIS Review, Vol. 32, No. 1)

Regarding Secretary Clinton’s first requirement, the risk of actual closure of the South China Sea remains remote, as instability in the region would affect the entire global economy, raising the price of various goods and commodities. According to some estimates, for example, as much as 50 percent of global oil tanker shipments pass through the South China Sea— that represents more than three times the tanker traffic through the Suez Canal and over five times the tanker traffic through the Panama Canal.4 It is in no country’s interest to see instability there, least of all China’s, given the central economic importance of Chinese exports originating from the country’s major southern ports and energy imports coming through the South China Sea (annual U.S. trade passing through the Sea amounts to $1.2 trillion).5 Invoking the language of nuclear deterrence theory, disruption in these sea lanes implies mutually assured economic destruction, and that possibility should moderate the behavior of all participants. Furthermore§ Marked 16:35 § , with the United States continuing to operate from a position of naval strength (or at least managing a broader alliance that collectively balances China’s naval presence in the future), the sea lanes will remain open. While small military disputes within such a balance of power are, of course, possible, the economic risks of extended conflict are so great that significant changes to the status quo are unlikely.

#### No China/Taiwan war—Both sides will work to avoid war

Jisi 2005 (Wang Jisi, Dean of the School of International Studies at Peking University, China's Serch for Stability With America. Foreign Affairs. Sep/Oct 2005. http://www.foreignaffairs.org/20050901faessay84504/wang-jisi/china-s-search-for-stability-with-america.html)

Meanwhile, at a time when political relations between China and the United States are basically stable and economic and trade links are expanding, Taiwan remains a major source of unease. War between China and the United States over Taiwan would be a nightmare, and both sides will try hard to avoid it. Despite their differences, there is no reason the two sides should have to resort to force to resolve the matter. Yet some people in Taiwan, looking out for their own interests and supported by outsiders -- notably parts of the U.S. defense establishment and certain members of the U.S. Congress -- continue stubbornly to push for independence, ignoring the will of most Taiwanese. It is a mistake for Americans to support such separatists. If a clash occurs, these parties will be responsible.China views the status of Taiwan as an internal matter. But only by coordinating its U.S. policy with its policy toward Taiwan can Beijing curb the separatist forces on the island. Despite U.S. displeasure at China's passage of an antisecession law in March 2005, policymakers in Washington have reiterated their opposition to Taiwan's independence and viewed favorably the spring 2005 visits by Taiwanese opposition leaders to the mainland, which eased cross-strait relations. Nonetheless, Washington has now asked Beijing to talk directly to Taipei's ruling party and its leader, Chen Shui-bian. To improve matters, Chinese and U.S. government agencies and their foreign policy think tanks should launch a sustained and thorough dialogue on the issue and explore ways to prevent separatist forces from making a rash move, dragging both countries toward a confrontation neither wants.

# 2NC

#### Cant find speech doc for the round – extended the mitigative counterstrikes CP and case. Email at [Killernun@gmial.com](mailto:Killernun@gmial.com) if need any cites but we more than likely won’t be reading this CP anymore

# 1NR

## terr

### 2NC Impact Calc (CBW)

#### Nuclear war doesn’t cause extinction

Yehoshua Socol (Ph.D.), an inter-disciplinary physicist, is an expert in electro-optics, high-energy physics and applications, and material science and Moshe Yanovskiy, Jan 2, 2011, “Nuclear Proliferation and Democracy”, http://www.americanthinker.com/2011/01/nuclear\_proliferation\_and\_demo.html

