### 1nc---disad

#### Debt ceiling will be raised now but it’s not certain --- Obama’s ironclad political capital is forcing the GOP to give in

Brian Beutler 10/3/13, “Republicans finally confronting reality: They’re trapped!,” Salon <http://www.salon.com/2013/10/03/republicans_finally_confronting_reality_theyre_trapped/>

After struggling for weeks and weeks in stages one through four, Republicans are finally entering the final stage of grief over the death of their belief that President Obama would begin offering concessions in exchange for an increase in the debt limit.¶ The catalyzing event appears to have been an hour-plus-long meeting between Obama and congressional leaders at the White House on Wednesday. Senior administration officials say that if the meeting accomplished only one thing it was to convey to Republican leaders the extent of Obama’s determination not to negotiate with them over the budget until after they fund the government and increase the debt limit. These officials say his will here is stronger than at any time since he decided to press ahead with healthcare reform after Scott Brown ended the Democrats’ Senate supermajority in 2010.¶ There’s evidence that it sunk in.¶ First, there’s this hot mic moment in which Senate Minority Leader Mitch McConnell tells Sen. Rand Paul, R-Ky., that the president’s position is ironclad.¶ Then we learn that House Speaker John Boehner has told at least one House Republican privately what he and McConnell have hinted at publicly for months, which is that they won’t execute their debt limit hostage. Boehner specifically said, according to a New York Times report, and obliquely confirmed by a House GOP aide, that he would increase the debt limit before defaulting even if he lost more than half his conference on a vote.¶ None of this is to say that Republicans have “folded” exactly, but they’ve pulled the curtain back before the stage has been fully set for the final act, and revealed who’s being fitted with the red dye packet.

#### Plan costs pc

Mark Young 12, Executive Director, Directorate of Plans and Policy, United States Cyber Command, 12 [“United States Government Cybersecurity Relationships,” I/S: A JOURNAL OF LAW AND POLICY, vol 8, no 2, pdf]

Fear of the loss of departmental resources and authority, and the perceived need to control information in and about federal agencies, encourages unilateral approaches to federal network operations and defense. The Center of Strategic and International Studies reported on the unsatisfying progress in U.S. cybersecurity: Unsurprisingly, protecting “turf” played a role [in slowing cybersecurity progress]. Cyber functions are scattered across the executive branch. Reorganization could mean that some offices would have to surrender control. The different offices argue that this would put important equities that they now oversee at risk. Turf concerns intertwine with the conceptual dispute over innovation, economics, and the nature of the Internet. The cabinet agencies also have little interest in supporting a stronger White House role in cybersecurity, as it would diminish their independence.19

#### Obama’s political capital is key --- it’s his sole focus now

Jonathan Allen 9/19, Politico, 9/19/13, GOP battles boost President Obama, dyn.politico.com/printstory.cfm?uuid=17961849-5BE5-43CA-B1BC-ED8A12A534EB

There’s a simple reason President Barack Obama is using his bully pulpit to focus the nation’s attention on the battle over the budget: In this fight, he’s watching Republicans take swings at each other. And that GOP fight is a lifeline for an administration that had been scrambling to gain control its message after battling congressional Democrats on the potential use of military force in Syria and the possible nomination of Larry Summers to run the Federal Reserve. If House Republicans and Obama can’t cut even a short-term deal for a continuing resolution, the government’s authority to spend money will run out on Oct. 1. Within weeks, the nation will default on its debt if an agreement isn’t reached to raise the federal debt limit. For some Republicans, those deadlines represent a leverage point that can be used to force Obama to slash his health care law. For others, they’re a zero hour at which the party will implode if it doesn’t cut a deal. Meanwhile, “on the looming fiscal issues, Democrats — both liberal and conservative, executive and congressional — are virtually 100 percent united,” said Sen. Charles Schumer (D-N.Y.). Just a few days ago, all that Obama and his aides could talk about were Syria and Summers. Now, they’re bringing their party together and shining a white hot light on Republican disunity over whether to shut down the government and plunge the nation into default in a vain effort to stop Obamacare from going into effect. The squabbling among Republicans has gotten so vicious that a Twitter hashtag — #GOPvsGOPugliness — has become a thick virtual data file for tracking the intraparty insults. Moderates, and even some conservatives, are slamming Texas Sen. Ted Cruz, a tea party favorite, for ramping up grassroots expectations that the GOP will shut down the government if it can’t win concessions from the president to “defund” his signature health care law. “I didn’t go to Harvard or Princeton, but I can count,” Sen. Bob Corker (R-Tenn.) tweeted, subtly mocking Cruz’s Ivy League education. “The defunding box canyon is a tactic that will fail and weaken our position.” While it is well-timed for the White House to interrupt a bad slide, Obama’s singular focus on the budget battle is hardly a last-minute shift. Instead, it is a return to the narrative arc that the White House was working to build before the Syria crisis intervened. And it’s so important to the president’s strategy that White House officials didn’t consider postponing Monday’s rollout of the most partisan and high-stakes phase even when a shooter murdered a dozen people at Washington’s Navy Yard that morning. The basic storyline, well under way over the summer, was to have the president point to parts of his agenda, including reducing the costs of college and housing, designed to strengthen the middle class; use them to make the case that he not only saved the country from economic disaster but is fighting to bolster the nation’s finances on both the macro and household level; and then argue that Republicans’ desire to lock in the sequester and leverage a debt-ceiling increase for Obamacare cuts would reverse progress made. The president is on firm ground, White House officials say, because he stands with the public in believing that the government shouldn’t shut down and that the country should pay its bills.

#### Debt ceiling collapses the global economy --- fast timeframe and no resiliency

Adam Davidson 9/10/13, economy columnist for The New York Times, co-founder of Planet Money, NPR’s team of economics reporters, “Our Debt to Society,” NYT, http://www.nytimes.com/2013/09/15/magazine/our-debt-to-society.html?pagewanted=all&\_r=0

If the debt ceiling isn’t lifted again this fall, some serious financial decisions will have to be made. Perhaps the government can skimp on its foreign aid or furlough all of NASA, but eventually the big-ticket items, like Social Security and Medicare, will have to be cut. At some point, the government won’t be able to pay interest on its bonds and will enter what’s known as sovereign default, the ultimate national financial disaster achieved by countries like Zimbabwe, Ecuador and Argentina (and now Greece). In the case of the United States, though, it won’t be an isolated national crisis. If the American government can’t stand behind the dollar, the world’s benchmark currency, then the global financial system will very likely enter a new era in which there is much less trade and much less economic growth. It would be, by most accounts, the largest self-imposed financial disaster in history.¶ Nearly everyone involved predicts that someone will blink before this disaster occurs. Yet a small number of House Republicans (one political analyst told me it’s no more than 20) appear willing to see what happens if the debt ceiling isn’t raised — at least for a bit. This could be used as leverage to force Democrats to drastically cut government spending and eliminate President Obama’s signature health-care-reform plan. In fact, Representative Tom Price, a Georgia Republican, told me that the whole problem could be avoided if the president agreed to drastically cut spending and lower taxes. Still, it is hard to put this act of game theory into historic context. Plenty of countries — and some cities, like Detroit — have defaulted on their financial obligations, but only because their governments ran out of money to pay their bills. No wealthy country has ever voluntarily decided — in the middle of an economic recovery, no less — to default. And there’s certainly no record of that happening to the country that controls the global reserve currency.¶ Like many, I assumed a self-imposed U.S. debt crisis might unfold like most involuntary ones. If the debt ceiling isn’t raised by X-Day, I figured, the world’s investors would begin to see America as an unstable investment and rush to sell their Treasury bonds. The U.S. government, desperate to hold on to investment, would then raise interest rates far higher, hurtling up rates on credit cards, student loans, mortgages and corporate borrowing — which would effectively put a clamp on all trade and spending. The U.S. economy would collapse far worse than anything we’ve seen in the past several years.¶ Instead, Robert Auwaerter, head of bond investing for Vanguard, the world’s largest mutual-fund company, told me that the collapse might be more insidious. “You know what happens when the market gets upset?” he said. “There’s a flight to quality. Investors buy Treasury bonds. It’s a bit perverse.” In other words, if the U.S. comes within shouting distance of a default (which Auwaerter is confident won’t happen), the world’s investors — absent a safer alternative, given the recent fates of the euro and the yen — might actually buy even more Treasury bonds. Indeed, interest rates would fall and the bond markets would soar.¶ While this possibility might not sound so bad, it’s really far more damaging than the apocalyptic one I imagined. Rather than resulting in a sudden crisis, failure to raise the debt ceiling would lead to a slow bleed. Scott Mather, head of the global portfolio at Pimco, the world’s largest private bond fund, explained that while governments and institutions might go on a U.S.-bond buying frenzy in the wake of a debt-ceiling panic, they would eventually recognize that the U.S. government was not going through an odd, temporary bit of insanity. They would eventually conclude that it had become permanently less reliable. Mather imagines institutional investors and governments turning to a basket of currencies, putting their savings in a mix of U.S., European, Canadian, Australian and Japanese bonds. Over the course of decades, the U.S. would lose its unique role in the global economy.¶ The U.S. benefits enormously from its status as global reserve currency and safe haven. Our interest and mortgage rates are lower; companies are able to borrow money to finance their new products more cheaply. As a result, there is much more economic activity and more wealth in America than there would be otherwise. If that status erodes, the U.S. economy’s peaks will be lower and recessions deeper; future generations will have fewer job opportunities and suffer more when the economy falters. And, Mather points out, no other country would benefit from America’s diminished status. When you make the base risk-free asset more risky, the entire global economy becomes riskier and costlier.

#### Economic collapse causes global nuclear war

Cesare Merlini 11, nonresident senior fellow at the Center on the United States and Europe and chairman of the Board of Trustees of the Italian Institute for International Affairs, May 2011, “A Post-Secular World?”, Survival, Vol. 53, No. 2

Two neatly opposed scenarios for the future of the world order illustrate the range of possibilities, albeit at the risk of oversimplification. The first scenario entails the premature crumbling of the post-Westphalian system. One or more of the acute tensions apparent today evolves into an open and traditional conflict between states, perhaps even involving the use of nuclear weapons. The crisis might be triggered by a collapse of the global economic and financial system, the vulnerability of which we have just experienced, and the prospect of a second Great Depression, with consequences for peace and democracy similar to those of the first. Whatever the trigger, the unlimited exercise of national sovereignty, exclusive self-interest and rejection of outside interference would self-interest and rejection of outside interference would likely be amplified, emptying, perhaps entirely, the half-full glass of multilateralism, including the UN and the European Union. Many of the more likely conflicts, such as between Israel and Iran or India and Pakistan, have potential religious dimensions. Short of war, tensions such as those related to immigration might become unbearable. Familiar issues of creed and identity could be exacerbated. One way or another, the secular rational approach would be sidestepped by a return to theocratic absolutes, competing or converging with secular absolutes such as unbridled nationalism**.**

### 1nc---topicality

#### Restrictions are prohibitions on action --- the aff is oversight

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

3. The ordinary definition of the term "restrictions" also does not include the reporting and monitoring or supervising terms and conditions that are included in the 2001 Stipulation.

Black's Law Dictionary, 'fifth edition,(1979) defines "restriction" as;

A limitation often imposed in a deed or lease respecting the use to which the property may be put. The term "restrict' is also cross referenced with the term "restrain." Restrain is defined as; To limit, confine, abridge, narrow down, restrict, obstruct, impede, hinder, stay, destroy. To prohibit from action; to put compulsion on; to restrict; to hold or press back. To keep in check; to hold back from acting, proceeding, or advancing, either by physical or moral force, or by interposing obstacle, to repress or suppress, to curb.

In contrast, the terms "supervise" and "supervisor" are defined as; To have general oversight over, to superintend or to inspect. See Supervisor. A surveyor or overseer. . . In a broad sense, one having authority over others, to superintend and direct. The term "supervisor" means an individual having authority, in the interest of the employer, to hire, transfer, suspend, layoff, recall, promote, discharge, assign, reward, or discipline other employees, or responsibility to direct them, or to adjust their grievances, or effectively to recommend such action, if in connection with the foregoing the exercise of such authority is not of a merely routine or clerical nature, but required the use of independent judgment.

Comparing the above definitions, it is clear that the definition of "restriction" is very different from the definition of "supervision"-very few of the same words are used to explain or define the different terms. In his 2001 stipulation, Mr. Kincheloe essentially agreed to some supervision conditions, but he did not agree to restrict his license.

#### Restrictions on authority are distinct from conditions

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

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

#### Vote neg---

#### Neg ground---only prohibitions on particular actions guarantee links to every core argument like flexibility and deference

#### Precision---only our interpretation defines “restrictions on authority”---that’s key to adequate preparation and policy analysis

#### Limits---there are an infinite number of small hoops they could require the president to jump through---overstretches our research burden

### 1nc---k

#### Security threats are political constructions by experts to justify constant militarism

Aziz Rana 12, Assistant Professor of Law, Cornell University Law School; A.B., Harvard College; J.D., Yale Law School; PhD., Harvard University, July 2012, “NATIONAL SECURITY: LEAD ARTICLE: Who Decides on Security?,” 44 Conn. L. Rev. 1417

Despite such democratic concerns, a large part of what makes today's dominant security concept so compelling are two purportedly objective sociological claims about the nature of modern threat. As these claims undergird the current security concept, this conclusion assesses them more directly and, in the process, indicates what they suggest about the prospects for any future reform. The first claim is that global interdependence means that the United States faces near continuous threats from abroad. Just as Pearl Harbor presented a physical attack on the homeland justifying a revised framework, the American position in the world since has been one of permanent insecurity in the face of new, equally objective dangers. Although today these threats no longer come from menacing totalitarian regimes like Nazi Germany or the Soviet Union, they nonetheless create a world of chaos and instability in which American domestic peace is imperiled by decentralized terrorists and aggressive rogue states. n310¶ [\*1486] ¶ Second, and relatedly, the objective complexity of modern threats makes it impossible for ordinary citizens to comprehend fully the causes and likely consequences of existing dangers. Thus, the best response is the further entrenchment of the national security state, with the U.S. military permanently mobilized to gather intelligence and to combat enemies wherever they strike-at home or abroad. Accordingly, modern legal and political institutions that privilege executive authority and insulated decision-making are simply the necessary consequence of these externally generated crises. Regardless of these trade-offs, the security benefits of an empowered presidency-one armed with countless secret and public agencies as well as with a truly global military footprint n311 -greatly outweigh the costs.¶ Yet although these sociological views have become commonplace, the conclusions that Americans should draw about security requirements are not nearly as clear cut as the conventional wisdom assumes. In particular, a closer examination of contemporary arguments about endemic danger suggests that such claims are not objective empirical judgments, but rather are socially complex and politically infused interpretations. Indeed, the openness of existing circumstances to multiple interpretations of threat implies that the presumptive need for secrecy and centralization is not self-evident. And as underscored by high profile failures in expert assessment, claims to security expertise are themselves riddled with ideological presuppositions and subjective biases. All this indicates that the gulf between elite knowledge and lay incomprehension in matters of security may be far less extensive than is ordinarily thought. It also means that the question of who decides-and with it the issue of how democratic or insular our institutions should be-remains open as well.¶ Clearly, technological changes, from airpower to biological and chemical weapons, have shifted the nature of America's position in the [\*1487] world and its potential vulnerability. As has been widely remarked for nearly a century, the oceans alone cannot guarantee our permanent safety. Yet in truth, they never fully ensured domestic tranquility. The nineteenth century was one of near continuous violence, especially with indigenous communities fighting to protect their territory from expansionist settlers. n312 But even if technological shifts make doomsday scenarios more chilling than those faced by Hamilton, Jefferson, or Taney, the mere existence of these scenarios tells us little about their likelihood or how best to address them. Indeed, these latter security judgments are inevitably permeated with subjective political assessments-assessments that carry with them preexisting ideological points of view-such as regarding how much risk constitutional societies should accept or how interventionist states should be in foreign policy.¶ In fact, from its emergence in the 1930s and 1940s, supporters of the modern security concept have-at times unwittingly-reaffirmed the political rather than purely objective nature of interpreting external threats. In particular, commentators have repeatedly noted the link between the idea of insecurity and America's post- World War II position of global primacy, one which today has only expanded following the Cold War. n313 In 1961, none other than Senator James William Fulbright declared, in terms reminiscent of Herring and Frankfurter, that security imperatives meant that "our basic constitutional machinery, admirably suited to the needs of a remote agrarian republic in the 18th century," was no longer "adequate" for the "20th-century nation." n314 For Fulbright, the driving impetus behind the need to jettison antiquated constitutional practices was the importance of sustaining the country's "pre-eminen[ce] in political and military power." n315 Fulbright believed that greater executive action and war- making capacities were essential precisely because the United States found itself "burdened with all the enormous responsibilities that accompany such power." n316 According to Fulbright, the United States had [\*1488] both a right and a duty to suppress those forms of chaos and disorder that existed at the edges of American authority. n317 Thus, rather than being purely objective, the American condition of permanent danger was itself deeply tied to political calculations about the importance of global primacy. What generated the condition of continual crisis was not only technological change, but also the belief that the United States' own national security rested on the successful projection of power into the internal affairs of foreign states.¶ The key point is that regardless of whether one agrees with such an underlying project, the value of this project is ultimately an open political question. This suggests that whether distant crises should be viewed as generating insecurity at home is similarly as much an interpretative judgment as an empirically verifiable conclusion. n318 To appreciate the open nature of security determinations, one need only look at the presentation of terrorism as a principle and overriding danger facing the country. According to National Counterterrorism Center's 2009 Report on Terrorism, in 2009 there were just twenty-five U.S. noncombatant fatalities from terrorism worldwide-nine abroad and sixteen at home. n319 While the fear of a terrorist attack is a legitimate concern, these numbers-which have been consistent in recent years-place the gravity of the threat in perspective. Rather than a condition of endemic danger-requiring ever-increasing secrecy and centralization-such facts are perfectly consistent with a reading that Americans do not face an existential crisis (one presumably comparable to Pearl Harbor) and actually enjoy relative security. Indeed, the disconnect between numbers and resources expended, especially in a time of profound economic insecurity, highlights the political choice of policymakers and citizens to persist in interpreting foreign events through a World War II and early Cold War lens of permanent threat. In fact, the continuous alteration of basic constitutional values to fit national security aims emphasizes just how entrenched Herring's old vision of security as pre-political and foundational has become, regardless of whether other interpretations of the present moment may be equally compelling.¶ It also underscores a telling and often ignored point about the nature of [\*1489] modern security expertise, particularly as reproduced by the United States' massive intelligence infrastructure. To the extent that political assumptions-like the centrality of global primacy or the view that instability abroad necessarily implicates security at home-shape the interpretative approach of executive officials, what passes as objective security expertise is itself intertwined with contested claims about how to view external actors and their motivations. These assumptions mean that while modern conditions may well be complex, the conclusions of the presumed experts may not be systematically less liable to subjective bias than judgments made by ordinary citizens based on publicly available information. It further underlines that the question of who decides cannot be foreclosed in advance by simply asserting deference to elite knowledge.¶ If anything, one can argue that the presumptive gulf between elite awareness and suspect mass opinion has generated its own very dramatic political and legal pathologies. In recent years, the country has witnessed a variety of security crises built on the basic failure of "expertise." n320 At present, part of what obscures this fact is the very culture of secret information sustained by the modern security concept. Today, it is commonplace for government officials to leak security material about terrorism or external threats to newspapers as a method of shaping the public debate. n321 These "open" secrets allow greater public access to elite information and embody a central and routine instrument for incorporating mass voice into state decision-making.

