# R3, MN ST, Open Source

# 1NC

### 1

#### Interpretation:

#### “restriction” is a method of prohibiting authority

P.A. Mohammed, J. Sri Chithira Aero And Adventure ... vs The Director General Of Civil ... on 24 January, 1997¶ Equivalent citations: AIR 1997 Ker 121¶ Sri Chithira Aero And Adventure ... vs The Director General Of Civil ... on 24 January, 1997. http://www.indiankanoon.org/doc/255504/?type=print

10. Microlight aircrafts or hang gliders shall not be flown over an assembly of persons or over congested areas or restricted areas including cantonment areas, defence installations etc. unless prior permission in writing is obtained from appropriate authorities. These provisions do not create any restrictions. There is no total prohibition of operation of microlight aircraft or hang gliders. The distinction between 'regulation' and 'restriction' must be clearly perceived. The 'regulation' is a process which aids main function within the legal precinct whereas 'restriction' is a process which prevents the function without legal sanction. Regulation is allowable but restriction is objectionable. What is contained in the impugned clauses is, only regulations and not restrictions, complete or partial. They are issued with authority conferred on the first respondent, under Rule 133A of the Aircraft Rules consistent with the provisions contained in the Aircraft Act 1934 relating to the operation, use etc. of aircrafts flying in India. Microlight aircrafts, hang gliders and powered hang gliders are all coming within the definition of 'aircraft' contained in Section 2( 1) of the Act. Section 5 of the Act authorises the Central Government to make rules regulating among other things use and operation of aircraft and lor securing the safety of aircraft operation. Rule 133A authorises the first respondent to issue directions relating to the operation and use of the aircraft. Thus the analysis of the above provisions would sufficiently indicate that the impugned clauses contained in Exts. P4 and P5 are purely measures regulating the use and operation of aircrafts.

#### “Statutory restrictions” means congress

**Mortenson 11** (Julian Davis Assistant Professor, University of Michigan Law School, “Review: Executive Power and the Discipline of History Crisis and Command: The History of Executive Power from George Washington to George W. Bush John Yoo. Kaplan, 2009. Pp vii, 524,” Winter 2011, University of Chicago Law Review 78 U. Chi. L. Rev. 377)

At least two of Yoo's main examples of presidential power are actually instances of presidential deference to statutory restrictions during times of great national peril. The earliest is Washington's military suppression of the Whiskey Rebellion (III, pp 66-72), a domestic disturbance that Americans viewed as implicating adventurism by European powers and threatening to dismember the new nation. n60 The Calling Forth Act of 1792 n61 allowed the President to mobilize state militias under federal control, but included a series of mandatory procedural checks--including judicial [\*399] approval--that restricted his ability to do so. n62 Far from defying these comprehensive restrictions at a moment of grave crisis, Washington satisfied their every requirement in scrupulous detail. He issued a proclamation ordering the Whiskey Rebels to disperse. n63 When they refused to do so, he submitted a statement to Justice James Wilson of the Supreme Court describing the situation in Pennsylvania and requesting statutory certification. n64 Only when Wilson issued a letter precisely reciting the requisite statutory language (after first requiring the President to come back with authentication of underlying reports and verification of their handwriting n65) did Washington muster the troops. n66 Washington's compliance with statutory restrictions on his use of force continued even after his forces were in the field. Because Congress was not in session when he issued the call-up order, Washington was authorized by statute to mobilize militias from other states besides Pennsylvania--but only "until the expiration of thirty days after the commencement of the ensuing [congressional] session." n67 When it became clear that the Pennsylvania campaign would take longer than that, Washington went back to Congress to petition for extension of the statutory time limit that would otherwise have required him to [\*400] disband his troops. n68 Far from serving as an archetypal example of presidential defiance, the Whiskey Rebellion demonstrates exactly the opposite. FDR's efforts to supply the United Kingdom's war effort before Pearl Harbor teach a similar lesson. During the run-up to America's entry into the war, Congress passed a series of Neutrality Acts that supplemented longstanding statutory restrictions on providing assistance to foreign belligerents. Despite these restrictions, FDR sent a range of military assistance to the future Allies. n69 Yoo makes two important claims about the administration's actions during this period. First, he claims the administration asserted that "[a]ny statutory effort by Congress to prevent the President from transferring military equipment to help American national security would be of 'questionable constitutionality'" (III, p 300). Second, he suggests that American military assistance in fact violated the neutrality statutes (III, pp 295-301, 310, 327-28).