Nuclear proliferation should no longer be treated as an unthinkable nightmare; it is likely to be the future reality. Nuclear weapons have been acquired not only by an extremely poor per capita but large country such as India, but also by even poorer and medium-sized nations such as Pakistan and North Korea. One could also mention South Africa, which successfully acquired a nuclear arsenal despite economic sanctions (the likes of which have not yet been imposed on Iran). It is widely believed that sanctions and rhetoric will not prevent Iran from acquiring nuclear weapons and that many countries, in the Middle East and beyond, will act accordingly (see, e.g., recent Heritage report). Nuclear Warfare -- Myths And Facts The direct consequences of the limited use of nuclear weapons -- especially low-yield devices most likely to be in the hands of non-state actors or irresponsible governments -- **would** probably **not be great enough** to bring about significant geopolitical upheavals. Casualties from a single 20-KT nuclear device are estimated [1] at about 25,000 fatalities with a similar number of injured, assuming a rather unfortunate scenario (the center of a large city, with minimal warning). Scaling the above toll to larger devices or to a larger number of devices is less than linear. For example, it has been estimated that it would take as many as eighty devices of 20-KT yield each to cause 300,000 civilian fatalities in German cities (a result actually achieved by Allied area attacks, or carpet-bombings, during the Second World War). A single 1-MT device used against Detroit has been estimated by U.S. Congress OTA to result in about 220,000 fatalities. It is anticipated that well-prepared civil defense measures, based on rather simple presently known techniques, would decrease these numbers by maybe an order of magnitude (as will be discussed later). There is little doubt that a nation determined to survive and with a strong sense of its own destiny **would not succumb to** such **losses**. It is often argued that the fallout effects of even the limited use of nuclear weapons would be worldwide and would last for generations. This is an **exaggeration**. The following facts speak for themselves. -- In Japan, as assessed by REFR, less than 1,000 excess cancer cases (i.e., above the natural occurrence) were recorded in over 100,000 survivors over the past sixty years -- compared with about 110,000 immediate fatalities in the two atomic bombings. No clinical or even sub-clinical effects were discovered in the survivors' offspring. -- In the Chernobyl area, as assessed by IAEA, only fifteen cancer deaths can be directly attributed to fallout radiation. No radiation-related increase in congenital formations was recorded. Nuclear Conflict -- Possible Scenarios With reference to a possible regional nuclear conflict between a rogue state and a democratic one, the no-winner (mutual assured destruction) scenario is probably false. An analysis by Anthony Cordesman, et al. regarding a possible Israel-Iran nuclear conflict estimated that while Israel might survive an Iranian nuclear blow, Iran would certainly not survive as an organized society. Even though the projected casualties cited in that study seem to us overstated, especially as regards Israel, the conclusion rings true. Due to the extreme high intensity ("above-conventional") of nuclear conflict, it is nearly certain that such a war, no matter its outcome, **would not last for years,** as we have become accustomed to in current low-intensity conflicts. Rather, we should anticipate a new geo-political reality: the emergence of clear winners and losers **within** several **days**, or at most weeks after the initial outbreak of hostilities. This latter reality will most probably contain fewer nuclear-possessing states than the former.

#### CBWs will cause extinction- outweighs nuclear war

Anders Sandberg et al., James Martin Research Fellow, Future of Humanity Institute, Oxford University, "How Can We Reduce the Risk of Human Extinction?" BULLETIN OF THE ATOMIC SCIENTISTS, 9-9-08, http://www.thebulletin.org/web-edition/features/how-can-we-reduce-the-risk-of-human-extinction, accessed 5-2-10.

The risks from anthropogenic hazards appear at present larger than those from natural ones. Although great progress has been made in reducing the number of nuclear weapons in the world, humanity is still threatened by the possibility of a global thermonuclear war and a resulting nuclear winter. We may face even greater risks from emerging technologies. Advances in synthetic biology might make it possible to engineer pathogens capable of extinction-level pandemics. The knowledge, equipment, and materials needed to engineer pathogens are more accessible than those needed to build nuclear weapons. And unlike other weapons, pathogens are self-replicating, allowing a small arsenal to become exponentially destructive. Pathogens have been implicated in the extinctions of many wild species. Although most pandemics "fade out" by reducing the density of susceptible populations, pathogens with wide host ranges in multiple species can reach even isolated individuals. The intentional or unintentional release of engineered pathogens with high transmissibility, latency, and lethality might be capable of causing human extinction. While such an event seems unlikely today, the likelihood may increase as biotechnologies continue to improve at a rate rivaling Moore's Law.