#### Don’t call it an alternative---our response is to interrogate the epistemological failures of the 1ac---this is a prereq to successful policy

Ahmed 12 Dr. Nafeez Mosaddeq Ahmed is Executive Director of the Institute for Policy Research and Development (IPRD), an independent think tank focused on the study of violent conflict, he has taught at the Department of International Relations, University of Sussex "The international relations of crisis and the crisis of international relations: from the securitisation of scarcity to the militarisation of society" Global Change, Peace & Security Volume 23, Issue 3, 2011 Taylor Francis

While recommendations to shift our frame of orientation away from conventional state-centrism toward a 'human security' approach are valid, this cannot be achieved without confronting the deeper theoretical assumptions underlying conventional approaches to 'non-traditional' security issues.106 By occluding the structural origin and systemic dynamic of global ecological, energy and economic crises, orthodox approaches are incapable of transforming them. Coupled with their excessive state-centrism, this means they operate largely at the level of 'surface' impacts of global crises in terms of how they will affect quite traditional security issues relative to sustaining state integrity, such as international terrorism, violent conflict and population movements. Global crises end up fuelling the projection of risk onto social networks, groups and countries that cross the geopolitical fault-lines of these 'surface' impacts - which happen to intersect largely with Muslim communities. Hence, regions particularly vulnerable to climate change impacts, containing large repositories of hydrocarbon energy resources, or subject to demographic transformations in the context of rising population pressures, have become the focus of state security planning in the context of counter-terrorism operations abroad.

The intensifying problematisation and externalisation of Muslim-majority regions and populations by Western security agencies - as a discourse - is therefore not only interwoven with growing state perceptions of global crisis acceleration, but driven ultimately by an epistemological failure to interrogate the systemic causes of this acceleration in collective state policies (which themselves occur in the context of particular social, political and economic structures). This expansion of militarisation is thus coeval with the subliminal normative presumption that the social relations of the perpetrators, in this case Western states, must be protected and perpetuated at any cost - precisely because the efficacy of the prevailing geopolitical and economic order is ideologically beyond question.

As much as this analysis highlights a direct link between global systemic crises, social polarisation and state militarisation, it fundamentally undermines the idea of a symbiotic link between natural resources and conflict per se. Neither 'resource shortages' nor 'resource abundance' (in ecological, energy, food and monetary terms) necessitate conflict by themselves.

There are two key operative factors that determine whether either condition could lead to conflict. The first is the extent to which either condition can generate socio-political crises that challenge or undermine the prevailing order. The second is the way in which stakeholder actors choose to actually respond to the latter crises. To understand these factors accurately requires close attention to the political, economic and ideological strictures of resource exploitation, consumption and distribution between different social groups and classes. Overlooking the systematic causes of social crisis leads to a heightened tendency to problematise its symptoms, in the forms of challenges from particular social groups. This can lead to externalisation of those groups, and the legitimisation of violence towards them.

Ultimately, this systems approach to global crises strongly suggests that conventional policy 'reform' is woefully inadequate. Global warming and energy depletion are manifestations of a civilisation which is in overshoot. The current scale and organisation of human activities is breaching the limits of the wider environmental and natural resource systems in which industrial civilisation is embedded. This breach is now increasingly visible in the form of two interlinked crises in global food production and the global financial system. In short, industrial civilisation in its current form is unsustainable. This calls for a process of wholesale civilisational transition to adapt to the inevitable arrival of the post-carbon era through social, political and economic transformation.

Yet conventional theoretical and policy approaches fail to (1) fully engage with the gravity of research in the natural sciences and (2) translate the social science implications of this research in terms of the embeddedness of human social systems in natural systems. Hence, lacking capacity for epistemological self-reflection and inhibiting the transformative responses urgently required, they reify and normalise mass violence against diverse 'Others', newly constructed as traditional security threats enormously amplified by global crises - a process that guarantees the intensification and globalisation of insecurity on the road to ecological, energy and economic catastrophe. Such an outcome, of course, is not inevitable, but extensive new transdisciplinary research in IR and the wider social sciences - drawing on and integrating human and critical security studies, political ecology, historical sociology and historical materialism, while engaging directly with developments in the natural sciences - is urgently required to develop coherent conceptual frameworks which could inform more sober, effective, and joined-up policy-making on these issues.

###  1nc---counterplan

The President of the United States should issue an executive order clarifying that offensive cyber operations presumptively rely on covert action authority and, unless being conducted as part of a conflict already authorized by Congress, require classified ex ante reports to congressional intelligence committees or the “Gang of Eight” whenever possible. When ex ante reports are not possible, the President must submit a timely ex post report with an explanation for the necessity of the delay.

#### Counterplan is the best middle ground --- solves oversight and legal legitimacy of cyberattacks while preserving presidential flexibility --- doesn’t link to politics

Brecher 12 Aaron Brecher is a JD candidate @ the University of Michigan Law School. “Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations,” December, 111 Mich. L. Rev. 423, Lexis

This Part argues that the federal government should adopt the presumption that cyberattacks will be carried out under the covert action statute, and that the best way forward is for the president to issue an executive order making the covert action regime the presumptive framework for cyberattacks. It includes a brief discussion of why a president might willingly constrain her discretion by issuing the proposed executive order. It also shows that while the internal executive processes associated with both military and intelligence legal frameworks help mitigate the risk of cyberattacks' misuse by the executive, only the covert action regime provides an adequate role for Congress. Finally, this Part argues that the executive order option is preferable to one alternative proposed by scholars - enacting legislation - because of the practical difficulties of passing new legislation. The covert action regime is the best approach for committing cyberattacks under the current law, as it would facilitate cooperation among executive agencies. The debate over which agency and set of legal authorities govern cyberattacks has caused no small amount of confusion. n145 Apparently, an Office of Legal Counsel ("OLC") memorandum declined to decide which legal regime should govern the use of cyberattacks, and the uncertainty has led to interagency squabbles, as well as confusion over how cyberattacks are to be regulated. n146 Establishing a presumptive answer would go far toward resolving this dispute. Most importantly, adopting the covert action framework as the presumptive legal regime would be a principled way to help ensure constitutional legitimacy when the president orders a cyberattack.n147 There is also reason to believe that presidential power is intimately bound up in credibility, which in turn is largely dependent on the perception of presidential compliance with applicable domestic law. n148 A practice of complying with the covert action [\*448] regime for cyberattacks, both when they do not constitute a use of force and when it is unclear whether they do, is most likely to be in compliance with the law. Compliance with the covert action regime would also encourage covert action procedures in close cases without unduly restricting the executive's choice to use military authorities in appropriate circumstances. The executive might also issue the proposed order, even though it would limit her freedom in some ways, because of the possible benefits of constraining future administrations or preempting legislative intervention. n149 For example, in this context, an administration may choose to follow the finding and reporting requirements in order to convince Congress that legislative intervention is unnecessary for proper oversight. This is acceptable if the covert action regime is in fact adequate on its own. Moreover, if greater statutory control over cyberattacks is needed, the information shared with Congress may give Congress the tools and knowledge of the issue necessary to craft related legislation. n150 Additionally, while executive orders are hardly binding, the inertia following adoption of an order may help constrain future administrations, which may be more or less trustworthy than the current one. Creating a presumption through an executive order also establishes a stable legal framework for cyberattacks that allows law to follow policy in this new field, and permits decisionmakers to learn more about the nature of cyberoperations before passing detailed statutes that may result in unintended consequences. A presumption in favor of the title 50 regime for cyberattacks is also desirable because it comports with the reality of an executive constrained by its own internal processes. Though energy, dispatch, and secrecy are among the key advantages the executive possesses over Congress, n151 the existence of a professional bureaucratic corps, including many lawyers, within the executive branch can foster necessary deliberation about important policy decisions. n152 For issues on which there is disagreement among executive agencies, such as a potential turf war between the military and intelligence communities over control of cyberattacks, advisory and adjudicatory bodies such as the Office of Legal Counsel can play a constructive role. n153 Even on an issue such as the best legal regime to govern cyberattacks, which is essentially [\*449] a policy choice, the friction between different competing agencies itself can serve a checking function. n154 Moreover, the covert action statute helps with the vital work of balancing the president's need for independence against the costs of an uninformed Congress, n155 especially on national security issues with such potential for unforeseeable diplomatic and military risks. The national interests at stake in the cyberattack context are too great to be left to the president alone. n156

### 1nc---arms races adv

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

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

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

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

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

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

#### Cyber-war impacts are a joke --- easily correctable

Zenko & Cohen 12 – Micah Zenko, Fellow in the Center for Preventive Action at the Council on Foreign Relations; and Michael A. Cohen, Fellow at the Century Foundation, March/April 2012, “Clear and Present Safety,” Foreign Affairs, Vol. 91, No. 2, p. 79-93

A more recent bogeyman in national security debates is the threat of so-called cyberwar. Policymakers and pundits have been warning for more than a decade about an imminent "cyber-Pearl Harbor" or "cyber-9/11." In June 2011, then Deputy Defense Secretary William Lynn said that "bits and bytes can be as threatening as bullets and bombs." And in September 2011, Admiral Mike Mullen, then chairman of the Joint Chiefs of Staff, described cyberattacks as an "existential" threat that "actually can bring us to our knees."¶ Although the potential vulnerability of private businesses and government agencies to cyberattacks has increased, the alleged threat of cyberwarfare crumbles under scrutiny. No cyberattack has resulted in the loss of a single U.S. citizen's life. Reports of "kinetic-like" cyberattacks, such as one on an Illinois water plant and a North Korean attack on U.S. government servers, have proved baseless. Pentagon networks are attacked thousands of times a day by individuals and foreign intelligence agencies; so, too, are servers in the private sector. But the vast majority of these attacks fail wherever adequate safeguards have been put in place. Certainly, none is even vaguely comparable to Pearl Harbor or 9/11, and most can be offset by commonsense prevention and mitigation efforts.

#### No cyberwar --- too difficult and unpredictable

Ian Brown 11, Associate Director of the Cyber Security Centre @ the University of Oxford, and Peter Sommers, Professor @ the London School of Economics, Reducing Systemic Cybersecurity Risk,” OECD, 1/14, http://www.oecd.org/governance/risk/46889922.pdf

It is unlikely that there will ever be a true cyberwar. The reasons are: many critical computer systems are protected against known exploits and malware so that designers of new cyberweapons have to identify new weaknesses and exploits; the effects of cyberattacks are difficult to predict – on the one hand they may be less powerful than hoped but may also have more extensive outcomes arising from the interconnectedness of systems, resulting in unwanted damage to perpetrators and their allies. More importantly, there is no strategic reason why any aggressor would limit themselves to only one class of weaponry.

### 1nc---allies adv

#### Allied cyber coop high

John Reed 12, national security reporter for Foreign Policy, 9/10, “U.S. swapping cyber notes with allies,” http://killerapps.foreignpolicy.com/posts/2012/09/10/us\_now\_swapping\_notes\_on\_cyber\_attacks\_with\_closest\_allies

The Defense Department has reached what Pentagon officials describe a key agreement with some of the United States' closest international allies to share information in the cyber realm.¶ The agreement allows the Pentagon to quickly share broad amounts of information on cyber attacks with the four other members of the so-called Five Eyes intelligence-sharing group (formally known as the UKUSA Agreement): the United Kingdom, Canada, Australia, and New Zealand.¶ "We have far more ability to share, particularly in relation to network defense and information assurance, than we've ever had previously. That's very positive," said Marine Corps Maj. Gen. George Allen, director of plans and policy for U.S. Cyber Command said on August 16. "I think you'll see a far better partnership with our coalition partners than you've ever seen" as the Five Eyes countries integrate the information into their exercises and planning.¶ "At this point it's not a full treaty because it's more an operational type cooperation; it's through a policy type memorandum of understanding," Eric Rosenbach, deputy assistant secretary of defense for cyber policy told Killer Apps during a Sept. 4 interview while discussing how the U.S. shares cyber information with its closest allies. The cyber information-sharing agreement falls under a 2003 MOU on general information sharing between the Five Eyes, according to a DoD spokesman.¶ The agreement will speed up information sharing, which is crucial in cyber, Allen said: "It's extremely important because you may see a certain threat in the U.K. that we haven't yet seen in the U.S. and you want to be able to try to bolster your defenses by seeing that before it hits us. We still have a long way to go on near real time information sharing but the technology is there."¶ Agreements like the one between the Five Eyes are being reached as a result of a National Disclosure Policy regarding the sharing of sensitive cyber information that was enacted "just a couple of months ago," said Allen.¶ The new policy also allows less extensive information sharing with other U.S. allies around the globe, according to Allen.¶ "In some cases [info-sharing agreements are part of] a bilateral relationship, depending upon the country, in other cases we have agreements with groups of countries that come together," such as the Five Eyes, explained DoD's Chief Information Officer, Teri Takai to Killer Apps during a Sept. 4 interview.¶ Defense officials say that information sharing partnerships like this one are badly needed to defeat cyber attacks since the cyber domain transcends national borders. Not only can attacks originate abroad, hackers in one country going after networks in another can often disguise their attacks to appear as if they are emanating from servers in a third nation. Furthermore, not all countries have the ability to detect cyber threats and attacks quickly. This means that a country whose servers are hijacked may not even know that it is hosting an attack.¶ "The more we can build a solid relationship with a partner, the more we're going to be able to crack the code in rapid information sharing, indications, and warnings with those partners," said Army Maj. Gen. John Davis, the military's top advisor for cyber to the undersecretary of defense for policy on August 15.¶ "If we can do that, we can get these partners to rapidly react to [cyber attacks] that we may be seeing that they may not see. We may be able to tip and cue them so that they can take action. If some of their equipment is being hijacked, we can inform them, and if we have good working relationships we can leverage that to get them to take action rather than relying on any type of U.S. government activity because then you run into issues of sovereignty and that can be very complex," he said.¶ To that end, the Five Eyes countries are already sharing lessons learned on how to defend networks, according to Davis.¶ "We are able to leverage lessons from across the five eyes, and in fact, where we find some of these nations that have particular skill or abilities in one area or another, may lead a common forum to develop that and share it with the rest of the group," said Davis.

#### New military doctrine means no A2AD threat

Jonathan Greenert 12, Chief of Naval Operations, 5/10/12, “Projecting Power, Assuring Access,” http://cno.navylive.dodlive.mil/2012/05/10/projecting-power-assuring-access/

There’s been attention recently about closing an international strait using, among other means, mines, fast boats, cruise missiles and mini-subs. These weapons are all elements of what we call an “Anti-Access /Area Denial (A2AD)” strategy. Keeping with my tenet of “Warfighting First,” I want to highlight for you how the Navy and Air Force have been planning to deal with A2AD threats like this today and into the future.¶ A goal of an A2AD strategy is to make others believe it can close off international airspace or waterways and that U.S. military forces will not be able (or willing to pay the cost) to reopen those areas or come to the aid of our allies and partners. In peacetime, this gives the country with the A2AD weapons leverage over their neighbors and reduces U.S. influence. In wartime, A2AD capabilities can make U.S. power projection more difficult. The areas where A2AD threats are most consequential are what I call “strategic maritime crossroads.” These include areas around the Straits of Hormuz and Gibraltar, Suez Canal, Panama Canal or Malacca Strait – but strategic crossroads can also exist in the air, on land, and in cyberspace.¶ To counter these strategies and assure U.S. freedom of action, Navy and Air Force spearheaded a comprehensive study, which included Army and Marine Corps participation, to bring forward a concept called Air Sea Battle (ASB). This concept identifies how we will defeat A2AD capabilities such as cyber attack, mines, submarines, cruise and ballistic missiles, and air defense systems and, where applicable, “natural access denial” such as weather, pollution, natural disaster, etc. The concept also describes what we will need to do these operations, especially as the threats improve due to technological advancements.¶ Air-Sea Battle relies on tightly coordinated operations across domains (air, land, maritime, undersea, space and cyberspace) to defeat A2AD capabilities, such as a submarine striking air defenses in support of Air Force bombers, Air Force stealth fighters destroying a radar site to prevent cruise missile attacks on Navy ships, or a Navy cryptologic technician (CT) confusing a radar system to allow an Air Force UAV to attack an enemy command center. This level of real-time coordination requires new approaches to developing systems, planning operations, and conducting command and control.¶ By working across domains, Air-Sea Battle takes advantage of unique U.S. advantages in global reach (long-range tankers, nuclear-powered carriers), and stealth above (F-22 and B-2) and below (SSN, SSGN) the sea. Putting Air Force and Navy capabilities together also creates new combinations of systems, or “kill-chains”, for warfighting operations that can add redundancy or make us more efficient. For example, a threat cruise missile could be detected by an Air Force E-3 AWACS or Navy E-2D Hawkeye, and if we invest in the right data links, either of them could cue an Air Force F-22, Aegis ship or Navy F/A-18 to engage the missile. This provides more “paths” we can follow to destroy the missile.¶ Using these integrated air and naval forces, the Air Sea Battle concept executes three main lines of effort:¶ Disrupt an adversary’s command, control, communications, computers and intelligence, surveillance and reconnaissance (C4ISR) – this reduces the adversary’s ability to find or target us with large raids; they will have to spread out their attacks to all our potential locations.¶ Destroy adversary weapons launch systems – To have sustained access to international seas and skies, we will eventually need to destroy the launchers on land, sea and in the air.¶ Defeat adversary weapons – until we destroy the launchers, our forces will kinetically or non-kinetically prevent the weapons launched at us from getting a hit.¶ We are using the Air Sea Battle concept to guide decisions in procurement, doctrine, organization, training, leadership, personnel and facilities. Our budgets for FY11, FY12 and now FY13 reflect hard choices that support Air-Sea Battle. In some cases we accepted reductions in capacity to ensure the needed capabilities were retained.