#### Violation: the plan is an affirmative obligation, not a restriction.

David J. Barron & Martin S. Lederman, Harvard Law Review, February 2008. “THE COMMANDER IN CHIEF AT THE LOWEST EBB — A CONSTITUTIONAL HISTORY,” http://www.harvardlawreview.org/media/pdf/barron\_lederman2.pdf

This compromise did not address Browning’s separation of powers ¶ concern. But it did make the bill more palatable from the Administration’s perspective. In fact, to the chagrin of the Radical Republicans,290 the Act proved difficult to enforce, partly because the Attorney ¶ General pointedly refused to offer guidance on its meaning to district ¶ attorneys.291 Nevertheless, the bill was, as Browning knew, a remarkable example of a law regulating the discretion of the Commander in ¶ Chief. It dealt specifically with a tactic to be applied directly to the ¶ enemy. It imposed not a restriction, but an affirmative obligation on the President, because Congress perceived him as being insufficiently ¶ aggressive. And it was enacted not as a background, framework statute to govern all wars, but in the midst of a particular war, as a corrective to what Congress saw as an inadequate executive policy toward a ¶ particular foe. Nevertheless, as far as we have been able to discern, no ¶ executive branch official — including the President and his Attorney ¶ General — contended at any point in the extensive debate that the Act ¶ unconstitutionally interfered with the President’s constitutional war ¶ authority.292

#### Vote neg for limits – they make the mechanism of the topic limitless - the Aff doesn’t have to actually decrease the presidents authority for war, they just add obligations to the authority, any form of notification becomes topical

#### Limits are key to clash and education – we can’t prepare without a predictable focus for the debate

### 2

#### Debt Ceiling will pass now—business lobby

Pollways, 9/19, (“Business groups tell House Republicans: No anti-Obamacare hostage-taking”, 9/19/2013, <http://pollways.bangordailynews.com/2013/09/19/national/business-groups-tell-house-republicans-no-anti-obamacare-hostage-taking/?ref=blogswidget>)

Business Republicans do not want a government shutdown. They do not want the full faith and credit of the United States to be undermined by a refusal to raise the debt limit. Threatening to shut down the government and to not increase the debt limit are the strategies chosen by Tea Party groups to try to stop funding of the Affordable Care Act. (By the way, a shutdown wouldn’t cut off the ACA’s revenue stream. Much like Social Security, nearly all of this funding commitment is now automatically set.) Now the U.S. Chamber of Commerce has joined the Wall St. Journal editorial page in opposing a shutdown and debt default. It’s fascinating to see how the Chamber of Commerce starts by telling its usual allies that they, you know, support capitalism. The Chamber’s open letter to House Republicans begins: The U.S. Chamber of Commerce, the world’s largest business federation representing the interests of more than three million businesses and organizations of all sizes, sectors, and regions, as well as state and local chambers and industry associations, and dedicated to promoting, protecting and defending America’s free enterprise system, urges the House of Representatives to pass H.J. Res. 59, the “Continuing Appropriations Resolution, 2014,” to ensure the uninterrupted funding of the federal government into the next fiscal year at spending levels consistent with P.L. 112-25, the Budget Control Act of 2011. Making clear a shutdown and default would cause real economic harm, the letter states: It is not in the best interest of the U.S. business community or the American people to risk even a brief government shutdown that might trigger disruptive consequences or raise new policy uncertainties washing over the U.S. economy. Likewise, the U.S. Chamber respectfully urges the House of Representatives to raise the debt ceiling in a timely manner and thus eliminate any question of threat to the full faith and credit of the United States government. Also weighing in on this hostage-taking is the Business Roundtable, which describes itself as “an association of chief executive officers of leading U.S. companies with $7.4 trillion in annual revenues and more than 16 million employees.” According to a new study by the Business Roundtable: Fifty percent of responding CEOs indicated that the ongoing disagreement in Washington over the 2014 budget and the debt ceiling is having a negative impact on their plans for hiring additional employees over the next six months. Typically allied with Republicans and consistently giving most of their campaign donations to Republicans, business groups are saying, please, please don’t do this. Will House Republicans listen? And, if not, will these business groups decide they have to reconsider which politicians they support? Look for Republican party leaders, to the extent they exist anymore, to try to resolve this situation and heal this schism.