## uq

#### Administration control over cyber-ops now

Fryer-Biggs 2013 [Zachary Fryer-Biggs June 17 2013 Defense News “US Begins To Define Military Cyber Ops” http://www.defensenews.com/article/20130617/DEFREG02/306170027/US-Begins-Define-Military-Cyber-Ops]

Beyond the definitions, the document included several major policy decisions about the use of cyberattack tools. The president maintained a requirement that any cyber operation that involves cyber effects in the US receive his approval but authorized the defense secretary to use DCEO against attackers outside of the United States without first receiving White House approval if action is immediately needed.¶ In May, Defense News reported that the Defense Department was close to completing new classified standing rules of engagement that outline how and when the military would use cyber tools against attackers without seeking presidential consent each time. Those rules will provide greater detail and specificity than the general framework provided in the presidential directive.¶ In a statement, National Security Council spokeswoman Caitlin Hayden described the document as part of the process of updating policy as cyber has evolved.¶ “This directive establishes principles and processes for the use of cyber operations, so that cyber tools are integrated with the full array of national security tools we have at our disposal,” she said. “This directive will establish principles and processes that can enable more effective planning, development and use of our capabilities. It enables us to be flexible, while also exercising restraint in dealing with the threats we face.

#### Offensive cyber ops now- executive controlled

Greenwald and MacAskill 2013 [Glenn Greenwald and Ewen MacAskill 7 June 2013 The Guardian “Obama orders US to draw up overseas target list for cyber-attacks” http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas]

Barack Obama has ordered his senior national security and intelligence officials to draw up a list of potential overseas targets for US cyber-attacks, a top secret presidential directive obtained by the Guardian reveals.¶ The 18-page Presidential Policy Directive 20, issued in October last year but never published, states that what it calls Offensive Cyber Effects Operations (OCEO) "can offer unique and unconventional capabilities to advance US national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging".¶ It says the government will "identify potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power".¶ The directive also contemplates the possible use of cyber actions inside the US, though it specifies that no such domestic operations can be conducted without the prior order of the president, except in cases of emergency. ¶ The aim of the document was "to put in place tools and a framework to enable government to make decisions" on cyber actions, a senior administration official told the Guardian.

## Link

#### Congressional oversight destroys the ability to carry out offensive cyber operations

Brennan 2012 [Lieutenant Colonel John W. Brennan 15 March 2012 US Army War College “United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?” http://nsfp.web.unc.edu/files/2012/09/Brennan\_UNITED-STATES-COUNTER-TERRORISM-CYBER-LAW-AND-POLICY.pdf]

As a matter of current U. S. policy, the decision to label a computer network ¶ operation (CNO) as a traditional military activity (TMA), thereby falling under the purview ¶ of Title 10 of the United States Code (USC), or as a covert action under Title 50 of the ¶ USC, has spurred a great deal of discussion at the highest levels of the U. S. ¶ Government.¶ 47¶ Although cyber warfare is only one aspect of the overall current Title ¶ 10/50 debate that is raging within Congress and the various departments within the ¶ executive branch, one cannot legitimately discuss the policies that govern the approvals ¶ to conduct CNOs without touching upon this current source of friction.¶ 48¶ Much of the¶ policy concerning the details of computer network operations is classified, but is gaining ¶ in importance such that many policy experts are speaking about it, some albeit from ¶ under the cloak of anonymity.¶ 49¶ As Andru E. Wall suggests, the confusion over Title 10 ¶ and Title 50 authorities appears to have, “…more to do with congressional oversight ¶ and its attendant internecine power struggles than with operational or statutory ¶ authorities,” despite the fact that by design, Title 10 and 50 authorities are mutually ¶ supporting and were not intended to be competing.¶ 50¶ Retired Admiral Dennis C. Blair ¶ (former ODNI) proclaimed that, “This infuriating business about who’s in charge and ¶ who gets to call the shots is just making us look muscle-bound.” ADM Blair went on to ¶ bemoan the “over-legalistic” approach to CT cyber--despite the fact that current cyber ¶ laws are woefully inadequate to address the, …”complexity of the global information ¶ network.”¶ 51¶ (Wall 2011101)