#### Zero data supports the resolve or credibility thesis

Jonathan Mercer 13, associate professor of political science at the University of Washington in Seattle and a Fellow at the Center for International Studies at the London School of Economics, 5/13/13, “Bad Reputation,” <http://www.foreignaffairs.com/articles/136577/jonathan-mercer/bad-reputation>

Since then, the debate about what to do in Syria has been sidetracked by discussions of how central reputation is to deterrence, and whether protecting it is worth going to war.

There are two ways to answer those questions: through evidence and through logic. The first approach is easy. Do leaders assume that other leaders who have been irresolute in the past will be irresolute in the future and that, therefore, their threats are not credible? No; broad and deep evidence dispels that notion. In studies of the various political crises leading up to World War I and of those before and during the Korean War, I found that leaders did indeed worry about their reputations. But their worries were often mistaken.

For example, when North Korea attacked South Korea in 1950, U.S. Secretary of State Dean Acheson was certain that America’s credibility was on the line. He believed that the United States’ allies in the West were in a state of “near-panic, as they watched to see whether the United States would act.” He was wrong. When one British cabinet secretary remarked to British Prime Minister Clement Attlee that Korea was “a rather distant obligation,” Attlee responded, “Distant -- yes, but nonetheless an obligation.” For their part, the French were indeed worried, but not because they doubted U.S. credibility. Instead, they feared that American resolve would lead to a major war over a strategically inconsequential piece of territory. Later, once the war was underway, Acheson feared that Chinese leaders thought the United States was “too feeble or hesitant to make a genuine stand,” as the CIA put it, and could therefore “be bullied or bluffed into backing down before Communist might.” In fact, Mao thought no such thing. He believed that the Americans intended to destroy his revolution, perhaps with nuclear weapons.

Similarly, Ted Hopf, a professor of political science at the National University of Singapore, has found that the Soviet Union did not think the United States was irresolute for abandoning Vietnam; instead, Soviet officials were surprised that Americans would sacrifice so much for something the Soviets viewed as tangential to U.S. interests. And, in his study of Cold War showdowns, Dartmouth College professor Daryl Press found reputation to have been unimportant. During the Cuban Missile Crisis, the Soviets threatened to attack Berlin in response to any American use of force against Cuba; despite a long record of Soviet bluff and bluster over Berlin, policymakers in the United States took these threats seriously. As the record shows, reputations do not matter.

#### No spillover — lack of credibility in one commitment doesn’t affect others at all

Paul K. MacDonald 11, Assistant Professor of Political Science at Williams College, and Joseph M. Parent, Assistant Professor of Political Science at the University of Miami, Spring 2011, “Graceful Decline?: The Surprising Success of Great Power Retrenchment,” International Security, Vol. 35, No. 4, p. 7-44

Second, pessimists overstate the extent to which a policy of retrenchment can damage a great power's capabilities or prestige. Gilpin, in particular, assumes that a great power's commitments are on equal footing and interdependent. In practice, however, great powers make commitments of varying degrees that are functionally independent of one another. Concession in one area need not be seen as influencing a commitment in another area.25 Far from being perceived as interdependent, great power commitments are often seen as being rivalrous, so that abandoning commitments in one area may actually bolster the strength of a commitment in another area. During the Korean War, for instance, President Harry Truman's administration explicitly backed away from total victory on the peninsula to strengthen deterrence in Europe.26 Retreat in an area of lesser importance freed up resources and signaled a strong commitment to an area of greater significance.

#### No South China Sea impact

Richard Katz 13 Richard Katz is the editor of the semiweekly Oriental Economist Alert, a report on the Japanese economy. “Mutual Assured Production,” Foreign Affairs, July/August, Vol. 92, Issue 4, EBSCO

Why Trade Will Limit Conflict Between China and Japan¶ During the Cold War, the United States and the Soviet Union carefully avoided triggering a nuclear war because of the assumption of "mutual assured destruction": each knew that any such conflict would mean the obliteration of both countries. Today, even though tensions between China and Japan are rising, an economic version of mutual deterrence is preserving the uneasy status quo between the two sides.¶ Last fall, as the countries escalated their quarrel over an island chain that Japan has controlled for more than a century, many Chinese citizens boycotted Japanese products and took to the streets in anti-Japanese riots. This commotion, at times encouraged by the Chinese government, led the Japanese government to fear that Beijing might exploit Japan's reliance on China as an export market to squeeze Tokyo into making territorial concessions. Throughout the crisis, Japan has doubted that China would ever try to forcibly seize the islands -- barren rocks known in Chinese as the Diaoyu Islands and in Japanese as the Senkaku Islands -- if only because the United States has made it clear that it would come to Japan's defense. Japanese security experts, however, have suggested that China might try other methods of intimidation, including a prolonged economic boycott.¶ But these fears have not materialized, for one simple reason: China needs to buy Japanese products as much as Japan needs to sell them. Many of the high-tech products assembled in and exported from China, often on behalf of American and European firms, use advanced Japanese-made parts. China could not boycott Japan, let alone precipitate an actual conflict, without stymieing the export-fueled economic miracle that underpins Communist Party rule.¶ For the moment, the combination of economic interdependence and Washington's commitment to Japan's defense will likely keep the peace. Still, an accidental clash of armed ships around the islands could lead to an unintended conflict. That is why defense officials from both countries have met with an eye to reducing that particular risk. With no resolution in sight, those who fear an escalation can nonetheless take solace in the fact that China and Japan stand to gain far more from trading than from fighting.

#### And, US will always deter China---even if they acted it would only cause a diplomatic fuss

Vu Duc ‘13 "Khanh Vu Duc is a Vietnamese-Canadian lawyer who researches on Vietnamese politics, international relations and international law. He is a frequent contributor to Asia Sentinel and BBC Vietnamese Service, "Who's Bluffing Whom in the South China Sea?" www.asiasentinel.com/index.php?option=com\_content&task=view&id=5237&Itemid=171

Conversely, China would find an increased American presence unacceptable and a nuisance. Of course, **neither country is likely to find itself staring down the barrel of the other's gu**n. China's plans for the region would undoubtedly be under greater American scrutiny if Washington decides to allocate more assets to Asia-Pacific.

For the US, returning in force to Asia-Pacific would prove to be a costly endeavour, resources the country may or may not be able to muster. Yet, even if this is true, Washington's calculations may determine that the security risk posed by China in the region outweighs whatever investment required by the US.

China's dispute with Japan over the Senkaku/Diaoyu Island, however heated, will prove to be a peripheral issue with respect to China's dispute with the several claimant states over the Spratlys. Ultimately, it is not improbable that China would seize one or several of the Spratlys under foreign control as a means to demonstrate its resolve in the disputes and the region; but to do so is to engage in unnecessary risk. The consequences stemming from such action are too great for Beijing to ignore.

**Although it is unlikely that China's neighbors would be able to mount more than a diplomatic protest**, the fuss deriving from such an incident could prove more burdensome for China than it is willing to risk. The real consequence for China of any and all conflict in the region is and has always been an American intervention. As is, it would benefit Beijing to seek a peaceful, mutually agreed upon resolution, rather than brute force.

#### **No Taiwan war**

Scott L. Kastner 8/15/13 PhD in Political Science and an Associate Professor, Department of Government and Politics, University of Maryland, College Park, 8/15/13, "A Relationship Transformed? Rethinking the prospects for conflict and peace in the Taiwan Strait," http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2300070**After long being viewed as** potential **flashpoint, relations across the Taiwan Strait have stabilized** tremendously in recent years, **reflecting moderation in the approaches** both **Beijing and Taipei have taken with regard to the** cross-Strait **sovereignty dispute.** This moderation has been most evident in Taiwan, where Ma Ying-jeou was elected president in 2008 (and reelected in 2012) after campaigning on an explicitly pro-status quo platform. But **Beijing also moderated its Taiwan policies in recent years, most notably by adopting a more flexible approach to the “one China” principle**, de-emphasizing the “one country, two systems” model for cross-Strait political integration (which was widely seen in Taiwan as being a non-starter), and consenting to the use of the “1992 consensus” as a basis for restarting quasi-official cross-Strait dialogue (which had been moribund for nearly a decade before 2008). **The result has been an unprecedented improvement in relations across the Taiwan Strait, reflected in frequent dialogue between officials** from the two sides**, numerous cooperative agreements** (including, most notably, the 2010 Economic Cooperation Framework Agreement), the **establishment of direct travel and commercial linkages across the Strait, and a** sharp **reduction in PRC threats of military force.** In this paper, I consider whether this new-found stability in the Taiwan Strait is likely to persist. To do so, I first discuss at some length how a conflict in the Taiwan Strait could occur. In particular, I consider several possible pathways to conflict that worried analysts of cross-Strait relations prior to the post-2008 détente. I then consider how fundamental trends in cross-Strait relations—such as rapidly growing Chinese military power and deepening cross-Strait economic exchange—are affecting the likelihood that any of these scenarios will emerge as future concerns. My (preliminary) analysis suggests that **the relationship across the Taiwan Strait is likely to be more stable in the years ahead than was the case in the years preceding 2008**; **this conclusion holds even if there is a change in ruling party in Taiwan.**

#### Economic interdependence prevents US-China conflict

Dobbins et al ’11 – James Dobbins is the director of the RAND International Security and Defense Policy Center, David C. Gompert is a Senior Fellow at the RAND Corporation. He is also former Senior Advisor for National Security and Defense for the Coalition Provisional Authority of Iraq, David A Shlapak is a Senior International Policy Analyst with Rand Corporation, and Andrew Scobell is Senior Political Scientist at RAND's Washington, DC, office and former Associate Professor of International Affairs at the Bush School of Government and Public Service at Texas A&M University (“Conflict with China: Prospects, Consequences, and Strategies for Deterrence,” RAND Corporation, <http://www.rand.org/pubs/occasional_papers/OP344>)

Short of a nuclear exchange, the greatest damage from any conflict with China is likely to come in the economic realm. Massive and mutual economic harm would indeed result from any significant Sino-U.S. armed conflict, even if the two sides eschewed employment of economic weapons. The two economies are linked with each other and with the rest of the world in a manner unparalleled in history. This mutual dependency can be an immensely powerful deterrent, in effect a form of mutually assured economic destruction. At the moment the balance of advantage rests with the United States, but even the winner in such a contest will wish it had been avoided.¶ The operation of MAED is somewhat different from classic mutual assured destruction (MAD). It is at least theoretically possible to limit the escalation of a military clash to the subnuclear level. It is not possible to so limit the economic consequences. China is not going to continue buying U.S. Treasury notes while the American and Chinese navies clash somewhere off Taiwan or in the South China Sea. Apple is not going to be shipping iPads from its factories in China. Markets will anticipate widespread disruption in U.S.-Chinese and world trade, and advance the consequences, however much Beijing and Washington seek to limit the damage.

#### No US intervention

**Sollenberger 10**, student at the Johns Hopkins University, graduate Swarthmore and analyst, [Matthew, spring, “Challenging US Command of the Commons:Evolving Chinese defense technologies as a threat to American hegemony?”, <http://bcjournal.org/2010/challenging-us-command-of-the-commons/>]

The advancement of Chinese military capabilities in the areas of information warfare, anti-access measures, and strategic nuclear forces has substantially altered the strategic environment surrounding a US-China conflict, particularly in the Chinese littoral theaters. By hampering US intelligence gathering and communication assets and using anti-access measures, China could delay a US military response to a possible confrontation across the Taiwan Strait. Given the Chinese-Taiwanese balance of forces, which has tilted significantly against Taiwan in the last years, any delay in the US response to such a crisis could allow China to achieve its unification goals militarily and present the US with a fait accompli. Meanwhile, China’s enhanced capability to inflict substantial damage on US military and civilian assets at different levels of escalation has increased the costs of a potential military conflict between the US and China and thus, may reduce the readiness of US decision-makers to intervene in favor of Taiwan – particularly given China’s evolving ability to withstand US nuclear coercion and deny the US potential benefits from escalation. China has thus effectively challenged US command of the commons, contesting US military power in several key areas. By definition, this erodes one of the pillars of hegemony, namely unrivaled military prowess.

#### No war and escalation

**GS 6** (Global Security, China's Options in the Taiwan Confrontation, http://www.globalsecurity.org/military/ops/taiwan-prc.htm)

With a belief that the US will come to Taiwan's aid should China initiate action to curb any independence-like moves, Chen has continued a campaign toward independence, betting on sympathetic voters to side with his positions. By 2005, however, the independence card had been trumped by the mainland's policy of reconciliation, and overshadowed by other domestic issues. While China has long avowed to prevent Taiwan's declaration of independence by force, if required, their response to current trends in Taiwan thus far has been **significantly tempered**.

China does not want to repeat the results of the 1995-96 Taiwan Strait missile crisis in which PRC military actions adversely influenced (in Beijing eyes) Taiwanese opinions and resulted in President Lee Teng-hui's re-election. Beijing recognizes that the economic and diplomatic costs of **even measured military responses** to the situation in Taiwan would be enormously high, and as such they will reserve such activity as an absolute last resort.

Should Chen begin openly promoting an independence platform, Beijing could undertake an escalating series of actions to bring Taiwan back into line. China's leaders will choose their courses of action (COA) based on the COA's perceived impact on internal stability and government authority. They can neither afford to risk growing unemployment during a period of fantastic economic growth nor risk appearing weak in dealing with one of their three primary separatist movements (Taiwan, Xinjiang, and Tibet).

It is generally assumed that China would likely attack Taiwan under certain previously defined circumstances [China's "Five Noes"]:

a formal declaration of independence by Taipei

a military alliance by Taiwan with a foreign power, or foreign intervention in Taiwan's internal affairs

indefinite delays in resumption of cross-Strait dialogue, and an unwillingness to negotiate on the basis of 'one China'

Taiwan's acquisition of nuclear weapons or other weapons of mass destruction

internal unrest or turmoil on Taiwan

As of mid-2004 President Hu Jintao's government was emphasizing formal independence, US-ROC cooperation on technology to defeat a PRC attack, and the lack of progress in negotiations.

Conversely, China's precise definition of "reunification" is somewhat opaque. In November 2004 Tang Jiaxuan, who was foreign minister until 2003, and serves as a vice minister in the Taiwan Affairs Office of the State Council, said that after reunification, Taiwan would enjoy broader autonomy than Hong Kong and Macao. He suggested that Taiwan could preserve its social system; freely choose its leaders; keep the first right of legal jurisdiction; not pay taxes to the central government; preserve its own armed forces and police; have external foreign commercial, economic, trade and cultural relations; and purchase some offensive weapons. Furthermore, the central government in Beijing would not send officials to Taiwan but island officials could be part of the central government.

A walk down the escalation ladder may illustrate the range of possible actions that may be expected. Those rungs on the escalation ladder of greatest interest are those that may not provoke direct American response, but that would demonstrate the dispositive influence of Beijing over the status of the territory presently controlled by the Taipei regime, and Beijing's ultimate control over the relationship between that territory and the rest of the world.

Diplomatic Initiatives

Although a climb at least mid-way up the escalation ladder has some surface appeal and plausibility, there is surely a case to be made that the costs to Beijing will outweigh the benefits, and that in any event such a provocative course of action would merely play into Taiwan's gameplan for reducing the ambiguity of American commitments in its favor. Taiwan's declaratory shift has not been followed by overt acts, such as President Lee's 1996 visit to the United States, and indeed its declaratory initiative has been rebuffed by the US Government and by others. The counsel of patience would suggest that time is on Beijing's side, and that at some point the post-Lee leadership in Taipei will recognize the futility of his "state to state" formulation and return to some more constructive approach.

Military Exercises

At a minimum, the PLA may repeat the military posturing of March 1996, and indeed it is difficult to imagine how a response of at least this intensity can be avoided under some circumstances. It is predictable, however, that the United States will respond by the deployment of military forces to some carefully calibrated locale, and that these manuevers alone will do little to resolve the present political crisis. To the extent that Taiwan's political challenge is viewed as being more substantial than that of 1995-96, a simple repetition of the firepower displays of that crisis could demonstrate a lack of credibility and resolve on the part of Beijing, and could be readily characterized as inadequate.

Unconventional Warfare

Chinese attacks on critical infrastructure could unsettle Taiwan's economy without provoking American military involvement, and perhaps without even being directly attributable to the Chinese government. Although apparently coincidental, the island-wide blackout of late July 1999 is illustrative of such possibilities, and subsequently reported attacks on government computer systems may forshadow more ambitious attacks.