**Plan destroys Obama’s credibility – makes it impossible for him to get anything through Congress**

Seeking Alpha 9-10, 9-10-2013, “Syria Could Upend Debt Ceiling Fight,” http://seekingalpha.com/article/1684082-syria-could-upend-debt-ceiling-fight

Unless President Obama can totally change a reluctant public's perception of another Middle-Eastern conflict, it seems unlikely that he can get 218 votes in the House, though he can probably still squeak out 60 votes in the Senate. This defeat would be totally unprecedented as a President has never lost a military authorization vote in American history. To forbid the Commander-in-Chief of his primary power renders him all but impotent. At this point, a rebuff from the House is a 67%-75% probability. I reach this probability by looking within the whip count. I assume the 164 declared "no" votes will stay in the "no" column. To get to 218, Obama needs to win over 193 of the 244 undecided, a gargantuan task. Within the "no" column, there are 137 Republicans. Under a best case scenario, Boehner could corral 50 "yes" votes, which would require Obama to pick up 168 of the 200 Democrats, 84%. Many of these Democrats rode to power because of their opposition to Iraq, which makes it difficult for them to support military conflict. The only way to generate near unanimity among the undecided Democrats is if they choose to support the President (recognizing the political ramifications of a defeat) despite personal misgivings. The idea that all undecided Democrats can be convinced of this argument is relatively slim, especially as there are few votes to lose. In the best case scenario, the House could reach 223-225 votes, barely enough to get it through. Under the worst case, there are only 150 votes. Given the lopsided nature of the breakdown, the chance of House passage is about one in four. **While a failure in the House would put action against Syria in limbo, I have felt that the market has overstated the impact of a strike there**, which would be limited in nature. Rather, **investors should focus on the profound ripple through the power structure in Washington, which would greatly impact impending battles over** spending and **the debt ceiling**. Currently, **the government** loses spending authority on September 30 while it **hits the debt ceiling by the middle of October. Markets have generally felt that Washington will once again strike a last-minute deal and avert total catastrophe**. Failure in the Syrian vote could change this**. For the Republicans to beat Obama on a President's strength (foreign military action), they will likely be emboldened that they can beat him on domestic spending issues.**  **Until now, consensus has been that the two sides would compromise** to fund the government at sequester levels while **passing a $1 trillion stand**

#### Political capital is finite and key --- the plan trades off

Moore, 9/10 --- Guardian's US finance and economics editor (Heidi, 9/10/2013, “Syria: the great distraction; Obama is focused on a conflict abroad, but the fight he should be gearing up for is with Congress on America's economic security,” [http://www.theguardian.com/commentisfree/2013/sep/10/obama-syria-what-about-sequester)](http://www.theguardian.com/commentisfree/2013/sep/10/obama-syria-what-about-sequester%29))

Before President Obama speaks to the nation about Syria tonight, take a look at what this fall will look like inside America. There are 49 million people in the country who suffered inadequate access to food in 2012, leaving the percentage of "food-insecure" Americans at about one-sixth of the US population. At the same time, Congress refused to pass food-stamp legislation this summer, pushing it off again and threatening draconian cuts. The country will crash into the debt ceiling in mid-October, which would be an economic disaster, especially with a government shutdown looming at the same time. These are deadlines that Congress already learned two years ago not to toy with, but memories appear to be preciously short. The Federal Reserve needs a new chief in three months, someone who will help the country confront its raging unemployment crisis that has left 12 million people without jobs. The president has promised to choose a warm body within the next three weeks, despite the fact that his top pick, Larry Summers, would likely spark an ugly confirmation battle – the "fight of the century," according to some – with a Congress already unwilling to do the President's bidding. Congress was supposed to pass a farm bill this summer, but declined to do so even though the task is already two years late. As a result, the country has no farm bill, leaving agricultural subsidies up in the air, farmers uncertain about what their financial picture looks like, and a potential food crisis on the horizon. The two main housing agencies, Fannie Mae and Freddie Mac, have been in limbo for four years and are desperately in need of reform that should start this fall, but there is scant attention to the problem. These are the problems going unattended by the Obama administration while his aides and cabinet members have been wasting the nation's time making the rounds on television and Capitol Hill stumping for a profoundly unpopular war. The fact that all this chest-beating was for naught, and an easy solution seems on the horizon, belies the single-minded intensity that the Obama White House brought to its insistence on bombing Syria. More than one wag has suggested, with the utmost reason, that if Obama had brought this kind of passion to domestic initiatives, the country would be in better condition right now. As it is, public policy is embarrassingly in shambles at home while the administration throws all of its resources and political capital behind a widely hated plan to get involved in a civil war overseas. The upshot for the president may be that it's easier to wage war with a foreign power than go head-to-head with the US Congress, even as America suffers from neglect. This is the paradox that President Obama is facing this fall, as he appears to turn his back on a number of crucial and urgent domestic initiatives in order to spend all of his meager political capital on striking Syria. Syria does present a significant humanitarian crisis, which has been true for the past two years that the Obama administration has completely ignored the atrocities of Bashar al-Assad. Two years is also roughly the same amount of time that key domestic initiatives have also gone ignored as Obama and Congress engage in petty battles for dominance and leave the country to run itself on a starvation diet imposed by sequestration cuts. Leon Panetta tells the story of how he tried to lobby against sequestration only to be told: Leon, you don't understand. The Congress is resigned to failure. Similarly, those on Wall Street, the Federal Reserve, those working at government agencies, and voters themselves have become all too practiced at ignoring the determined incompetence of those in Washington. Political capital – the ability to horse-trade and win political favors from a receptive audience – is a finite resource in Washington. Pursuing misguided policies takes up time, but it also eats up credibility in asking for the next favor. It's fair to say that congressional Republicans, particularly in the House, have no love for Obama and are likely to oppose anything he supports. That's exactly the reason the White House should stop proposing policies as if it is scattering buckshot and focus with intensity on the domestic tasks it wants to accomplish, one at a time. The president is scheduled to speak six times this week, mostly about Syria. That includes evening news interviews, an address to the nation, and numerous other speeches. Behind the scenes, he is calling members of Congress to get them to fall into line. Secretary of State John Kerry is omnipresent, so ubiquitous on TV that it may be easier just to get him his own talk show called Syria Today. It would be a treat to see White House aides lobbying as aggressively – and on as many talk shows – for a better food stamp bill, an end to the debt-ceiling drama, or a solution to the senseless sequestration cuts, as it is on what is clearly a useless boondoggle in Syria. There's no reason to believe that Congress can have an all-consuming debate about Syria and then, somehow refreshed, return to a domestic agenda that has been as chaotic and urgent as any in recent memory. The President should have judged his options better. As it is, he should now judge his actions better.