#### Unrestricted authority is key to offensive cyber operations

Brennan 2012 [Lieutenant Colonel John W. Brennan 15 March 2012 US Army War College “United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?” http://nsfp.web.unc.edu/files/2012/09/Brennan\_UNITED-STATES-COUNTER-TERRORISM-CYBER-LAW-AND-POLICY.pdf]

Although identifying international terrorists in cyberspace is critical to successful ¶ counterterrorism operations, it is only half of the battle in bringing them to justice. ¶ Monitoring terrorists’ electronic communications is extremely important, but further work ¶ is required by the CT community to isolate, and eventually kill or capture the terrorists¶ overseas. Manipulation or disruption of a terrorist organization’s computer networks is a¶ potential means to this end, and it is also a possible tactic that is employed to preempt a ¶ cyber or kinetic terrorist attack.¶ 37¶ The laws that govern the actual manipulation of ¶ terrorists’ electronic accounts and devices in order to make them more targetable, are ¶ not explicit or simply do not exist. The primary document that gives the President of the ¶ United States the authority to conduct offensive CT cyber operations overseas is the ¶ 2001 Authorization of the Use of Military Force, which gives the president the authority ¶ to “use all necessary and appropriate force” to protect the country for further attacks.¶ 38¶ The extrapolation of this authority which permits the targeting of al-Qa’ida and its ¶ adherents, was employed in order to legally kill Anwar al Awlaki (an American citizen) in ¶ Yemen, and was invoked in permitting the planned (but not executed) computer ¶ network attack against his online magazine, Inspire.¶ 39

#### Restrictions and oversight on cyber operations prevents them from being effective in counterterror

Brennan 2012 [Lieutenant Colonel John W. Brennan 15 March 2012 US Army War College “United States Counter Terrorism Cyber Law and Policy, Enabling or Disabling?” http://nsfp.web.unc.edu/files/2012/09/Brennan\_UNITED-STATES-COUNTER-TERRORISM-CYBER-LAW-AND-POLICY.pdf]

Of considerable concern is the fact that current U. S. CT cyber policies are not ¶ necessarily completely sourced in domestic or international law, and they inhibit ¶ American CT professionals from efficiently implementing the very strategies which they ¶ are charged to execute. These restrictive and hierarchical CT cyber policies clearly ¶ hinder the ability of strategic and operational-level military commanders who are 2-2¶ deployed in support of Overseas Contingency Operations (OCO) to manipulate ¶ cyberspace to their greatest advantage. ¶ In 2010 General David Petraeus, then Commander of United States Central ¶ Command (USCENTCOM) accurately described the degree to which al-Qa’ida was ¶ operating with impunity in cyberspace to finance, command, and recruit its forces.¶ 3¶ The ¶ tactical and operational commanders subordinate to General Petraeus in Iraq and ¶ Afghanistan often lamented that they were permitted to drop two-thousand pound ¶ bombs on terrorists’ homes, but were forced to request from USCENTCOM ¶ Headquarters, or even the Secretary of Defense, the approval to attack or manipulate ¶ terrorists’ computer networks.¶ 4¶ This dichotomous situation flies in the face of logic and is ¶ caused by a trifurcated divergence between: what is expected of military CT ¶ professionals in order kill or capture terrorists; what is permissible under current CT ¶ cyber law; and the current policies that actually govern offensive CT operations in¶ cyberspace.

#### OCO is key to eliminate virtual safe havens

Arquilla 2009 [John Arquilla is professor of defense analysis at the U.S. Naval Postgraduate School and author of Worst Enemy: The Reluctant Transformation of the American Military. 12-12-2009 Foreign Policy “How to Lose a Cyberwar” http://www.foreignpolicy.com/articles/2009/12/11/how\_to\_lose\_a\_cyberwar?page=0,0]

The five young men detained in Pakistan this week -- like a whole new generation of jihadis -- appear to have made considerable use of the Internet in their alleged approach to al Qaeda. Their story points out that, more than eight years after 9/11, terrorist networks are still not only able to stay in touch via cyberspace, but that they are even extending their reach thanks to our giving them a free ride in the virtual domain.¶ U.S. President Barack Obama often speaks about his central strategic objective of denying al Qaeda its haven in Waziristan, but he says nary a word about taking away its "virtual haven" in cyberspace. This omission is more than his alone, as none of the key military, intelligence, and law-enforcement arms of the U.S. government have done much to curtail terrorist use of the Net.¶ Those who do try to keep an eye on terrorism in cyberspace often argue that they learn a lot about enemy networks by monitoring their narratives on jihadi websites. But if this made a real difference, we would have already won the war on terror.¶ Instead of thinking of cyberspace principally as a place to gather intelligence, we need to elevate it to the status of "battlespace." This means that we either want to exploit terrorists' use of the Web and Net unbeknownst to them, or we want to drive them from it.