On 04 October 2004 Richard Lawless, Deputy Undersecretary of Defence, warned the US-Taiwan Business Council China is developing the means to electronically blockade Taiwan with attacks to the island's vital utilities, the Internet and other communications networks. He warned that China might first target things that keep Taiwan's high-tech society running if a war broke out between China and Taiwan. "China is actively developing options to create chaos on the island, to compromise components of Taiwan's critical infrastructure - telecommunications, utilities, broadcast media, cellular, Internet and computer networks," he saidl. Such a strategy could be called an "acupuncture" attack aimed at "the destruction of a national will" with "the insertion of a hundred needles."

It is rather difficult to envision effective modalities for American enhancements to Taiwan's physical or technical security to counter such infrastructure attacks beyond modest technical assistance efforts. Although the potentially unattributable character of infrastructure attacks would deny Beijing the pleasure of explicit mastery over Taiwan, the absence of attribution would not diminish the impact on Taiwan's economy nor would it diminish from the depiction of Taipei as lacking effective control over its nominal territory.

Peripheral Assaults

Taiwan occupies one island in the disputed Spratly chain, and the handful of small islands occupied by Taiwan near the mainland coast are far less heavily fortified than Quemoy and Matsu. Chinese seizure of these otherwise insiginificant specks of real estate could be accomplished with relative ease, and as with a partial naval blockade would concrete demonstrate Beijing's dispositive influence over territory claimed by Taipei. The United States is extremely unlikely to assist Taiwan in the recovery of the legally disputed Spratly, and would be only somewhat less unlikely to directly participate in the recovery by Taiwan of minor specks of territory in the Taiwan Strait.

Naval Blockade

The PLA Navy would face serious difficulties in coordinating an effective naval blockade enforced through the combined efforts of air, surface, and submarine forces. But the reaction by Taiwan and the international community to the PLA's March 1996 exercises and missile tests suggests that less comprehensive measures could substantially disrupt Taiwan's economic life, potentially creating pressure over time for a political settlement. Depending on the modalities of such an embargo, the United States might have difficulty in identifying politically appropriate or militarily effective means of countering Beijing's interdiction of international commerce with Taiwan. Mine-sweeping operations might not be sufficiently effective to restore the confidence of commercial shippers, and the US Navy might be loath to proactively sink Chinese submarines that were not immediately attacking friendly shipping. Consequently, a partially effective Chinese blockade of Taiwan would appear to be an attactive option for concretely demonstrating China's ultimate authority over Taiwan without prokoking an American military challenge to this assertion.

Air Operations

Air operations could be conducted in concert with a naval blockade, amphibious operations, missile strikes against Taiwan-held islands, or missile strikes against Taiwan. Taipei's qualitative advantages would help offset the PLA's numerical superiority. But air operations could cause great damage that might eventually enable China to achieve air superiority, and could force Taipei into a political settlement on China's terms unless Taiwan were to receive external assistance. The United States would almost certainly be prepared to provide aircraft and ordnance to replace combat losses, though it is rather difficult to imagine modern counterparts to the "Flying Tigers." It is unclear how or whether American carrier-based aviation would be used to enforce a no-fly zone in the Taiwan Strait. Such enforcement would probably come towards the end of a military crisis to either administer a cease fire or revser the declining fortunes of Taiwan. American carrier aviation combat operations at the outset of a Chinese air campaign against Taiwan would appear unlikely under current US declaratory policy, although there could be substantial Congressional pressure for such a committment.

Full-scale Invasion

A main force attack to "Liberate Taiwan" would be an extremely high risk undertaking with uncertain prospects for success. Invasion is unlikely, since the PLA cannot yet transport a credible invasion force to Taiwan. Amphibious forces are capable of transporting no more than a single division [15,000 troops], and military air transports could add possibly an additional divisions worth of troops. Taipei would have significant warning time if Beijing were to prepare for an invasion, and could mobilize significant reserves that would outnumber the invading force by a wide margin. Taiwan retains significant qualitative advantages against the numerically superior PLA in fighter aircraft, surface warships, air defenses, and many ground force capabilities.

Although it is unlikely that China would initiate the use of weapons of mass destruction in the context of a conventional invasion of Taiwan, it is possible that Taiwan would initiate the use of chemical weapons in respose to such an invasion in the event that a purely conventional military response appeared inadequate. In any event, if Beijing's amphibious assault did not spontaneously collapse, such an invasion would almost certainly provoke an American intervention sufficient to terminate hostilities on terms unfavorable to Beijing, unless Taiwan collapses before America can intervene.

Every spring China masses amphibious units on their coast facing Taiwan. The Pentagon normally dismisses Chinese amphibious exercises as "routine" though they could provide an opportunity for a standing start "out-of-the-blue" (OOTB) surprise attack. Taiwan has responded by having some warships at sea and some aircraft in the air during Chinese exercises.

In the 20th Century, China's amphibious exercises were mainly designed to intimidate Taiwan. The annual Dongshan drill started in 1996. In these exercises, the emphasis was on crossing the 130km-wide Taiwan Strait and landing on Taiwan itself. But with the new century, the PLA began to address logistical issues, questions of timing, and command and control problems.

Of particular note is the fact that the PLA has been frequently conducting offensive "integrated" (Yitihua) training with a focus on the use of armed forces against Taiwan and blocking the US military intervention. The concepts of integration (yitihua) and seamless operations (feixianxing zuozhan) are defined as tying together the five dimensions of warfare - air, land, sea, space, and the electromagnetic spectrum, integrating sensors with mobile missiles, air, and sea-based forces.

In June 2001 the numbers of Chinese forces massing in the "Liberation No. 1." exercise were three times higher than during previous exercises of this kind. The main goals of the exercises were reported to be practicing "attacking and occupying an outlying Taiwanese island and fighting off an aircraft carrier." The exercise, which lasted for four months, was the biggest since 1996.

China held two large-scale amphibious exercises in 2004 (division to group-army level in size), one of which explicitly dealt with a Taiwan scenario, bringing the total number of amphibious exercises to ten over the previous five years. In June and July 2004 exercises were conducted on Dongshan Island in southeastern Fujian province, just 150 nautical miles west of Taiwan's Penghu Island. The military wargames were aimed at "taking control of the Taiwan Strait", with 18,000 troops and the amphibious landing of a tank brigade. Soldiers deployed on Dongshan Island in mid-May 2004, with tanks and armoured personnel carriers practicing amphibious landings on Jinluan beach.

During July 2004 China conducted exercise "Liberation Number Two", commanded by Chief of General Staff General Liang Guanglie, an expert on amphibious warfare. However, during the 2004 exercise off the Fujian coast, the Chinese military tested its ability to capture the Penghu archipelago not far from Taiwan. This was the first time the chain of 64 islands, lying east of the midway line between Taiwan and the mainland, was the target. Observers sugggested that the People's Liberation Army had adopted a cautious, step-by-step approach in its preparations for a showdown with Taiwan. After the 'Liberation Number One' drill on Dongshan island in 2001, the PLA concluded that it would suffer significant losses if it failed to control Penghu.

In 2004 a computer simulation suggested that it would take China six days to complete the occupation of Taiwan. When this was publicly reported, "authoritative military sources" told Taiwan media that, in fact, Taiwan could hold out for two weeks. The logic behind this view is that Taiwan has to hold out until the US comes to its aid and, given thespeed of US military deployment, the longer the better.

Early arriving forces, often involving warships stationed close to the Strait, would be of particular importance in a short conflict over Taiwan. At an expected average speed of 25 knots, over long Pacific Ocean distances, US submarines, aircraft carriers, cruisers and destroyers based in San Diego, CA would take nearly 10 days to reach an area east of Taiwan after setting sail. By contrast, a US warship based in Yokosuka, Japan, would take just under two days, one in Guam would take 2.2 days, and a ship sailing from Pearl Harbor in Hawaii would take more than seven days.

Nuclear Attack on Taiwan

China would almost certainly not contemplate a nuclear strike against Taiwan, nor would Beijing embark on a course of action that posed significant risks of the use of nuclear weapons. The mainland's long term goal is to liberate Taiwan, not to obliterate it, and any use of nuclear weapons by China would run a substantial risk of the use of nuclear weapons by the United States. An inability to control escalation beyond "demonstrative" detonations would cause utterly disproportionate destruction.

#### Drones destroy U.S. credibility---outweighs detention

Stephen Holmes 13, the Walter E. Meyer Professor of Law, New York University School of Law, July 2013, “What’s in it for Obama?,” The London Review of Books, <http://www.lrb.co.uk/v35/n14/stephen-holmes/whats-in-it-for-obama>

On the basis of undisclosed evidence, evaluated in unspecified procedures by rotating personnel with heterogeneous backgrounds, the US is continuing to kill those it classifies as suspected terrorists in Somalia, Yemen and Pakistan. It has certainly been eliminating militants who had nothing to do with 9/11, including local insurgents fighting local battles who, while posing no realistic threat to America, had allied themselves opportunistically with international anti-American jihadists. By following the latter wherever they go, the US is allowing ragtag militants to impose ever new fronts in its secret aerial war. Mistakes are made and can’t be hidden, at least not from local populations. Nor can the resentment of surrounding communities be easily assuaged. This is because, even when it finds its target, the US is killing not those who are demonstrably guilty of widely acknowledged crimes but rather those who, it is predicted, will commit crimes in the future. Of course, the civilian populations in the countries where these strikes take place will never accept the hunches of CIA or Pentagon futurologists. And so they will never accept American claims about the justice of Obama’s slimmed-down war on terror, but instead claim the right of self-defence, and this would be true even if drone operators could become as error-free as Brennan once claimed they already are. But of course collateral damage and mistaken-identity strikes will continue. They are inevitable accompaniments of all warfare. And they, too, along with intentional killings that are never publicly justified, will communicate resoundingly to the world that the arbitrary and unpredictable killing of innocent Muslims falls within America’s commodious concept of a just war.

The rage such strikes incite will be all the greater if onlookers believe, as seems likely, that the killing they observe makes relatively little contribution to the safety of Americans. Indeed, this is already happening, which is the reason that the drone, whatever its moral superiority to land armies and heavy weaponry, has replaced Guantánamo as the incendiary symbol of America’s indecent callousness towards the world’s Muslims. As Bush was the Guantánamo president, so Obama is the drone president. This switch, whatever Obama hoped, represents a worsening not an improvement of America’s image in the world.

#### PRISM destroyed soft power / credibility

Migranyan 7/5 (Andranik is the director of the Institute for Democracy and Cooperation in New York. He is also a professor at the Institute of International Relations in Moscow, a former member of the Public Chamber and a former member of the Russian Presidential Council. “Scandals Harm U.S. Soft Power,” 2013, http://nationalinterest.org/commentary/scandals-harm-us-soft-power-8695)

For the past few months, the United States has been rocked by a series of scandals. It all started with the events in Benghazi, when Al Qaeda-affiliated terrorists attacked the General Consulate there and murdered four diplomats, including the U.S. ambassador to Libya. Then there was the scandal exposed when it was revealed that the Justice Department was monitoring the calls of the Associated Press. The Internal Revenue Service seems to have targeted certain political groups. Finally, there was the vast National Security Agency apparatus for monitoring online activity revealed by Edward Snowden. Together, these events provoke a number of questions about the path taken by contemporary Western societies, and especially the one taken by America.¶ Large and powerful institutions, especially those in the security sphere, have become unaccountable to the public, even to representatives of the people themselves. Have George Orwell’s cautionary tales of total government control over society been realized?¶ At the end of the 1960s and the beginning of the 1970s, my fellow students and I read Orwell’s 1984 and other dystopian stories and believed them to portray fascist Germany or the Soviet Union—two totalitarian regimes—but today it has become increasingly apparent that Orwell, Huxley and other dystopian authors had seen in their own countries (Britain and the United States) certain trends, especially as technological capabilities grew, that would ultimately allow governments to exert total control over their societies. The potential for this type of all-knowing regime is what Edward Snowden revealed, confirming the worst fears that the dystopias are already being realized.¶ On a practical geopolitical level, the spying scandals have **seriously tarnished the reputation of the United States**. They have circumscribed its ability to exert soft power; the same influence that made the U.S. model very attractive to the rest of the world. This former lustre is now diminished. The blatant everyday intrusions into the private lives of Americans, and violations of individual rights and liberties by runaway, unaccountable U.S. government agencies, have deprived the United States of its authority to dictate how others must live and what others must do. Washington can no longer lecture others when its very foundational institutions and values are being discredited—or at a minimum, when all is not well “in the state of Denmark.”¶ Perhaps precisely because not all is well, many American politicians seem unable to adequately address the current situation. Instead of asking what isn’t working in the government and how to ensure accountability and transparency in their institutions, they try, in their annoyance, to blame the messenger—as they are doing in Snowden’s case. Some Senators hurried to blame Russia and Ecuador for anti-American behavior, and threatened to punish them should they offer asylum to Snowden.¶ These threats could only cause confusion in sober minds, as every sovereign country retains the right to issue or deny asylum to whomever it pleases. In addition, the United States itself has a tradition of always offering political asylum to deserters of the secret services of other countries, especially in the case of the former Soviet Union and other ex-socialist countries. In those situations, the United States never gave any consideration to how those other countries might react—it considered the deserters sources of valuable information. As long as deserters have not had a criminal and murderous past, they can receive political asylum in any country that considers itself sovereign and can stand up to any pressure and blackmail.¶ Meanwhile, the hysteria of some politicians, if the State Department or other institutions of the executive branch join it, can only accelerate the process of Snowden’s asylum. For any country he might ask will only be more willing to demonstrate its own sovereignty and dignity by standing up to a bully that tries to dictate conditions to it. In our particular case, **political pressure on Russia and President Putin could turn out to be utterly counterproductive.** I believe that Washington has enough levelheaded people to understand that fact, and correctly advise the White House. The administration will need sound advice, as many people in Congress fail to understand the consequences of their calls for punishment of sovereign countries or foreign political leaders that don’t dance to Washington’s tune.¶ Judging by the latest exchange between Moscow and Washington, it appears that the executive branches of both countries will find adequate solutions to the Snowden situation without attacks on each other’s dignity and self-esteem. Russia and the United States are both Security Council members, and much hinges on their decisions, including a slew of common problems that make cooperation necessary.¶ Yet **the recent series of scandals has caused irreparable damage to the image and soft power of the United States.** I do not know how soon this damage can be repaired. But gone are the days when Orwell was seen as a relic of the Cold War, as the all-powerful Leviathan of the security services has run away from all accountability to state and society. Today the world is looking at America—and its model for governance—with a more critical eye.

#### Syria tanked credibility

Anthony Cordesman 9/1/13, holds the Arleigh A. Burke Chair in Strategy at the Center for Strategic and International Studies (CSIS) in Washington, D.C., “President Obama and Syria: The ‘Waiting for Godot’ Strategy,” http://csis.org/publication/president-obama-and-syria-waiting-godot-strategy

Instead, the Administration first rushed into the kind of rhetoric you only use if you actually intend to act regardless of domestic and international support. It tied its entire effort to Syrian use of chemical weapons and the precedent for using such weapons forever. And only then did it suddenly spun around and talked about then need for delay, measured action, and Congressional approval.¶ While Beckett might not appreciate my efforts to define Godot as the Syrian Civil war, the Administration followed the script of Beckett’s play to the extent it never defined the reasons for what the actors were doing, why they were waiting, or what would happen after Godot came. Chemical weapons are a very real issue, but they are only a subset of the real issue: the overall level of suffering and growing regional instability coming out of the Syrian civil war.¶ We now face the inevitable reaction. The President’s decisions have reinforced all of the doubts about American strength, and our willingness to act, of both our friends and foes. We now have ten days of confusion and uncertainty to deal with, and then Congress will be evidently be asked to act only on a strike tailored to deter the future use of chemical weapons. It will still lack a meaningful plan for dealing with the Syrian civil war and its impact on the region.¶ Israel is threatening to return to hawk mode over Iran. Russia and China are in the “we told you so” mode. Assad has already launched new conventional artillery barrages against Syrian civilian areas and now has time enough to disperse a significant number of key physical assets from fixed target sites. France is left hanging – as is Britain for very different reasons. Our Arab allies and Turkey have no clear lead to follow. Our whole strategy in the Middle East remains unclear, as is our entire national security posture in an era of Sequestration and funding crises.¶ If the Congress does support the President, it will only be after we have openly faltered, and after having rushed forward before deciding on a course of delay. The President will have set a uniquely dangerous precedent by turning to Congress only after he appeared weak, rather than doing from the start, and will have then committed himself to wait at least ten days for the congress to return for its holiday. The message to the world is obvious.