#### This will destroy the U.S. and global economy

Davidson, 9/10 (Adam - co-founder of NPR’s “Planet Money” 9/10/2013, “Our Debt to Society,” <http://www.nytimes.com/2013/09/15/magazine/our-debt-to-society.html?pagewanted=all&_r=0)>)

This is the definition of a deficit, and it illustrates why the government needs to borrow money almost every day to pay its bills. Of course, all that daily borrowing adds up, and we are rapidly approaching what is called the X-Date — the day, somewhere in the next six weeks, when the government, by law, cannot borrow another penny. Congress has imposed a strict limit on how much debt the federal government can accumulate, but for nearly 90 years, it has raised the ceiling well before it was reached. But since a large number of Tea Party-aligned Republicans entered the House of Representatives, in 2011, raising that debt ceiling has become a matter of fierce debate. This summer, House Republicans have promised, in Speaker John Boehner’s words, “a whale of a fight” before they raise the debt ceiling — if they even raise it at all. 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.

**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 (IAI) in Rome. He served as IAI president from 1979 to 2001. Until 2009, he also occupied the position of executive vice chairman of the Council for the United States and Italy, which he co-founded in 1983. His areas of expertise include transatlantic relations, European integration and nuclear non-proliferation, with particular focus on nuclear science and technology. A Post-Secular World? Survival, 53:2, 117 – 130

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.

### 3

#### Cyber-insecurity injects an adversarial frame into the debate—fear of an invisible cyber threat militarizes the cyber domain

Cavelty, October 22, 2012 (Myriam Dunn, The Militarisation of Cyber Security as a Source of Global Tension, <http://isn.ch/Digital-Library/Articles/Special-Feature/Detail/?lng=en&id=153888&tabid=1453349960&contextid774=153888&contextid775=153887> )

Over the last few years, cyber security has been catapulted from the confined realm of technical experts into the political limelight. The discovery of the industry- sabotaging Stuxnet computer worm, numerous tales of (Chinese) cyber espionage, the growing sophistication of cyber criminals, and the well-publicised activities of hacker collectives have combined to give the impression that cyber attacks are becoming more frequent, more organised, more costly, and altogether more dangerous. As a result, a growing number of countries consider cyber security to be one of the top security issues of the future. This is just the latest ‘surge’ of attention in the three- to four-decade-long history of cyber issues. The importance attached to cyber security in politics grew steadily in response to a continual parade of incidents such as computer viruses, data theft, and other penetrations of networked computer systems, which, combined with heightening media attention, created the feeling that the level of cyber insecurity was on the rise. As a result, the debate spread in two directions: up- wards, from the expert level to executive decision-makers and politicians; and horizontally, advancing from mainly being an issue of relevance to the US to the top of the threat list of more and more countries. The debate on ‘cyber security’ originated in the US in the 1970s, built momentum in the late 1980s, and spread to other countries in the late 1990s.Early on, US policy-makers politicised the issue. They presented cyber security as a matter that requires the attention of state actors because it cannot be solved by market forces. As concern increased, they securitised the issue: They represented it as a challenge requiring the urgent attention of the national security apparatus. In 2010, against the background of the Stuxnet incident, the tone and intensity of the debate changed even further: The latest trend is to frame cyber security as a strategic-military issue and to focus on countermeasures such as cyber offence and defence, or cyber deterrence. Though this trend can easily be understood when considering the political (and psychological) effects of Stuxnet, it nonetheless invokes images of a sup- posed adversary even though there is no identifiable enemy, is too strongly focused on national security measures instead of economic and business solutions, and wrongly suggests that states can establish control over cyberspace. Not only does this create an unnecessary atmosphere of insecurity and tension in the international system, it is also based on a severe misperception of the nature and level of cyber risk and on the feasibility of different protection measures. While it is undisputed that the cyber dimension will play a substantial role in future conflicts of all grades and shades, threat-representations must remain well informed and well balanced at all times in order to rule out policy reactions with excessively high costs and uncertain benefits.