# Adv

creehan

the United States continuing to operate from a position of naval strength (or at least managing a broader alliance that collectively balances China’s naval presence in the future), the sea lanes will remain open. While small military disputes within such a balance of power are, of course, possible, the economic risks of extended conflict are so great that significant changes to the status quo are unlikely.

#### Multiple factors ensure cooperation

Zhu ’12 – professor in the School of International Studies and the deputy director of the Center for International and Strategic Studies at Beijing University (Zhu Feng, “No One Wants a Clash,” May 3, New York Times, <http://www.nytimes.com/roomfordebate/2012/05/02/are-we-headed-for-a-cold-war-with-china/no-one-wants-a-cold-war-between-the-us-and-china>)

However there is little worry that the two powers will collide into a “new cold war.” First of all, China’s authoritarian system has been tremendously mobilized for international integration. Beijing has been pretty conservative and doesn’t welcome democratization. But it does not strictly adhere to traditional communism either. Any new confrontation like the cold war would risk a huge backlash in China by greatly damaging the better-off Chinese people. Such a conflict could ultimately undermine the Communist Party’s ruling legitimacy.¶ Second, the power disparity between Washington and China hasn’t significantly narrowed, regardless of Chinese achievements in the past decades. My view is that Beijing remains an adolescent power, and should learn how to be a great power rather than unwisely rushing to any confrontation. Though some Chinese want the nation to assert itself more forcefully, the huge disparity in power should keep China in place. China is in no position to challenge the U.S. But China will be more enthusiastic and straightfoward about addressing and safeguarding its legal interests. Competition between Washington and Beijing will intensify, but that does not automatically mean that the relationship will be unmanageable.¶ Lastly, the cycle of action and reaction has mostly turned out to be fruitful for the U.S. and China. Further competition § Marked 17:22 § is promising. The U.S. doesn’t want to put China in a corner, or force Beijing to stand up desperately. The dealings over many thorny issues have respond? The country’s cold war experience offers a useful strategy. The stalemate imposed by “mutually assured destruction” that prevented the US-Soviet conflict from igniting created a sense of stability. Today, the US and China are locked in a new form of “proved that each side wants to handle the conflict, not escalate it. Chen Guangcheng’s departure from the U.S. Embassy is telling evidence. Neither side wants diplomatic confrontation. Rather, it seems that both sides are struggling to react constructively.¶ In the years to come, China-U.S. relations will continue to be very complicated, but also very important. The glue to keep these two nations together is not pragmatism only, but mutual interest — especially in trade.

#### No US/China war—It’s in neither country’s best interest

Ackerman 2011 (Robert Ackerman, May 10, 2011, “War Between China, U.S. Not Likely,” http://www.afcea.org/signal/signalscape/index.php/2011/05/10/11510/)

The United States and China are not likely to go to war with each other because neither country wants it and it would run counter to both nations’ best interests. That was the conclusion of a plenary panel session hosted by former Good Morning America host David Hartman at the 2011 Joint Warfighting Conference in Virginia Beach. Adm. Timothy J. Keating, USN (Ret.), former head of the U.S. Pacific Command, noted that China actually wants the United States to remain active in the Asia-Pacific region as a hedge against any other country’s adventurism. And, most of the other countries in that region want the United States to remain active as a hedge against China. Among areas of concern for China is North Korea. Wallace “Chip” Gregson, former assistant secretary of Defense for Asian and Pacific Security Affairs, said that above all China fears instability, and a North Korean collapse or war could send millions of refugees streaming into Manchuria, which has economic problems of its own.