# 2NC CP

#### Russia blocks, the U.S. has no influence

Tim Stevens 12, Associate for the Centre for Science and Security Studies and an Associate Fellow of the International Centre for the Study of Radicalisation and Political Violence, PhD candidate @ King’s College London, MA in War Studies, “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace,” Contemporary Security Policy, Vol. 33, Iss. 1, Apr. 13, Taylor and Francis Online

The United States is positioning itself as a global norm entrepreneur but it is by no means the only one. A long-running Canadian-American academic study on global information control finds that ‘as the Internet has grown in political significance, an architecture of control – through technology, regulation, norms, and political calculus – has emerged to shape a new geopolitical information landscape’.90 Under this formulation, one function of the normative turn would be to normalize the exercise of power in cyberspace.91 The US is far from alone in attempting to stake out vital ground in this politicized environment, and in the following section I examine how it is not the only norm entrepreneur in global cyberspace, and how its normative project is meeting with substantial opposition from other actors with their own agendas.¶ Norm Entrepreneurs in Global Cyberspace¶ Secretary Clinton's January 2010 speech called upon the UN Human Rights Council to adopt five new internet ‘freedoms’.92 Four of these were existing human rights transposed from the Universal Declaration of Human Rights (UDHR) to cyberspace: the freedoms of expression and worship, and the freedoms from want and fear. The fifth – the freedom to connect – is analogous to UDHR Article 20 – the right to peaceful assembly and association – in that ‘governments should not prevent people from connecting to the internet, to websites, or to each other’. Clinton spoke of ‘devoting the diplomatic, economic, and technological resources necessary to advance these freedoms’ as part of what she called ‘21st century statecraft’, and made it clear that technology in particular could be used ‘to advance democracy and human rights’. She made reference to ‘new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship’, for their own local needs and to further American foreign policy goals. An editorial in the Chinese government-owned Global Times pulled no punches in its response to Clinton's speech: ‘The US campaign for uncensored and free flow of information on an unrestricted Internet is a disguised attempt to impose its values on other cultures in the name of democracy … the bulk of information flowing from the United States and other Western countries is loaded with aggressive rhetoric against those countries that do not follow their lead’.93¶ Prior to Clinton's speech, the United States had already intervened in the internal affairs of its Western Asian bête noire, Iran. During the 2009 Iranian election protests, the State Department is reported to have requested that micro-blogging platform Twitter delay planned maintenance operations in order to allow it to continue to be used for coordinating anti-government demonstrations and spreading dissent.94 Although the significance of Twitter's role in the protests is unclear,95 the US perceived it as important enough to approach a commercial company directly with a view to altering its internal decision-making process in the national interest, despite President Obama's reported desire not to be seen to be ‘meddling’ in Iran's domestic affairs.96 Unsurprisingly, some officials from countries with traditions of media control have described Twitter as ‘an American plot to destabilize foreign governments’.97 Although this claim is otherwise unsubstantiated, it is evident that US intentions to promote norms consistent with its neoliberal outlook are being challenged by other states with different ideological stances. Russia, in particular, has tended to view US proposals in a dim light, as Sergei Korotkov of the Russian Defence Ministry argued in 2008:¶ Practically any information operation conducted by a state or a number of states against another state would be qualified as an interference into internal affairs … So any good cause, like promotion of democracy, cannot be used as a justification for such actions.98¶ This speaks to a fundamental difference between American and Russian views on cybersecurity, as summarized by an American think tank:¶ … the United States focuses on a law enforcement approach at the domestic level with voluntary international collaboration, while Russia focuses on developing binding international regimes. There are also quite different philosophies at work: Russia favors social control of the Internet as a medium, while the United States, for the most part, does not.99¶ These ‘philosophies’ are manifest as normative frameworks that both the United States and Russia are attempting to promote to other states and in multilateral fora.¶ One such contribution by the United States is to the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, whose 2009–2010 report makes repeated reference to the development of ‘norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure’.100 The GGE continues to promote cooperation, dialogue and collaboration between states, civil society and the private sector to improve cybersecurity. For its part, the US State Department distinguishes five inter-related normative fields that together contribute towards a ‘global culture of cybersecurity’: the responsibility of states to ensure their own cybersecurity; the continued relevance of jus ad bellum and jus in bello to cyber conflict; the requirement to address the use of proxies in cyber conflict; the responsibility to allow the free flow of information along the lines of Clinton's five freedoms; and the responsibility to combat terrorism.101 To institutionalize these norms, the United States favours a voluntary initiative rather than a negotiated treaty instrument, and prefers to pursue informal and non-obligatory transgovernmental cooperation rather than formally enforceable and binding intergovernmental coordination. Arguably, this would also avoid many potential legal constraints on the licit or illicit activities of the US and its allies in this security field.¶ The United States has also consulted widely with strategic allies, and has chaired the NATO Group of Experts review on a new strategic concept for NATO that addresses ‘cyber assaults of varying degrees of severity’ as one of three most likely threats to member states up to 2020.102 Allies of the United States, like the UK, have backed these initiatives and British armed forces minister Nick Harvey made explicit reference to the deterrent possibilities of collective action through the active application of NATO's Clause V commitment to mutual defence to aggressive acts in cyberspace.103¶ By contrast, Russia has tended to view cybersecurity as a matter of internal security rather than foreign policy. Its efforts to broker multilateral agreements have been founded on the need to control information (‘content’) within its sovereign borders rather than encourage the relatively unimpeded flow of information across those borders, as in the American model. Through the Shanghai Cooperation Organization (SCO), Russia – along with China, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan – in 2009 adopted an accord which defined ‘information war’ as ‘dissemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other States’.104 This interpretation of ‘information war’ was also reported as being akin to ‘mass psychologic [sic] brainwashing’.105 In late 2011, China, Russia, Tajikistan and Uzbekistan proposed a new code of conduct for consideration by the UN General Assembly.106 Framed in terms of ‘information security’, it called for a variety of sensible measures such as a curb on hostile and destabilizing cyber attacks but also for the need to prevent the dissemination of information incompatible with countries' internal ‘political, economic and social stability, as well as their spiritual and cultural environment’. Although we might take this to be a means of reducing external interference in domestic affairs, it has been widely interpreted as a defence of internet censorship and states' rights to prohibit access to materials deemed inimical to their ideologies.107 Much of this document was expressed in the language of ‘norms’ but the unfortunate irony is that even whilst criticizing the US for its hegemonic discourse, all of the SCO member states have demonstrable histories of attempting to censor internet content, restrict access to ICTs and otherwise shape the online media environment for the purposes of domestic political control, including through the use of physical force.108¶ Through the SCO and the UN, Russia has consistently called for a global ‘cyber arms control’ agreement. It has been repeatedly blocked in these attempts by the US, whose chief cybersecurity coordinator in the Clinton administration viewed Russian proposals as ‘largely a propaganda tool’, the lack of traditional dimensionality of ‘cyber arms’ mitigating against the monitoring and verification of any arms control regime.109 In addition, he noted that Russia has not signed ‘the one serious international agreement on disruptive cyber activity’, the Council of Europe's Convention on Cybercrime (2001), a conspicuous oversight given the level of cybercrime emanating from the Russian Federation.110 These sticking points seem to be exacerbated by traditional geopolitical distrust. The United States' normative priorities derive from their outwards-facing commitments to free trade and information exchange, as well as national security concerns about offensive cyber actions against its networks. Russia's proposals also draw on concerns with security, albeit principally of an internal nature, to which are closely linked the perceived deleterious impact of Western socio-cultural norms on Russian society. Both countries are acting as international norm entrepreneurs and they do not see eye to eye. Perhaps this should not surprise us. Régis Debray, reacting to the common thesis that global information technologies render obsolescent the nation-state and ‘political rivalries of yore’, writes that ‘territorial disputes are replaced by wars between competitors about norms, the euphemistic technological equivalent of nationalist expansion. This heralded rejection of ideology turns exorbitantly ideological in reality’.111 This idea resonates strongly with what we are witnessing in the international political environment with respect to cyberspace and security.112 Not least, this manifests in the degree of government intervention proposed by parties to the debate. Whereas the United States wishes to devolve much of the responsibility for cybersecurity to the private companies that own and operate ICT infrastructure, Russia prefers a more interventionist and regulatory stance, for example.¶ Nevertheless, the prospects for some form of global cybersecurity coordination are changing. The head of the UN International Telecommunications Union (ITU) has called for a treaty to prevent ‘cyberwar’, which would act to reduce states' inclination to launch cyber first-strikes against other states, a proposal supported by Russia, China and many non-aligned countries, although not the United States.113 The United States rejects their focus on ‘content’ regulation and is engaged in tortuous diplomatic negotiations with the ITU on this point. Ron Deibert – himself categorizable as a left-leaning norm entrepreneur – notes that the aim of international negotiations should be ‘a framework of international agreements focused on promoting norms of mutual behavior, clarification of jurisdictional responsibilities, and institutions designed to facilitate the exchange of information between security communities worldwide’.114 Elsewhere, the Council of Europe has proposed a global internet treaty that would perform these functions and others designed to protect ‘internet freedom’ and the technological infrastructures of cyberspace.115 There are also signs that the US is willing to engage with Russia on proposals to limit the military use of cyberspace, thereby reversing the trend of recent years.116 In particular, an Organization for Security and Cooperation in Europe (OSCE) resolution to share information on cyber deployments during military conflicts was co-sponsored by the US, Russia and others in July 2011.117 This apparent thaw led the US cybersecurity coordinator Howard Schmidt to comment that the ‘reset’ in US–Russia relations had extended itself to cyberspace.118 However, at present, the US opposes any form of negotiated treaty instrument as robustly as Russia and her allies favour one.¶ At the rarefied level of state interactions, global cyberspace agreements might have some deterrent effect, serving to constrain state military and espionage activities in cyberspace, although given the problems of identity, attribution and monitoring, its benefits may not be as obvious as with nuclear and conventional arms agreements. This is particularly pertinent if we consider the possible minimal effect on the actions of non-state actors, be they hackers, terrorists, criminals, or disgruntled citizens, especially as norms exist at many levels below the state and global society. Arquilla and Ronfeldt, for example, draw on the work of Kathryn Sikkink to illustrate their social netwar thesis, in which global information networks facilitate inter alia the flow of shared norms and goals, helping to form and maintain militant social activist networks, such as might be identified with online communities engaged in anti-state cyber activism.119 Nir Kshetri has suggested that social norms may act to legitimize various forms of cybercrime, proposing that ‘cybercrimes are more justifiable in some societies compared to others’.120 Research indicates that adherence to norms of group identity in the Russophone internet community was an important factor in establishing the base of hacktivists responsible for the compromise of Estonia's internet infrastructure in 2007.121 More generally, cyberspace is characterized by the development of ‘cybernorms’ as ‘informal constraints on human behavior’ within online communities, rather than imposed from without.122 The roles of non-governmental organizations in effecting normative change at the transnational level should also not be underestimated.123 Even in the field of security, Mueller notes that most of the routine cybersecurity work of ‘identifying, preventing and responding’ to threats to cyberspace systems ‘seems to be done by a transnational network that relies on cooperative frameworks and norms that were developed independently of states’.124¶ As the CSIS 2008 report noted, the United States is ‘not indispensable, a hegemon, or unchallenged, and the evolution of cyberspace clearly reflects this’.125 There are many different actors who have access to cyberspace and are capable of using it to their own strategic ends, and who as individuals and communities are subject to differing normative constraints and opportunities. States attempting to develop global normative frameworks for cyberspace may find their efforts have limited effect on cyberspace non-state communities. Cyber deterrence, even if it can be made to work between states, in conjunction with other tools of state power, is a far more problematic proposition at the sub-state level, precisely because, in contrast to traditional military domains, the tools and ‘weapons’ of cyber conflict are readily available to non-state actors who operate under different normative regimes. In the United States context, for example, Duncan Hollis notes that ‘non-attribution’ – one of the characteristics of cyberspace making cyber deterrence difficult – ‘is a value to be celebrated’ and is deeply entrenched in American culture, on- and offline.126 Attempts to alter this by government fiat are likely to meet substantial domestic resistance, not to mention external accusations of hypocrisy given the tenets of the stated United States commitment to ‘internet freedom’. Calls by United States national security actors to ‘re-engineer’, redesign or even replace the internet to facilitate personal identification of users and their activities are deeply problematic in this context.127 Nevertheless, as ‘norms’ are one of the regulative ‘laws’ of cyberspace, alongside code, the market, and physical ‘architecture’, states will continue to explore ways in which to influence this aspect of cyberspace.128¶ Conclusions¶ It is too early to tell quite how norms will emerge in this developing field, although we have tried to delineate the broad outlines of strategy, political discourse and policy proposals. As such, we cannot tell what the consequences of these developments will be, although further moves will be made towards bilateral and multilateral technical and information-sharing agreements and frameworks, even whilst the utility of these actions will continue to be hotly debated. It is likely that the ability to broker global agreements or treaty mechanisms will be hampered as much by cultural differences between, for example, the US and Russia, as it will by the tactical and operational difficulties in achieving technical security regimes satisfactory to all parties. The central unstated purpose of these activities is to normalize the exercise of state power in cyberspace. In this respect, all state parties agree; the differences emerge in how this is pursued.¶ Even as states attempt to regulate the use of cyberspace for, inter alia, military first strikes, they will retain significant military and intelligence cyber capabilities to be exercised below the level of an as-yet unascertained cyber conflict threshold. The latter may require legal definition at the global level, or it may yet fall to unilateral declarations of tolerance, or displays of force posture or operational capacity, most likely in conjunction with strategic allies. It may be that the norm that emerges from this situation is not of non-use but of ‘acceptable’ use, which serves to demonstrate where the ‘red lines’ of cyber operations are. It is unlikely, therefore, that a ‘cyber taboo’ analogous to nuclear and chemical weapons taboos will be constructed.129 In the absence of any firm notion of what, for example, a ‘cyberwar’ might actually look like, there may be little immediate societal pressure to avoid one, and plenty of latitude afforded to states to develop capabilities that might conceivably be used in one, if such a thing even exists.130 Nevertheless, as Nina Tannenwald argues with respect to the nuclear taboo, a norm of non-use may stand a greater chance of being adopted by alliances of democracies than by authoritarian states.131 However, given the possible US-Israeli involvement in the Stuxnet sabotage of Iranian nuclear technology, we must wonder if we are already past this point.132 The lure of a voluntary framework banning the offensive use of cyberspace may prove irresistible to many ‘like-minded nations’, even if its actual applicability is strictly limited. Importantly, an international normative regime not backed with coordinated and credible force will serve no deterrent function against exactly those ‘rogue’ and non-state actors most likely to conduct disruptive cyber operations.¶ Yet the question remains: how effective is a norms-based approach to cyber deterrence likely to be? How can we tell what aspects of a deterrence strategy are working, or which aren't? In truth, it is much too early to know. Even if it were possible to get all parties to comply with a set of norms hammered out through diplomacy and other forms of negotiation, what guarantees are there that these would be adhered to? Again, there are no such guarantees. It may be that states can be persuaded to comply with international normative frameworks through a mix of inducement, coercion and moral pressure. So too might industry and civil society be persuaded to do their part through a gradual process of cultural learning, and all parties work together to achieve the ‘global culture of cybersecurity’ currently aspired to. Even were these norms to operate strongly and bind together these actors such that norms of non-use or acceptable use became institutionalized, they are never likely to persuade all who might have the capabilities to prosecute actions in cyberspace that constitute strategic threats. For this reason alone, states and their militaries and security services will, even whilst pursuing denial strategies and improving defensive cybersecurity, be loath to abandon the search for effective punitive measures through which deterrence might be achieved. In turn, the norm of retaliatory punishment may prove to be a powerful deterrent in itself.

# 2NC Adv 1

#### It’s all hype --- cyberattacks are just a nuisance, not effective war tactics

Thomas Rid 12, PhD, reader in war studies @ King’s College London, former visiting scholar @ Hebrew University, has previously worked at the School for Advanced International Studies, Johns Hopkins, and RAND, “Think Again: Cyberwar,” March/April, Foreign Affairs, <http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,1>

Time for a reality check: Cyberwar is still more hype than hazard. Consider the definition of an act of war: It has to be potentially violent, it has to be purposeful, and it has to be political. The cyberattacks we've seen so far, from Estonia to the Stuxnet virus, simply don't meet these criteria. Take the dubious story of a Soviet pipeline explosion back in 1982, much cited by cyberwar's true believers as the most destructive cyberattack ever. The account goes like this: In June 1982, a Siberian pipeline that the CIA had virtually booby-trapped with a so-called "logic bomb" exploded in a monumental fireball that could be seen from space. The U.S. Air Force estimated the explosion at 3 kilotons, equivalent to a small nuclear device. Targeting a Soviet pipeline linking gas fields in Siberia to European markets, the operation sabotaged the pipeline's control systems with software from a Canadian firm that the CIA had doctored with malicious code. No one died, according to Thomas Reed, a U.S. National Security Council aide at the time who revealed the incident in his 2004 book, At the Abyss; the only harm came to the Soviet economy. But did it really happen? After Reed's account came out, Vasily Pchelintsev, a former KGB head of the Tyumen region, where the alleged explosion supposedly took place, denied the story. There are also no media reports from 1982 that confirm such an explosion, though accidents and pipeline explosions in the Soviet Union were regularly reported in the early 1980s. Something likely did happen, but Reed's book is the only public mention of the incident and his account relied on a single document. Even after the CIA declassified a redacted version of Reed's source, a note on the so-called Farewell Dossier that describes the effort to provide the Soviet Union with defective technology, the agency did not confirm that such an explosion occurred. The available evidence on the Siberian pipeline blast is so thin that it shouldn't be counted as a proven case of a successful cyberattack. Most other commonly cited cases of cyberwar are even less remarkable. Take the attacks on Estonia in April 2007, which came in response to the controversial relocation of a Soviet war memorial, the Bronze Soldier. The well-wired country found itself at the receiving end of a massive distributed denial-of-service attack that emanated from up to 85,000 hijacked computers and lasted three weeks. The attacks reached a peak on May 9, when 58 Estonian websites were attacked at once and the online services of Estonia's largest bank were taken down. "What's the difference between a blockade of harbors or airports of sovereign states and the blockade of government institutions and newspaper websites?" asked Estonian Prime Minister Andrus Ansip. Despite his analogies, the attack was no act of war. It was certainly a nuisance and an emotional strike on the country, but the bank's actual network was not even penetrated; it went down for 90 minutes one day and two hours the next. The attack was not violent, it wasn't purposefully aimed at changing Estonia's behavior, and no political entity took credit for it. The same is true for the vast majority of cyberattacks on record. Indeed, there is no known cyberattack that has caused the loss of human life. No cyberoffense has ever injured a person or damaged a building. And if an act is not at least potentially violent, it's not an act of war. Separating war from physical violence makes it a metaphorical notion; it would mean that there is no way to distinguish between World War II, say, and the "wars" on obesity and cancer. Yet those ailments, unlike past examples of cyber "war," actually do kill people. Keep waiting. U.S. Defense Secretary Leon Panetta delivered a stark warning last summer: "We could face a cyberattack that could be the equivalent of Pearl Harbor." Such alarmist predictions have been ricocheting inside the Beltway for the past two decades, and some scaremongers have even upped the ante by raising the alarm about a cyber 9/11. In his 2010 book, Cyber War, former White House counterterrorism czar Richard Clarke invokes the specter of nationwide power blackouts, planes falling out of the sky, trains derailing, refineries burning, pipelines exploding, poisonous gas clouds wafting, and satellites spinning out of orbit -- events that would make the 2001 attacks pale in comparison. But the empirical record is less hair-raising, even by the standards of the most drastic example available. Gen. Keith Alexander, head of U.S. Cyber Command (established in 2010 and now boasting a budget of more than $3 billion), shared his worst fears in an April 2011 speech at the University of Rhode Island: "What I'm concerned about are destructive attacks," Alexander said, "those that are coming." He then invoked a remarkable accident at Russia's Sayano-Shushenskaya hydroelectric plant to highlight the kind of damage a cyberattack might be able to cause. Shortly after midnight on Aug. 17, 2009, a 900-ton turbine was ripped out of its seat by a so-called "water hammer," a sudden surge in water pressure that then caused a transformer explosion. The turbine's unusually high vibrations had worn down the bolts that kept its cover in place, and an offline sensor failed to detect the malfunction. Seventy-five people died in the accident, energy prices in Russia rose, and rebuilding the plant is slated to cost $1.3 billion. Tough luck for the Russians, but here's what the head of Cyber Command didn't say: The ill-fated turbine had been malfunctioning for some time, and the plant's management was notoriously poor. On top of that, the key event that ultimately triggered the catastrophe seems to have been a fire at Bratsk power station, about 500 miles away. Because the energy supply from Bratsk dropped, authorities remotely increased the burden on the Sayano-Shushenskaya plant. The sudden spike overwhelmed the turbine, which was two months shy of reaching the end of its 30-year life cycle, sparking the catastrophe. If anything, the Sayano-Shushenskaya incident highlights how difficult a devastating attack would be to mount. The plant's washout was an accident at the end of a complicated and unique chain of events. Anticipating such vulnerabilities in advance is extraordinarily difficult even for insiders; creating comparable coincidences from cyberspace would be a daunting challenge at best for outsiders. If this is the most drastic incident Cyber Command can conjure up, perhaps it's time for everyone to take a deep breath.