#### Security discourse is constructed and shapes policy- root cause of war, causes dehumanization and extermination

**Talbot 8** ( 'Us' and 'Them': Terrorism, Conflict and (O)ther Discursive Formations by Steven Talbot Defence Science and Technology Organisation Sociological Research Online, Volume 13, Issue 1Published: 21/3/2008

As a point of departure, this paper aims to explore the significance of identity[1](http://www.socresonline.org.uk/13/1/17.html#fn1)formation and negotiation as it pertains to various representations of terrorism. Particularly, this paper examines the ways in which adversarial identities are socially constructed according to notions of difference which simultaneously encourages a comparison to, and rejection of, [O]thers. Drawing upon the notion of the Other, this paper examines some of the ways in which identity is constructed through a variety of social and historical processes, and articulated within a range of discourses evoking different and often mutually exclusive combinations of sameness and difference. Using a social constructionist lens, I argue that representations of terrorism are constructed from within specific discourses which accentuate difference. My analysis therefore positions identity formation within a dynamic and relational context where discursive representation, ways of knowing, power and language intertwine. 1.4 Consequently, the following discussion explores identity formation and terrorism through an interpretive, constitutive and discursive lens. I start my discussion with an overview of the socially constructed or constituted nature of identity. This is followed by an exploration of the roles various discursive frameworks play in shaping representations of identity. I then examine some of the implications for viewing terrorism and identities within dichotomous frameworks, particularly within notions of Self and Other, and consequently, the discursive practice of ‘Othering.’ Finally, I interrogate the relational and discursive context of identity further by exploring the relationship between the above theoretical concerns as they pertain to polarised collective identities and intractable conflicts. Socially constituted identities 2.1 Identity construction pertains to the creation, maintenance and articulation of social identities by individuals or groups. Rummens ([2001](http://www.socresonline.org.uk/13/1/17.html#rummens2001)), draws a distinction between personal and social identities. Personal identity usually refers to the result of an identification of self, by self, or in other words the self-identification on the part of the individual. Social identity in contrast refers to the outcome of an identification of self by others, or the identity that is assigned an individual by another (p.3). Both of these concepts differ from self-identity, the individual self which is reflexively understood and worked upon by the individual through self-monitoring and self reflection ([Beck, 1992](http://www.socresonline.org.uk/13/1/17.html#beck1992); [Giddens, 1991](http://www.socresonline.org.uk/13/1/17.html#giddens1991)). 2.2 Sociological research into identity tends to focus on issues concerning the ascribed nature of identity, and the social construction and negotiation of group differences, whereas psychological approaches are more inclined to look at identity development and formation within the individual (i.e. identity searching, self concept and identity crisis). However it is important to remember that identities are not just ascribed or ‘achieved’ through socialisation processes, but are also socially constructed and negotiated between social actors. Through a sociological lens, identities by definition are socially constituted phenomena. In this sense, an individual’s or group’s identity is created, negotiated, and actively recreated through interaction with others. Identity can therefore be viewed as being a verb – it is something that one does, or is accomplished through social interaction ([West and Zimmerman, 1987](http://www.socresonline.org.uk/13/1/17.html#westzimmerman1987)). 2.3 Identity underscores how humans organise and therefore understand their social world. The notion of collective identity has been examined in classic sociological constructs like Marx’s ([1977](http://www.socresonline.org.uk/13/1/17.html#marx1977)) ‘class consciousness,’ Durkheim’s ([1960](http://www.socresonline.org.uk/13/1/17.html#durkheim1960)) ‘collective conscience’ and Weber’s ([1922](http://www.socresonline.org.uk/13/1/17.html#weber1922)) Verstehen (meaningful understanding). The commonality between these works is found in their emphasis on shared attributes, similarities, or the ‘We-ness’ of groups ([Cerulo, 1997](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22cerulo1997), p.386). Thus, the construction of group identities often involves a normative component, or in other words, individuals need to be able to recognise themselves in certain qualities, characteristic or behaviours associated with their group ([Schulte-Tenckhoff, 2001](http://www.socresonline.org.uk/13/1/17.html#schulte-tenckhoff2001), p.6). This recognition of ‘we-ness’ is important given the origins of the term identity. Identity finds its linguistic roots in the Latin noun identitas, with titas being a derivation of the Latin adjective idem meaning the same. Thus, the term is comparative in nature in relation to sharing a degree of sameness with others ([Rummens, 2001](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22rummens2001), p.3). Identity is therefore a relational construct, or as Connolly astutely asserts, ‘[t]here is no identity without difference’ ([1995](http://www.socresonline.org.uk/13/1/17.html#connolly1995), p.xx). 