#### Risk of cyberattack pales in comparison to other impacts

Brandon Valeriano 12 and Ryan Maness, Lecturer in Social and Political Sciences at the University of Glasgow AND Ph.D. candidate at the University of Illinois at Chicago, "The Fog of Cyberwar," Foreign Affairs, 11/21, [www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar?page=show](http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar?page=show)

Some cyberattacks over the past decade have briefly affected state strategic plans, but none has resulted in death or lasting damage. For example, the 2007 cyberattacks on Estonia by Russia shut down networks and government websites and disrupted commerce for a few days, but things swiftly went back to normal. The majority of cyberattacks worldwide have been minor: easily corrected annoyances such as website defacements or basic data theft -- basically the least a state can do when challenged diplomatically.¶ Our research shows that although warnings about cyberwarfare have become more severe, the actual magnitude and pace of attacks do not match popular perception. Only 20 of 124 active rivals -- defined as the most conflict-prone pairs of states in the system -- engaged in cyberconflict between 2001 and 2011. And there were only 95 total cyberattacks among these 20 rivals. The number of observed attacks pales in comparison to other ongoing threats: a state is 600 times more likely to be the target of a terrorist attack than a cyberattack. We used a severity score ranging from five, which is minimal damage, to one, where death occurs as a direct result from cyberwarfare. Of all 95 cyberattacks in our analysis, the highest score -- that of Stuxnet and Flame -- was only a three.

#### Cyber-attacks “burnout” --- the bigger the impact, the faster it can be corrected --- checks escalation

Ian Brown 11, Associate Director of the Cyber Security Centre @ the University of Oxford, and Peter Sommers, Professor @ the London School of Economics, Reducing Systemic Cybersecurity Risk,” OECD, 1/14, http://www.oecd.org/governance/risk/46889922.pdf

Pure cybersecurity risks tend to be localised and temporary rather than global and long - term. This is for two fundamental reasons:¶ The longer an attack persists, the greater the likelihood it will be detected, routed around, and become attributable to a specific party against whom actions can be taken (including disconnection, arrest and retribution). ¶ Larger-scale attacks result in more of the data needed to diagnose and fix system vulnerabilities, and provide a stronger incentive to system suppliers and administrators to do so (Libicki, 2009: xiv).¶ Even for the best-resourced and most determined attackers – nation states taking military action – these conditions are likely to hold. RAND Corporation recently reported to the US Air Force “operational cyberwar has an important niche role, but only that,” commenting:¶ “Investigation may reveal that a particular system has a particular vulnerability. Predicting what an attack can do requires knowing how the system and its operators will respond to signs of dysfunction and knowing the behaviour of processes and systems associated with the system being attacked. Even then, cyberwar operations neither directly harm individuals nor destroy equipment (albeit with some exceptions). At best, these operations can confuse and frustrate operators of military systems, and then only temporarily. Thus, cyberwar can only be a support function for other elements of warfare, for instance, in disarming the enemy‖ (Libicki, 2009: xiv — xv).”

#### Diminishing marginal returns means there’s no impact

Martin C. Libicki 9, Senior Management Scientist @ RAND and adjunct fellow @ Georgetown’s Center for Security Studies, “Cyberdeterrence and Cyberwar,” RAND, <http://www.rand.org/pubs/monographs/MG877.html>

Strategic Cyberwar Is Unlikely to Be Decisive ¶ No one knows how destructive any one strategic cyberwar attack would be. Estimates of the damage from today’s cyberattacks within the United States range from hundreds of billions of dollars to just a few billion dollars per year. ¶ The higher dollar figures suggest that cyberattacks on enemy civilian infrastructures—strategic cyberwar—may be rationalized as a way to assist military efforts or as a way to coerce the other side to yield to prevent further suffering. But can strategic cyberwar induce political compliance the way, say, strategic airpower would? Airpower tends to succeed when societies are convinced that matters will only get worse. With cyberattacks, the opposite is more likely. As systems are attacked, vulnerabilities are revealed and repaired or routed around. As systems become more hardened, societies become less vulnerable and are likely to become more, rather than less, resistant to further coercion.

#### Cyberattacks can’t launch nukes --- airgapping solves

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

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

#### Airgapping solves

Weimann 4 – Gabriel Weimann is a senior fellow at the United States Institute of Peace and professor of communication at the University of Haifa, Israel. December 2004, "Cyberterrorism: How Real is the Threat?" http://dspace.cigilibrary.org/jspui/bitstream/123456789/15033/1/Cyberterrorism How Real Is the Threat.pdf?1

Many computer security experts do not believe that it is possible to use the Internet to inflict death on a large scale. Some pointed out that the resilience of computer systems to attack is the result of significant investments of time, money, and expertise. As Green describes, nuclear weapons systems are protected by “air-gapping”: **they are not connected to the Internet or** to **any open computer network** and thus they cannot be accessed by intruders, terrorists, or hackers. Thus, for example, the Defense Department protects sensitive systems by isolating them from the Internet and even from the Pentagon’s own internal network. The CIA’s classified computers are also air-gapped, as is the FBI’s entire computer system. The 9/11 events and the subsequent growing awareness of cyberterror highlighted other potential targets for such attacks. In 2002, Senator Charles Schumer (D-N.Y.) described “the absolute havoc and devastation that would result if cyberterrorists suddenly shut down our air traffic control system, with thousands of planes in mid-flight.” However, argues Green, “cybersecurity experts give some of their highest marks to the Federal Aviation Authority, which reasonably separates its administrative and air traffic control systems and strictly air-gaps the latter.”

#### Zero impact to cyber-attacks --- overwhelming consensus of qualified authors goes neg

- No motivation---can’t be used for coercive leverage

- Defenses solve---benefits of offense are overstated

- Too difficult to execute/mistakes in code are inevitable

- AT: Infrastructure attacks

- Military networks are air-gapped/difficult to access

- Overwhelming consensus goes neg

Colin S. Gray 13, Prof. of International Politics and Strategic Studies @ the University of Reading and External Researcher @ the Strategic Studies Institute @ the U.S. Army War College, April, “Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling,” U.S. Army War College Press, <http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1147.pdf>

CONCLUSIONS AND RECOMMENDATIONS: THE SKY IS NOT FALLING¶ This analysis has sought to explore, identify, and explain the strategic meaning of cyber power. The organizing and thematic question that has shaped and driven the inquiry has been “So what?” Today we all do cyber, but this behavior usually has not been much informed by an understanding that reaches beyond the tactical and technical. I have endeavored to analyze in strategic terms what is on offer from the largely technical and tactical literature on cyber. What can or might be done and how to go about doing it are vitally important bodies of knowledge. But at least as important is understanding what cyber, as a fifth domain of warfare, brings to national security when it is considered strategically. Military history is stocked abundantly with examples of tactical behavior un - guided by any credible semblance of strategy. This inquiry has not been a campaign to reveal what cy ber can and might do; a large literature already exists that claims fairly convincingly to explain “how to . . .” But what does cyber power mean, and how does it fit strategically, if it does? These Conclusions and Rec ommendations offer some understanding of this fifth geography of war in terms that make sense to this strategist, at least. ¶ 1. Cyber can only be an enabler of physical effort. Stand-alone (popularly misnamed as “strategic”) cyber action is inherently grossly limited by its immateriality. The physicality of conflict with cyber’s human participants and mechanical artifacts has not been a passing phase in our species’ strategic history. Cyber action, quite independent of action on land, at sea, in the air, and in orbital space, certainly is possible. But the strategic logic of such behavior, keyed to anticipated success in tactical achievement, is not promising. To date, “What if . . .” speculation about strategic cyber attack usually is either contextually too light, or, more often, contextually unpersuasive. 49 However, this is not a great strategic truth, though it is a judgment advanced with considerable confidence. Although societies could, of course, be hurt by cyber action, it is important not to lose touch with the fact, in Libicki’s apposite words, that “[i]n the absence of physical combat, cyber war cannot lead to the occupation of territory. It is almost inconceivable that a sufficiently vigorous cyber war can overthrow the adversary’s government and replace it with a more pliable one.” 50 In the same way that the concepts of sea war, air war, and space war are fundamentally unsound, so also the idea of cyber war is unpersuasive. ¶ It is not impossible, but then, neither is war conducted only at sea, or in the air, or in space. On the one hand, cyber war may seem more probable than like environmentally independent action at sea or in the air. After all, cyber warfare would be very unlikely to harm human beings directly, let alone damage physically the machines on which they depend. These near-facts (cyber attack might cause socially critical machines to behave in a rogue manner with damaging physical consequences) might seem to ren - der cyber a safer zone of belligerent engagement than would physically violent action in other domains. But most likely there would be serious uncertainties pertaining to the consequences of cyber action, which must include the possibility of escalation into other domains of conflict. Despite popular assertions to the contrary, cyber is not likely to prove a precision weapon anytime soon. 51 In addition, assuming that the political and strategic contexts for cyber war were as serious as surely they would need to be to trigger events warranting plausible labeling as cyber war, the distinctly limited harm likely to follow from cyber assault would hardly appeal as prospectively effective coercive moves. On balance, it is most probable that cyber’s strategic future in war will be as a contribut - ing enabler of effectiveness of physical efforts in the other four geographies of conflict. Speculation about cyber war, defined strictly as hostile action by net - worked computers against networked computers, is hugely unconvincing.¶ 2. Cyber defense is difficult, but should be sufficiently effective. The structural advantages of the offense in cyber conflict are as obvious as they are easy to overstate. Penetration and exploitation, or even attack, would need to be by surprise. It can be swift almost beyond the imagination of those encultured by the traditional demands of physical combat. Cyber attack may be so stealthy that it escapes notice for a long while, or it might wreak digital havoc by com - plete surprise. And need one emphasize, that at least for a while, hostile cyber action is likely to be hard (though not quite impossible) to attribute with a cy - berized equivalent to a “smoking gun.” Once one is in the realm of the catastrophic “What if . . . ,” the world is indeed a frightening place. On a personal note, this defense analyst was for some years exposed to highly speculative briefings that hypothesized how unques - tionably cunning plans for nuclear attack could so promptly disable the United States as a functioning state that our nuclear retaliation would likely be still - born. I should hardly need to add that the briefers of these Scary Scenarios were obliged to make a series of Heroic Assumptions. ¶ The literature of cyber scare is more than mildly reminiscent of the nuclear attack stories with which I was assailed in the 1970s and 1980s. As one may observe regarding what Winston Churchill wrote of the disaster that was the Gallipoli campaign of 1915, “[t]he terrible ‘Ifs’ accumulate.” 52 Of course, there are dangers in the cyber domain. Not only are there cyber-competent competitors and enemies abroad; there are also Americans who make mistakes in cyber operation. Furthermore, there are the manufacturers and constructors of the physical artifacts behind (or in, depending upon the preferred definition) cyber - space who assuredly err in this and that detail. The more sophisticated—usually meaning complex—the code for cyber, the more certain must it be that mistakes both lurk in the program and will be made in digital communication.¶ What I have just outlined minimally is not a reluc - tant admission of the fallibility of cyber, but rather a statement of what is obvious and should be anticipat - ed about people and material in a domain of war. All human activities are more or less harassed by friction and carry with them some risk of failure, great or small. A strategist who has read Clausewitz, especially Book One of On War , 53 will know this. Alternatively, anyone who skims my summary version of the general theory of strategy will note that Dictum 14 states explicitly that “Strategy is more difficult to devise and execute than are policy, operations, and tactics: friction of all kinds comprise phenomena inseparable from the mak - ing and execution of strategies.” 54 Because of its often widely distributed character, the physical infrastruc - ture of an enemy’s cyber power is typically, though not invariably, an impracticable target set for physical assault. Happily, this probable fact should have only annoying consequences. The discretionary nature and therefore the variable possible characters feasible for friendly cyberspace(s), mean that the more danger - ous potential vulnerabilities that in theory could be the condition of our cyber-dependency ought to be avoidable at best, or bearable and survivable at worst. Libicki offers forthright advice on this aspect of the subject that deserves to be taken at face value: ¶ [T]here is no inherent reason that improving informa - tion technologies should lead to a rise in the amount of critical information in existence (for example, the names of every secret agent). Really critical information should never see a computer; if it sees a computer, it should not be one that is networked; and if the computer is networked, it should be air-gapped.¶ Cyber defense admittedly is difficult to do, but so is cyber offense. To quote Libicki yet again, “[i]n this medium [cyberspace] the best defense is not necessarily a good offense; it is usually a good defense.” 56 Unlike the geostrategic context for nuclear-framed competition in U.S.–Soviet/Russian rivalry, the geographical domain of cyberspace definitely is defensible. Even when the enemy is both clever and lucky, it will be our own design and operating fault if he is able to do more than disrupt and irritate us temporarily.¶ When cyber is contextually regarded properly— which means first, in particular, when it is viewed as but the latest military domain for defense planning—it should be plain to see that cyber performance needs to be good enough rather than perfect. 57 Our Landpower, sea power, air power, and prospectively our space systems also will have to be capable of accepting combat damage and loss, then recovering and carrying on. There is no fundamental reason that less should be demanded of our cyber power. Second, given that cyber is not of a nature or potential character at all likely to parallel nuclear dangers in the menace it could con - tain, we should anticipate international cyber rivalry to follow the competitive dynamic path already fol - lowed in the other domains in the past. Because the digital age is so young, the pace of technical change and tactical invention can be startling. However, the mechanization RMA of the 1920s and 1930s recorded reaction to the new science and technology of the time that is reminiscent of the cyber alarmism that has flour - ished of recent years. 58 We can be confident that cyber defense should be able to function well enough, given the strength of political, military, and commercial motivation for it to do so. The technical context here is a medium that is a constructed one, which provides air-gapping options for choice regarding the extent of networking. Naturally, a price is paid in convenience for some closing off of possible cyberspace(s), but all important defense decisions involve choice, so what is novel about that? There is nothing new about accepting some limitations on utility as a price worth paying for security.¶ 3. Intelligence is critically important, but informa - tion should not be overvalued. The strategic history of cyber over the past decade confirms what we could know already from the science and technology of this new domain for conflict. Specifically, cyber power is not technically forgiving of user error. Cyber warriors seeking criminal or military benefit require precise information if their intended exploits are to succeed. Lucky guesses should not stumble upon passwords, while efforts to disrupt electronic Supervisory Con - trol and Data Acquisition (SCADA) systems ought to be unable to achieve widespread harmful effects. But obviously there are practical limits to the air-gap op - tion, given that control (and command) systems need to be networks for communication. However, Internet connection needs to be treated as a potential source of serious danger.¶ It is one thing to be able to be an electronic nuisance, to annoy, disrupt, and perhaps delay. But it is quite another to be capable of inflicting real persisting harm on the fighting power of an enemy. Critically important military computer networks are, of course, accessible neither to the inspired amateur outsider, nor to the malignant political enemy. Easy passing reference to a hypothetical “cyber Pearl Harbor” reflects both poor history and ignorance of contemporary military common sense. Critical potential military (and other) targets for cyber attack are extremely hard to access and influence (I believe and certainly hope), and the technical knowledge, skills, and effort required to do serious harm to national security is forbiddingly high. This is not to claim, foolishly, that cyber means absolutely could not secure near-catastrophic results. However, it is to say that such a scenario is extremely improbable. Cyber defense is advancing all the time, as is cyber offense, of course. But so discretionary in vital detail can one be in the making of cyberspace, that confidence—real confidence—in cyber attack could not plausibly be high. It should be noted that I am confining this particular discussion to what rather idly tends to be called cyber war. In political and strategic practice, it is unlikely that war would or, more importantly, ever could be restricted to the EMS. Somewhat rhetorically, one should pose the question: Is it likely (almost anything, strictly, is possible) that cyber war with the potential to inflict catastrophic damage would be allowed to stand unsupported in and by action in the other four geographical domains of war? I believe not.¶ Because we have told ourselves that ours uniquely is the Information Age, we have become unduly respectful of the potency of this rather slippery catch-all term. As usual, it is helpful to contextualize the al - legedly magical ingredient, information, by locating it properly in strategic history as just one important element contributing to net strategic effectiveness. This mild caveat is supported usefully by recognizing the general contemporary rule that information per se harms nothing and nobody. The electrons in cyber - ized conflict have to be interpreted and acted upon by physical forces (including agency by physical human beings). As one might say, intelligence (alone) sinks no ship; only men and machines can sink ships! That said, there is no doubt that if friendly cyber action can infiltrate and misinform the electronic informa - tion on which advisory weaponry and other machines depend, considerable warfighting advantage could be gained. I do not intend to join Clausewitz in his dis - dain for intelligence, but I will argue that in strategic affairs, intelligence usually is somewhat uncertain. 59 Detailed up-to-date intelligence literally is essential for successful cyber offense, but it can be healthily sobering to appreciate that the strategic rewards of intelligence often are considerably exaggerated. The basic reason is not hard to recognize. Strategic success is a complex endeavor that requires adequate perfor - mances by many necessary contributors at every level of conflict (from the political to the tactical). ¶ When thoroughly reliable intelligence on the en - emy is in short supply, which usually is the case, the strategist finds ways to compensate as best he or she can. The IT-led RMA of the past 2 decades was fueled in part by the prospect of a quality of military effec - tiveness that was believed to flow from “dominant battle space knowledge,” to deploy a familiar con - cept. 60 While there is much to be said in praise of this idea, it is not unreasonable to ask why it has been that our ever-improving battle space knowledge has been compatible with so troubled a course of events in the 2000s in Iraq and Afghanistan. What we might have misunderstood is not the value of knowledge, or of the information from which knowledge is quarried, or even the merit in the IT that passed information and knowledge around. Instead, we may well have failed to grasp and grip understanding of the whole context of war and strategy for which battle space knowledge unquestionably is vital. One must say “vital” rather than strictly essential, because relatively ignorant armies can and have fought and won despite their ig - norance. History requires only that one’s net strategic performance is superior to that of the enemy. One is not required to be deeply well informed about the en - emy. It is historically quite commonplace for armies to fight in a condition of more-than-marginal reciprocal and strategic cultural ignorance. Intelligence is king in electronic warfare, but such warfare is unlikely to be solely, or even close to solely, sovereign in war and its warfare, considered overall as they should be.¶ 4. Why the sky will not fall. More accurately, one should say that the sky will not fall because of hostile action against us in cyberspace unless we are improb - ably careless and foolish. David J. Betz and Tim Ste vens strike the right note when they conclude that “[i]f cyberspace is not quite the hoped-for Garden of Eden, it is also not quite the pestilential swamp of the imagination of the cyber-alarmists.” 61 Our understanding of cyber is high at the technical and tactical level, but re - mains distinctly rudimentary as one ascends through operations to the more rarified altitudes of strategy and policy. Nonetheless, our scientific, technological, and tactical knowledge and understanding clearly indicates that the sky is not falling and is unlikely to fall in the future as a result of hostile cyber action. This analysis has weighed the more technical and tactical literature on cyber and concludes, not simply on balance, that cyber alarmism has little basis save in the imagination of the alarmists. There is military and civil peril in the hostile use of cyber, which is why we must take cyber security seriously, even to the point of buying redundant capabilities for a range of command and control systems. 62 So seriously should we regard cyber danger that it is only prudent to as - sume that we will be the target for hostile cyber action in future conflicts, and that some of that action will promote disruption and uncertainty in the damage it will cause.¶ That granted, this analysis recommends strongly that the U.S. Army, and indeed the whole of the U.S. Government, should strive to comprehend cyber in context. Approached in isolation as a new technol - ogy, it is not unduly hard to be over impressed with its potential both for good and harm. But if we see networked computing as just the latest RMA in an episodic succession of revolutionary changes in the way information is packaged and communicated, the computer-led IT revolution is set where it belongs, in historical context. In modern strategic history, there has been only one truly game-changing basket of tech - nologies, those pertaining to the creation and deliv - ery of nuclear weapons. Everything else has altered the tools with which conflict has been supported and waged, but has not changed the game. The nuclear revolution alone raised still-unanswered questions about the viability of interstate armed conflict. How - ever, it would be accurate to claim that since 1945, methods have been found to pursue fairly traditional political ends in ways that accommodate nonuse of nuclear means, notwithstanding the permanent pres - ence of those means.¶ The light cast by general strategic theory reveals what requires revealing strategically about networked computers. Once one sheds some of the sheer wonder at the seeming miracle of cyber’s ubiquity, instanta - neity, and (near) anonymity, one realizes that cyber is just another operational domain, though certainly one very different from the others in its nonphysi - cality in direct agency. Having placed cyber where it belongs, as a domain of war, next it is essential to recognize that its nonphysicality compels that cyber should be treated as an enabler of joint action, rather than as an agent of military action capable of behav - ing independently for useful coercive strategic effect. There are stand-alone possibilities for cyber action, but they are not convincing as attractive options either for or in opposition to a great power, let alone a superpower. No matter how intriguing the scenario design for cyber war strictly or for cyber warfare, the logic of grand and military strategy and a common sense fueled by understanding of the course of strategic history, require one so to contextualize cyber war that its independence is seen as too close to absurd to merit much concern.