2.4 More significantly, identity constructions often emerge in response to the types of political systems governing that society. Political systems are extensions of societal identity. For example, liberal democracy is a political structure that forms and reflects a part of a societal identity construction in that it proscribes certain ideals and practices which inform members of liberal democratic societies how to live together and treat others. In turn, the pursuit of political goals is also linked to the pursuit of identity (superpower identities inform superpower interests). Consequently, a political system can also be viewed as a source of threat to societal identity ([Hughes, 2004](http://www.socresonline.org.uk/13/1/17.html#hughes2004), p.26). As Hughes observes, for those societies who draw their identity from non-liberal democratic (Western) traditions, the liberal democratic structure, and the values contained within this structure, may be perceived as a threat to group identity. The rhetoric of Osama Bin Laden is an example of this, with its emphasis on acts of violence against the Western, liberal democratic influences and their perceived threat to Islamic identity. 2.5 Political structures and associated organising principles exert influence on political agendas, policy and collective self-definition. Moreover, political elites create, manipulate and dismantle identities of nations and thus shape the subsequent construction of allies and enemies ([Corse, 1996](http://www.socresonline.org.uk/13/1/17.html#corse1996); [Gillis, 1994](http://www.socresonline.org.uk/13/1/17.html#gillis1994); [Zerubavel, 1995](http://www.socresonline.org.uk/13/1/17.html#zerubavel1995) cited in [Cerulo, 1997](http://www.socresonline.org.uk/13/1/17.html#cerulo1997) p.390). Identity shifts can therefore also occur based on changing socio-political factors, for example, as a result of changing policy, increased ethnic politics, and political activism. Constructivists would contend that identities, norms, and culture play an integral role for understanding world politics (and related policy) and international relations, particularly with its emphasis on those processes through which behaviour and identity construction is conceptualised and legitimated by various political agencies. The roles knowledge construction and discourse plays in facilitating this process will be explored in the following discussion. Discourse and identity 3.1 Cultural constructions of identity are shaped by ‘a series of specific dialogues, impositions, and inventions’ ([Clifford, 2004](http://www.socresonline.org.uk/13/1/17.html#clifford2004), p.14). Such a position invariably requires a closer examination of the relationship between identity construction, language, power, knowledge creation and associated discursive practices. 3.2 For Hall, a discourse: ‘defines and produces the objects of our knowledge. It governs the way that a topic can be meaningfully talked about and reasoned about. It also influences how ideas are put into practice and used to regulate the conduct of others’ ([1997](http://www.socresonline.org.uk/13/1/17.html#hall1997), p.44). 3.3 The same discourse (which characterises a way of thinking or the given state of knowledge at one time) can appear throughout a range of texts, across numerous sites. When these discursive events refer to the same object, say terrorism for example, and share a similar style and support a strategy, they are said to belong to the same discursive formation ([Hall, 1997](http://www.socresonline.org.uk/13/1/17.html#hall1997), p.44). It is through these discursive formations that things/practices acquire their meaning. However, discursive representation is not a benign practice, for it is often those in positions of power and authority who are able to construct ‘reality’ and thus knowledge **itself**. As Klein ([1994](http://www.socresonline.org.uk/13/1/17.html#klein1994)) explains: ‘[a] discourse, then, is not a way of learning ‘about’ something out there in the ‘real world’; it is rather a way of producing that something as real, as identifiable, classifiable, knowable, and therefore, meaningful. Discourse creates the conditions of knowing’ (cited in [George, 1994](http://www.socresonline.org.uk/13/1/17.html#george1994), p.30). 3.4 Foucault contends that knowledge is a form of power, and that power is present or exercised within decisions regarding what circumstances knowledge is applied or not. Moreover, Foucault argues that knowledge (when linked to power) assumes the authority of ‘the truth’ and has the power to make itself true through a variety of regulatory and disciplining practices ([Hall, 1997](http://www.socresonline.org.uk/13/1/17.html#hall1997), p.49). Knowledge (ways of knowing about others through discursive representations) therefore is constructed by humans through their interactions with the world around them and is a reflection of existing social, historical and political factors, and as such, is never neutral. 3.5 In his analysis of the socially constructed nature of knowledge, Foucault explores the production of knowledge through discourse, and particularly how knowledge about the social, the individual, and associated shared meanings are produced in specific periods. In Madness and Civilization: A History of Insanity in the Age of Reason (1988) and The History of Sexuality Volume One ([1981](http://www.socresonline.org.uk/13/1/17.html#foucault1981)), Foucault provides examples of the shifting historical significance of sexuality and mental illness and the emergence of deviant identities. In this respect, mental illness and sexuality did not exist as independent objects, which remained the same and meant the same thing throughout all periods. Rather, it was through distinct discursive formations that the objects ‘madness’ or ‘heterosexuality’ emerged and appeared as meaningful constructs. Sexual relations and desires have always been present, but the constructs ‘heterosexual’ and ‘homosexual’ were produced through moral, legal, and medical discourses and practices. Through these discourses and practices, behaviours and acts were aligned with the construction of ‘types of’ people or identities - identities which were subject to medical treatment and legal constraints designed to regulate behaviour. In this respect, social and self identities are a consequence of power reflected in historically and institutionally specific systems/sites of discourse. 3.6 As social constructs, it is important therefore to view knowledge and discourse production through the socio-historical conditions in which they are produced. In this respect, discourses concerning terrorism, security dilemmas and threat, and world order, are produced within specific historical, geographical and socio-political contexts as well as within social relations of power. Furthermore, the controlling and legitimising aspects of discourse are such that proponents of violence are not likely to construct a narrative that is contrary to their values. For instance, Al Qaeda is unlikely to construct a narrative that posits them in a contrary manner to their own moral values by engaging in ‘terrorist’ activities. Rather, they would position themselves as acting morally, and as victims of oppression or humiliation ([Cobb, 2004](http://www.socresonline.org.uk/13/1/17.html#cobb2004)). Similarly, the US and her coalition allies are also likely to construct a narrative which posits their involvement in a ‘fight against terror’ within a discursive framework of liberty and democracy, rather than expansionist or imperialist terms. 3.7 This paper now turns its attention to some of the ways in which identities are constituted through discursive practices which accentuate difference or sameness through the use of binaries. Dichotomous logic and identity construction Self/Other binaries 4.1 Notions of self and other and their implications for identity formation have been explored through psychoanalytical and postcolonial inquiry. In his book The Analysis of the Self: A Systematic Analysis of the Treatment of the Narcissistic Personality Disorders ([1971](http://www.socresonline.org.uk/13/1/17.html#kohut1971)), the founder of the psychology of the self Heinz Kohut extends Freud’s theory of narcissism (which has a dual orientation) in his examination of narcissistic rage and accompanying desires for revenge, and introduces the idea of ‘self-object relationships and transferences’ associated with mirroring and idealisation. Lacan ([2002](http://www.socresonline.org.uk/13/1/17.html#lacan2002)) also draws upon the notion of mirroring in regard to the identity formation of infants. Lacan’s ‘mirror stage’ occurs when the infant recognises its reflection and begins to view itself as being separate from its mother, or observes its mirrored image as viewed by the mother. The mirror stage represents the initial recognition of self as a unified subject, apart from external world and the ‘Other.’ This ‘Other’ (the first ‘big Other’ in an infant’s life being the mother) is fundamental to the constitution of self, as well as sexual identity. 4.2 In his foundational work Orientalism ([1978](http://www.socresonline.org.uk/13/1/17.html#said1978)), Edward Said examines the historical construction of the East (Them/Other) and West (Us/Self) as essentially different entities through discursive practices. Drawing upon Foucault’s notion of discourse, Said contends that Orientalism is a discourse: by which European culture was able to manage – and even produce – the Orient politically, sociologically, militarily, ideologically, scientifically, and imaginatively during the post-Enlightenment period (p. 3). 4.3 Such a discourse draws upon assumptions that are imperialist by design, privilege European sensibilities and representations of the Other, and reinforce ideas concerning the fixed nature of states of being and difference ([McDowell, 2003](http://www.socresonline.org.uk/13/1/17.html#mcdowell2003)). Said argues that Orientalist ideas can be found in current representations of ‘Arab’ cultures as backward, lacking democracy, threatening and anti-Western ([2003](http://www.socresonline.org.uk/13/1/17.html#said2003)). Similarly, Occidentalism[2](http://www.socresonline.org.uk/13/1/17.html#fn2) can be found in stereotypical representations of an “imperialist, corrupting, decadent and alienating West” (Nadje Al-Ali cited in [Freund, 2001](http://www.socresonline.org.uk/13/1/17.html#freund2001)). As I suggest later, these representations have become a feature of the current Western perceptions of terrorism. 