#### No threat of large-scale cyber-attacks---alarmist predictions are empirically denied

Sean Lawson 11, Ph.D. Department of Communication University of Utah "BEYOND CYBER-DOOM: Cyberattack Scenarios and the Evidence of History" Jan 11 mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history\_1.pdf

Despite persistent ambiguity in cyber-threat perceptions, cyber-doom scenarios have remained animportant tactic used by cybersecurity proponents. Cyber-doom scenarios are hypothetical stories about prospective impacts of a cyberattack and are meant to serve as cautionary tales that focus the attention of policy makers, media, and the public on the issue of cybersecurity. These stories typically follow a set pattern involving a cyberattack disrupting or destroying critical infrastructure. Examples include attacks against the electrical grid leading to mass blackouts, attacks against the financial system leading to economic losses or complete economic collapse, attacks against the transportation system leading to planes and trains crashing, attacks against dams leading floodgates to open, or attacks against nuclear power plants leading to meltdowns (Cavelty, 2007: 2).¶ Recognizing that modern infrastructures are closely interlinked and interdependent, such scenarios often involve a combination of multiple critical infrastructure systems failing simultaneously, what is sometimes referred to as a “cascading failure.” This was the case in the “Cyber Shockwave” war game televised by CNN in February 2010, in which a computer worm spreading among cell phones eventually led to serious disruptions of critical infrastructures (Gaylord, 2010). Even more ominously, in their recent book, Richard Clarke and Robert Knake (2010: 64–68) present a scenario in which a cyberattack variously destroys or seriously disrupts all U.S. infrastructure in only fifteen minutes, killing thousands and wreaking unprecedented destruction on U.S. cities.¶ Surprisingly, some argue that we have already had attacks at this level, but that we just have not recognized that they were occurring. For example, Amit Yoran, former head of the Department of Homeland Security’s National Cyber Security Division, claims that a “cyber- 9/11” has already occurred, “but it’s happened slowly so we don’t see it.” As evidence, he points to the 2007 cyberattacks on Estonia, as well as other incidents in which the computer systems of government agencies or contractors have been infiltrated and sensitive information stolen (Singel, 2009). Yoran is not alone in seeing the 2007 Estonia attacks as an example of the cyberdoom that awaits if we do not take cyber threats seriously. The speaker of the Estonian parliament, Ene Ergma, has said that “When I look at a nuclear explosion, and the explosion that happened in our country in May, I see the same thing” (Poulsen, 2007).¶ Cyber-doom scenarios are not new. As far back as 1994, futurist and best-selling author Alvin Toffler claimed that cyberattacks on the World Trade Center could be used to collapse the entire U.S. economy. He predicted that “They [terrorists or rogue states] won’t need to blow up the World Trade Center. Instead, they’ll feed signals into computers from Libya or Tehran or Pyongyang and shut down the whole banking system if they want to. We know a former senior intelligence official who says, ‘Give me $1 million and 20 people and I will shut down America. I could close down all the automated teller machines, the Federal Reserve, Wall Street, and most hospital and business computer systems’” (Elias, 1994).¶ But we have not seen anything close to the kinds of scenarios outlined by Yoran, Ergma, Toffler, and others. Terrorists did not use cyberattack against the World Trade Center; they used hijacked aircraft. And the attack of 9/11 did not lead to the long-term collapse of the U.S. economy; we would have to wait for the impacts of years of bad mortgages for a financial meltdown. Nor did the cyberattacks on Estonia approximate what happened on 9/11 as Yoran has claimed, and certainly not nuclear warfare as Ergma has claimed. In fact, a scientist at the NATO Co-operative Cyber Defence Centre of Excellence, which was established in Tallinn, Estonia in response to the 2007 cyberattacks, has written that the immediate impacts of those attacks were “minimal” or “nonexistent,” and that the “no critical services were permanently affected” (Ottis, 2010: 72).¶ Nonetheless, many cybersecurity proponents continue to offer up cyber-doom scenarios that not only make analogies to weapons of mass destruction (WMDs) and the terrorist attacks of 9/11, but also hold out economic, social, and even civilizational collapse as possible impacts of cyberattacks. A report from the Hoover Institution has warned of so-called “eWMDs” (Kelly & Almann, 2008); the FBI has warned that a cyberattack could have the same impact as a “wellplaced bomb” (FOXNews.com, 2010b); and official DoD documents refer to “weapons of mass disruption,” implying that cyberattacks might have impacts comparable to the use of WMD (Chairman of the Joint Chiefs of Staff 2004, 2006). John Arquilla, one of the first to theorize cyberwar in the 1990s (Arquilla & Ronfeldt, 1997), has spoken of “a grave and growing capacity for crippling our tech-dependent society” and has said that a “cyber 9/11” is a matter of if, not when (Arquilla, 2009). Mike McConnell, who has claimed that we are already in an ongoing cyberwar (McConnell, 2010), has even predicted that a cyberattack could surpass the impacts of 9/11 “by an order of magnitude” (The Atlantic, 2010). Finally, some have even compared the impacts of prospective cyberattacks to the 2004 Indian Ocean tsunami that killed roughly a quarter million people and caused widespread physical destruction in five countries (Meyer, 2010); suggested that cyberattack could pose an “existential threat” to the United States (FOXNews.com 2010b); and offered the possibility that cyberattack threatens not only the continued existence of the United States, but all of “global civilization” (Adhikari, 2009).¶ In response, critics have noted that not only has the story about who threatens what, how, and with what potential impact shifted over time, but it has done so with very little evidence provided to support the claims being made (Bendrath, 2001, 2003; Walt, 2010). Others have noted that the cyber-doom scenarios offered for years by cybersecurity proponents have yet to come to pass and question whether they are possible at all (Stohl, 2007). Some have also questioned the motives of cybersecurity proponents. Various think tanks, security firms, defense contractors, and business leaders who trumpet the problem of cyber attacks are portrayed as selfinterested ideologues who promote unrealistic portrayals of cyber-threats (Greenwald, 2010).

#### No impact to cyberattacks --- they’ll either be weak or contained to specific systems

Thomas Rid 12, PhD, reader in war studies @ King’s College London, former visiting scholar @ Hebrew University, has previously worked at the School for Advanced International Studies, Johns Hopkins, and RAND, “Think Again: Cyberwar,” March/April, Foreign Affairs, <http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,1>

"Cyberweapons Can Create Massive Collateral Damage." Very unlikely. When news of Stuxnet broke, the New York Times reported that the most striking aspect of the new weapon was the "collateral damage" it created. The malicious program was "splattered on thousands of computer systems around the world, and much of its impact has been on those systems, rather than on what appears to have been its intended target, Iranian equipment," the Times reported. Such descriptions encouraged the view that computer viruses are akin to highly contagious biological viruses that, once unleashed from the lab, will turn against all vulnerable systems, not just their intended targets. But this metaphor is deeply flawed. As the destructive potential of a cyberweapon grows, the likelihood that it could do far-reaching damage across many systems shrinks. Stuxnet did infect more than 100,000 computers -- mainly in Iran, Indonesia, and India, though also in Europe and the United States. But it was so specifically programmed that it didn't actually damage those machines, afflicting only Iran's centrifuges at Natanz. The worm's aggressive infection strategy was designed to maximize the likelihood that it would reach its intended target. Because that final target was not networked, "all the functionality required to sabotage a system was embedded directly in the Stuxnet executable," the security software company Symantec observed in its analysis of the worm's code. So yes, Stuxnet was "splattered" far and wide, but it only executed its damaging payload where it was supposed to. Collateral infection, in short, is not necessarily collateral damage. A sophisticated piece of malware may aggressively infect many systems, but if there is an intended target, the infection will likely have a distinct payload that will be harmless to most computers. Especially in the context of more sophisticated cyberweapons, the image of inadvertent collateral damage doesn't hold up. They're more like a flu virus that only makes one family sick.

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

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

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

#### Norms fail—cheating and miscalc

Stewart Baker 12, former official at the U.S. Department of Homeland Security and the National Security Agency, 5/1/12, “What Is the Role of Lawyers in Cyberwarfare?,” http://www.abajournal.com/magazine/article/what\_is\_the\_role\_of\_lawyers\_in\_cyberwarfare/

Former Prime Minister Stanley Baldwin summed up Britain’s strategic position in 1932 with a candor no American leader has dared to match in talking about cyberwar: “I think it is well also for the man in the street to realize that there is no power on earth that can protect him from being bombed, whatever people may tell him. The bomber will always get through. ... The only defense is in offense, which means that you have got to kill more women and children more quickly than the enemy if you want to save yourselves.”¶ The British may have been realists about air war, but Americans still hoped to head off the nightmare. The American tool of choice was international law. (Some things never change.) When war broke out on Sept. 1, 1939, President Franklin D. Roosevelt sent a cable to all the combatants seeking express limits on the use of airpower and expressing his view that “ruthless bombing from the air of civilians in unfortified centers of population … has sickened the hearts of every civilized man and woman, and has profoundly shocked the conscience of humanity. ... I am therefore addressing this urgent appeal to every government which may be engaged in hostilities publicly to affirm its determination that its armed forces shall in no event, and under no circumstances, undertake the bombardment from the air of civilian populations or of unfortified cities.”¶ Roosevelt had a pretty good legal case. The Hague Conventions on the Law of War, adopted just two years after the Wright Brothers’ first flight, declared that in bombardments “all necessary steps should be taken to spare as far as possible edifices devoted to religion, art, science, and charity, hospitals, and places where the sick and wounded are collected, provided they are not used at the same time for military purposes.” The League of Nations had recently declared that, in air war, “the intentional bombing of civilian populations is illegal.”¶ But FDR didn’t rely just on law. He asked for a public pledge that would bind all sides. Remarkably, he got it. The horror of aerial bombardment ran so deep in that era that England, France, Germany and Poland all agreed—before nightfall on the same day.¶ What’s more, they tried to honor their pledges. In a June 1940 order for Luftwaffe operations against Britain, Hermann Göring “stressed that every effort should be made to avoid unnecessary loss of life amongst the civilian population.”¶ It began to look like a great victory for the international law of war. All sides had stared into the pit of horrors that civilian bombing would open up. And all had stepped back.¶ It was exactly what the lawyers and diplomats now dealing with cyberwar hope to achieve.¶ But as we know, that’s not how this story ends. On the night of Aug. 24, a Luftwaffe air group made a fateful navigational error. Aiming for oil terminals along the Thames, they miscalculated, instead dropping their bombs in the civilian heart of the city of London.¶ It was a mistake. But that’s not how Churchill saw it. He insisted on immediate retaliation. The next night, British bombers hit targets in Berlin for the first time. The military effect was negligible, but the political impact was profound. Göring had promised that the Luftwaffe would never allow a successful attack on Berlin. The Nazi regime was humiliated, the German people enraged. Ten days later, Hitler told a wildly cheering crowd that he had ordered the bombing of London: “Since they attack our cities, we will extirpate theirs.”¶ The Blitz was on.¶ In the end, London survived. But the extirpation of enemy cities became a permanent part of both sides’ strategy. No longer an illegal horror to be avoided at all costs, the destruction of enemy cities became deliberate policy. Later in the war, British strategists would launch aerial attacks with the avowed aim of causing “the destruction of German cities, the killing of German workers, … the disruption of civilized life throughout Germany … the creation of a refugee problem on an unprecedented scale, and the breakdown of morale both at home and at the battle fronts.”¶ The Hague Conventions, the League of Nations resolution, even the explicit pledges given to President Roosevelt—all these “norms” for the use of airpower had been swept away by the logic of the technology and the predictable psychology of war.¶ So, why do today’s lawyers think that their limits on cyberwar will fare better than FDR’s limits on air war?¶ It beats me. If anything, they have a much harder task. Roosevelt could count on a shared European horror at the aerial destruction of cities. He used that to extract an explicit and reciprocal understanding from both sides as the war was beginning. We have no such understanding, indeed no such shared horror. Quite the contrary, for some of our potential adversaries, cyberweapons are uniquely asymmetric—a horror for us, another day in the field for them. It doesn’t take a high-tech infrastructure to maintain an army that is ready in a pinch to live on grass.¶ What’s more, cheating is easy and strategically profitable. American compliance will be enforced by all those lawyers. Our adversaries can ignore the rules and say—hell, they are saying—“We’re not carrying out cyberattacks. We’re victims too. Maybe you’re the attacker. Or maybe it’s Anonymous. Where’s your proof?”¶ Even if all sides were genuinely committed to limiting cyberwar, as all sides were in 1939, we’ve seen that the logic of airpower eventually drove all sides to the horror they had originally recoiled from. Each side felt that it had observed the limits longer than the other. Each had lawyerly justifications for what it did, and neither understood or gave credence to the other’s justifications. In that climate, all it took was a single error to break the legal limits irreparably.¶ And error was inevitable. Bombs dropped by desperate pilots under fire go astray. But so do cyberweapons. Stuxnet infected thousands of networks as it searched blindly for Natanz. The infections lasted far longer than intended. Should we expect fewer errors from code drafted in the heat of battle and flung at hazard toward the enemy?¶ Of course not. But the lesson for the lawyers and the diplomats is stark: Their effort to impose limits on cyberwar is almost certainly doomed.¶ No one can welcome this conclusion, at least not in the United States. We have advantages in traditional war that we lack in cyberwar. We are not used to the idea that launching even small wars on distant continents may cause death and suffering here at home. That is what drives the lawyers. They hope to maintain the old world. But they’re driving down a dead end.¶ If we want to defend against the horrors of cyberwar, we need first to face them with the candor of a Stanley Baldwin. Then we need to charge our military strategists, not our lawyers, with constructing a cyberwar strategy for the world we live in, not the world we’d like to live in.

#### Cheating is strategically profitable and accidents prevent norms from sticking

Stewart Baker 11, a former official at the U.S. Department of Homeland Security and the National Security Agency, 9/30, “Denial of Service,” FP, http://www.foreignpolicy.com/articles/2011/09/30/denial\_of\_service

What's more, cheating is easy and strategically profitable. America's compliance will be enforced by all those lawyers. Its adversaries' compliance will be enforced by, well, by no one. It will be difficult, if not impossible, to find a return address on their cyberattacks. They can ignore the rules and say -- hell, they are saying -- "We're not carrying out cyberattacks. We're victims too. Maybe you're the attacker. Or maybe it's Anonymous. Where's your proof?"¶ Even if all sides were genuinely committed to limiting cyberwar, as they were in 1939, history shows that it only takes a single error to break the legal limits forever. And error is inevitable. Bombs dropped by desperate pilots under fire go astray -- and so do cyberweapons. Stuxnet infected thousands of networks as it searched blindly for Iran's uranium-enrichment centrifuges. The infections lasted far longer than intended. Should we expect fewer errors from code drafted in the heat of battle and flung at hazard toward the enemy?¶ Of course not. But the lesson of all this for the lawyers and the diplomats is stark: Their effort to impose limits on cyberwar is almost certainly doomed.¶ No one can welcome this conclusion, at least not in the United States. The country has advantages in traditional war that it lacks in cyberwar. Americans are not used to the idea that launching even small wars on distant continents may cause death and suffering at home. That is what drives the lawyers -- they hope to maintain the old world. But they're being driven down a dead end.

# 2NC Adv 2

#### Cyber cooperation with Japan is high and spills over—their evidence says that’s key

Mihoko Matsubara 6/13/13, cybersecurity analyst, adjunct Fellow with the Center for Strategic and International Studies Pacific Forum, “Japan's New Cybersecurity Strategy - Implications For The Alliance?,” http://www.forbes.com/sites/jonathanmiller/2013/06/13/japans-new-cybersecurity-strategy-implications-for-the-alliance/

On June 10, the Japanese government adopted the Cybersecurity Strategy to replace the Information Security Strategy for Protecting the Nation, which was crafted in May 2010 and expires in March 2014. This is the first time for Tokyo to employ the word, “cybersecurity,” in its strategy to deal with information security issues and cyber threats to its national interests. Japan is planning on creating an action plan based on this strategy by the end of June.¶ In the past, Tokyo focused its efforts on minimizing cyber espionage although the 2010 strategy briefly mentions about potential risks of disruption to critical infrastructure. A series of cyber espionage incidents against the Japanese government and defense industry were revealed recently which has served to elevate the issue of cyber security for Japan. Indeed there have been notable espionage attacks on Mitsubishi Heavy Industriesand the Japanese Diet in 2011.¶ Yet, information theft is just one of many potential consequences from cyber-attacks. Physical disruption of critical services can occur and such cases have happened elsewhere in the world. For example, in August 2003, a computer worm penetrated the network of the Davis-Besse nuclear plantin Ohio and disabled two monitoring systems for five hours. Needless to say, a similar scenario could be potentially devastating for Japan’s already beleaguered nuclear program.¶ While the Information Security Strategy notices that cyber-attacks can bring grave impacts on national security and crisis management, the true wake-up call did not ring until 2013. On March 20, cyber-attacks were launched against South Korean banks and TV broadcasters and paralyzed their business operations.¶ Following this incident, both the Japanese public and private sectors became more concerned about cyber incidents and their adverse effects. Despite a rapid growth in cybersecurity-related projects and an increasing demand for experts, Japan continues to struggle with building an adequate capacity to fend off this threat. The country recognizes the necessity for public-private or academia-public-private partnerships to share information; however, most of organizations are unable to take advantage of this information flow due to a lack of financial and human resources. While the Cybersecurity Strategy points out the necessity of developing human resources, the Action Plan needs to elucidate how to recruit, educate, or train such experts and how to utilize the expertise within each organization.¶ The Cybersecurity Strategy refers to the survey result regarding the shortage of cybersecurity experts, but focuses on technical expertise only. According to the Information-technology Promotion Agency, Japan is short of 80,000 technical experts, whereas the country has about 265,000 experts and 160,000 of them need further education or training. Still, because cyber threats can affect any aspect of human activities, cybersecurity efforts also demand anthropological, defense, geopolitics, legal, linguistic, and technical expertise. This wide variety of skill collaboration calls forcareful selection of trustworthy partners to work together in the academia, government, and industry — most likely not only within Japan but also outside the country. Japan has no domestic anti-virus software manufacturer known in the international market.¶ On the other hand, the strategy addresses epoch-making initiatives by the government. For example, echoing the first cybersecurity principle of the Ministry of Defense (MOD) and Self-Defense Forces (SDF), the government emphasizes that the SDF is responsible for countering cyber-attacks when they constitute armed attacks although the strategy does not elucidate what is “armed attack” in cyberspace. Accordingly, the MOD is launching the Cyber Defense Unit. Next , the document proposes to add new categories to critical infrastructure if necessary in order to minimize disruption to the lives of citizens and their socioeconomic activities.¶ In September 2012, Harold Koh, Legal Advisor to the U.S. Department of State, gave three examples of “use of force” in cyberspace. Interestingly enough, all of them are sabotage against critical infrastructure: a nuclear plant meltdown; disruption to a dam to cause flood; and airplane crashes.¶ This interpretation certainly raised a sensitive question for the Japan-U.S. alliance and prompted officials on both sides to ponder the need to transcend beyond the traditional scope of the alliance. Tokyo and Washington are currently discussing the revision of their bilateral defense-cooperation guidelines and the modification may cover cybersecurity for the first time. Japan has interpreted that the constitution does not allow the country to execute the right of collective self-defense. Under the 2nd Shinzo Abe administration, his national security advisory panel started studying if the execution of this right should cover cyberspace. Because attribution is difficult and there is no internationally-agreed definition of “armed attack” or “use of force” in cyberspace, this makes collective self-defense in the domain challenging. Still, Washington is pursuing collective cybersecurity with allies and this may have a symbolic meaning for the alliances to show the strong will to counter cyber threats collaboratively.¶ The U.S. government would appreciate information-sharing about the defense industry, given the series of cyber espionage targeting American and Japanese defense contractors. The United States counts the defense industry as part of its critical infrastructure. Also, Washington is expanding an information-sharing framework this year, based on the cooperative mechanism of the defense industrial base under the Executive Order to improve critical infrastructure’s cybersecurity. Thus, Washington would find it encouraging that Japan’s Cybersecurity Strategy specifically argues that Tokyo will start discussions on including the critical infrastructure sector.¶ The Cybersecurity Strategy surely presents Tokyo’s determination to deal with growing cyber threats and would send positive signals to its ally, the United States. The Japanese government should incorporate specific steps for human resources and domestic or international cooperation in the action plan.

#### U.S. can adapt to A2/AD

James Dobbins 12, directs the International Security and Defense Policy Center at the RAND Corporation, previously served as American Ambassador to the European Community and Assistant Secretary of State, August/September 2012, “War with China,” Survival, Vol. 54, No. 4, p. 7-24

The increasing difficulty in ensuring direct defence could be consequential even if Sino-American hostilities are unlikely, for they could stimulate Chinese risk-taking, increase US inhibitions, and weaken the resolve of US allies and China’s neighbours to withstand greater Chinese insistence on sett ling disputes on Beijing’s terms. These trends are the result of underlying general technological progress; sustainable growth in military spending, reform and doctrinal adaptation within the People’s Liberation Army; and geographic distances for China and the United States. On the other hand, most of China’s neighbours are growing both economically and in technological sophistication, and some may choose to keep pace in quality (if not quantity) with Chinese advances in the military field. ¶ Barring unforeseen technological developments that assure survivability for US forces and C4ISR capabilities, it will not be possible or affordable for the United States to buck these trends. As the defence of Taiwan is already becoming problematic for US forces (including for its carriers and nearby air bases), so will US operational options in the event of a confrontation with China over a North Korean collapse or a crisis in Southeast Asia. Over time, the United States is likely to become increasingly reliant on its more distant and less vulnerable capabilities. As US forward-operating survivability declines, strike range must increase. US military-operational emphasis in the Western Pacific will thus shift from geographically limited direct defence to more escalatory responses, and eventually, when even these will not suffice, from deterrence based on denial to deterrence based on the threat of punishment, with the speed of the shift likely to be more swift in Taiwan, followed by Northeast Asia and then Southeast Asia at a somewhat later date.

#### US can counter A2AD—empirics

Daniel Goure 09, Ph.D. degrees in international relations and Russian Studies, Vice President with the Lexington Institute, former Deputy Director, International Security Program at the Center for Strategic and International Studies, former director of the Office of Strategic Competitiveness in the Office of the Secretary of Defense, adjunct professor in graduate programs at the Center for Peace and Security Studies at Georgetown University, and an adjunct professor at National Defense University since 2002, 10/23, “The Overblown Anti-Access, Area Denial Threat,” http://www.lexingtoninstitute.org/the-overblown-anti-access-area-denial-threat

For more than a decade, the national security community has spilt an amazing amount of ink discussing the so-called anti-access, area denial (AA/AD) threat. For the few of you who have been spared the barrage of reports and discussions of this particular problem, it involves our adversaries’ use of systems and techniques to prevent U.S. military forces from operating overseas in areas where we have vital national interests, friends and allies. Enemies would attack or interdict airfields, ports and land bases overseas, block the sea lanes and deny us the use of critical airspace. The national security literature is replete with warnings that all our potential adversaries from China to Iran and even Hezbollah are pursuing an AA/AD strategy.¶ As a consequence of this threat, the devotees of AA/AD tell us, the entire U.S. military is becoming unusable for any serious kind of conflict. Our fighters will either be destroyed on their forward bases or will have to deploy to airfields that are too distant from the battlefield for them to be effective. The bombers will be shot down by the enemy’s advanced air defenses. Enemy cruise and ballistic missiles and submarines will be used to sink our Navy. Mines deployed at sea and on land will prevent the Marine Corps and the Army from being landed on enemy shores or from maneuvering once they arrive.¶ It is time for the national security community to get a grip on itself. The AA/AD threat is neither new nor all that daunting. The U.S. military has already faced down the mother of all AA/AD threats. It was the Soviet military. The Red Army was postured for the ultimate AA/AD operation, including a massive air and missile assault -- employing chemical weapons -- on all our forward bases and using hundreds of submarines and aircraft to sweep the seas of our ships. The AA/AD Cassandras are hyping today’s threat. Equally bad, they are forgetting recent history.¶ The U.S. military will employ a full sweep of technologies, tactics and techniques to counter the AA/AD threat. As my colleague Loren Thompson pointed out in Early Warning a few weeks ago the U.S. Navy has ways of addressing the anti-shipping ballistic missile threat. Advanced organic mine warfare capabilities are being developed to counter sea mines. The Air Force will employ a combination of airfield defenses, electronic warfare, SEAD, unmanned systems, long-range precision weapons and most important, stealthy aircraft to defeat the AA/AD threat. There is an AA/AD threat, but it is not an apocalyptic danger.

#### US doctrinal shifts solve the impact

General Norton Schwartz 12, USAF, is Chief of Staff of the United States Air Force. Admiral Jonathan W. Greenert, USN, is Chief of Naval Operations, 2/20/12, “Air-Sea Battle,” http://www.the-american-interest.com/article.cfm?piece=1212#sthash.1ydZ7O5m.dpuf

Air-Sea Battle is designed to sustain America’s freedom of action in the face of these developments. Although Air-Sea Battle aims to create a more credible fighting force, our vision should not be mistaken for a one-dimensional combat plan against specific adversaries. Air-Sea Battle’s purpose is to guide our services’ efforts to organize, train and equip our forces by describing how to ensure freedom of action for the entire Joint Force. Operational plans building on the Air-Sea Battle concept will not be developed in the Pentagon but by the combatant commanders themselves. Our focus is on how to provide combatant commanders the capabilities needed to gain and maintain access as part of their plans.¶ We will organize, train and equip, however, with increasingly constrained resources. We cannot expect to defeat modern anti-access threats by building larger numbers of more advanced, more expensive, less-integrated ships and aircraft. The emerging geopolitical environment, the rapid expansion and proliferation of anti-access and area-denial weapons capabilities, and looming domestic budgetary constraints dictate that we must improve our power projection capabilities in smarter, more cost-effective ways.¶ We will of course continue to develop superior technology, but we must also focus on improving the ability of existing platforms to operate or deliver effects in denied areas. This will include new, more integrated weapons, sensors, cyber and electronic warfare, and unmanned systems. These systems and payloads can evolve more quickly than their manned host platforms, allowing more rapid exploitation of new technologies. This is an essential element of Air Sea Battle capabilities.¶ We will also rely on a uniquely American capability that cannot be hacked or reverse-engineered: our skilled sailors and airmen, our long histories of success, and our shared values. We will foster a more permanent, well-institutionalized partnership, with corresponding organizational structure, operational concepts, training, readiness and acquisition strategies that will capitalize on our commonalities and maximize our collective ingenuity.¶ The first steps to implement Air-Sea Battle are already underway here at the Pentagon. In our FY 2012 and FY 2013 budgets we increased investment in the systems and capabilities we need to defeat access threats. We also established a new Air-Sea Battle Office to improve integration and inter-service communication. Institutionalizing these arrangements is a key to fostering persistent and sustainable progress in Air-Sea Battle implementation and to engender the “culture of change” highlighted in the new strategic guidance to the Department of Defense. Much as AirLand Battle and its “31 Initiatives” influenced a generation of airmen and soldiers, we want Air-Sea Battle to shape a new generation of airmen and sailors. Active collaboration between our services will reveal untapped synergies in key areas such as intelligence, surveillance and reconnaissance; electronic warfare; command and control; and building and sustaining fruitful international partnerships with U.S. allies, partners and friends.¶ Our future investment, doctrine development and innovation will be guided by employing tightly integrated, cross-domain operations to defeat anti-access and area-denial threats and restore our freedom of action. This central idea is embodied in the construct of “Networked, Integrated Attack-in-Depth.” This construct is used to pursue three lines of effort to disrupt, destroy and defeat adversary anti-access and area-denial capabilities:¶ “Networked”: By establishing resilient communications networks and reinforcing the links between people and organizations, air and naval forces will maintain decision advantage and effective cross-domain operations despite an adversary’s anti-access and area-denial efforts.¶ “Integrated”: Air and naval forces will tightly coordinate their operations across each domain to defeat anti-access and area-denial threats. This will require new models for command and control to allow, for example, cyber or undersea operations to defeat air defense systems or air attacks to eliminate submarine or mine threats. Air and naval force integration will also capitalize on multiple attack pathways to increase combat efficiency and hold targets at risk that would otherwise be immune from attack.¶ “Attack-in-Depth”: In traditional attrition models of warfare, forces attack the outer layer of an enemy’s defenses and deliberately fight their way in. In contrast, under Air-Sea Battle, forces will attack adversary systems wherever needed to gain access to contested areas needed to achieve operational objectives.¶ Using “Networked, Integrated Attack-in-Depth”, American air and naval forces will conduct operations along three main lines of effort:¶ Disrupt. This category includes offensive operations to deceive or deny adversary battle networks, particularly intelligence, surveillance and reconnaissance (ISR) and command and control (C2) systems. This reduces the effective density of adversary anti-access systems by forcing attacks against false targets, causing adversary hesitation in the face of poor information, and preventing the cueing of adversary ships, missiles, electronic warfare systems and aircraft.¶ Destroy. Offensive operations to neutralize adversary weapon delivery platforms such as ships, submarines, aircraft and missile launchers fall into this category. This also prevents the adversary from extending the range of the denied area, and reduces the density of anti-access and area-denial attacks.¶ Defeat. Defensive operations to protect joint forces and their enablers from weapons launched by an adversary are important to the Air-Sea Battle concept. Our efforts to disrupt the enemy’s C2 and ISR will reduce the density of attacks to enhance the effectiveness of our defensive systems.¶ The Air-Sea Battle operational concept will guide our efforts to train and prepare air and naval forces for combat. We already train together and share joint doctrine. Under Air-Sea Battle, we will take “jointness” to a new level, working together to establish more integrated exercises against more realistic threats. Our people will practice coordinated operations combining stealthy submarines, stealthy aircraft and remotely piloted vehicles. We will learn to deliver full-motion video directly from Air Force remotely piloted aircraft to Navy ships transiting high-threat regions. We will coordinate between Air Force and Navy operations centers to create seamless and resilient command and control networks. We will learn how to integrate naval forces into airfield defense, and we will train our Air Force aircrews to defend ships at sea. To identify and exploit these synergies, commanders will promulgate promising ideas across the services, and we will incorporate them into our budgeting, acquisition, and development of doctrine and tactics. These efforts will sustain American military credibility, enhance the expeditionary credibility of ground forces and bolster international trust in critical areas where U.S. power projection capabilities underpin regional stability and security.

# \*\*\*1NR\*\*\*