4.4 As a practice, Othering is not solely a province of East versus West relations, but also exists as a strategy within other non-Westerns nations. For example, Shah ([2004](http://www.socresonline.org.uk/13/1/17.html#shah2004)), Kennedy-Pipe and Welch ([2005](http://www.socresonline.org.uk/13/1/17.html#kennedy-pipewelch2005)) and Baev ([2007](http://www.socresonline.org.uk/13/1/17.html#baev2007)) note how the ‘war on international terrorism’ discourse has been used by Russia to legitimate it actions against former Soviet republics like Chechnya. 4.5 Within a sociological context, identity discourse is often characterised by issues concerning essentialising and marginalising social groups, as well as totalising and categorising individuals and groups ([Gaudelli, 2001](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22gaudelli2001), p.60). Categorisation results as a response to diversity, wherein categorisation assists with making the diversity (of people) more understandable. As a consequence of this, people become viewed as being more typical of certain categories (eg. a Muslim from Iraq is stereotypically viewed as being ‘Muslim’ in comparison to an Australian Muslim in Cronulla within some discursive frameworks). Following the construction and application of these categories, is a tendency to essentialise (belief in essence) as is evident in notions of ‘the laconic Aussie,’ ‘the whingeing Pom,’ and the ‘fanatical terrorist.’ In this sense, the act of ‘naming’ is akin to ‘knowing.’ 4.6 Dividing practices evident in the categorisation and essentialising processes which inform the production of binaries reflect power struggles, as they primarily entail an external authority imposing a ‘condition of life upon people’ ([Gaudelli, 2001](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22gaudelli2001), p.74) that are supposed to have certain essences. These power relations become evident in the abilities of claim-makers or particular agents to make certain discourses, categories and labels acceptable and make them ‘stick’ as it were. In turn, essentialism results in reifying culture by viewing cultural systems as being discrete and homogeneous units (nationally, ethnically and ideologically), which are ‘naturally given’ and fixed in locality ([Jones, 1999](http://www.socresonline.org.uk/13/1/17.html#jones1999)). Here it is important to remember, that it is not culture that is ‘found’ or ‘discovered’ out in the field, but individuals who act and interact and express their views of culture ([Schulte-Tenckhoff, 2001](http://www.socresonline.org.uk/13/1/17.html#schulte-tenckhoff2001), p.5). This paper contends that it is the relations between groups and related boundary making practices (insider/outsider, Self/Other) rather than ‘traits’ which are important indicators and producers of identity. As discussed above, binaries such as those of Self/Other have a tendency to convey world views in concrete, simplified and often imperialist ways ([Berry, 2006](http://www.socresonline.org.uk/13/1/17.html#berry2006)). The process of ‘Othering’ is commensurate with identification (as culture, community, or nation) which further entails an act of differentiation, authentication, and at times, exclusion – creating boundaries between members of the ‘in’ group and outsiders. In this sense the: ‘Self/Other relation induces comparisons used by social actors to describe themselves or to describe others, depending on their location. In locking a given group into a substantially transformed identity, one constructs and immobilises this relation so that it operates in favour of those to whose advantage it is’ ([Schulte-Tenckhoff, 2001](http://www.socresonline.org.uk/13/1/17.html#schulte-tenckhoff2001), p.11). 4.7 Self/Other relations are therefore ‘matters of power and rhetoric rather than of essence’ ([Clifford, 2004](http://www.socresonline.org.uk/13/1/17.html#clifford2004), p.14). Within this context, boundary-making practices are a way of ‘locking’ ‘imagined communities’ into strategically informed ontological states of being. Moreover, these boundaries are inter-subjectively determined, that is, they are constructed through an emphasis on only a subset of many identity labels that apply (eg. religion). President George Bush has described his war on terror as a ‘crusade’ and a ‘divine plan’ guided by God. These sentiments are similar to Islamic calls for Jihad, with religious terrorists viewing themselves as God’s people and their enemies as God’s enemies, ‘infidels’, or sinners. As a consequence, for both sides, the conflict takes on the form of a ‘spiritual battle.’ Thus religious doctrine acts as fuel for Islamic-based terrorism as it does for the US led ‘war on terror’. Inside this discursive framework, both would contend that each party’s religion is the only meaningful one ([Berry, 2006](http://www.socresonline.org.uk/13/1/17.html#berry2006) p.4). Indeed, the construction of identity plays a key role in relation to the prospect for religious and political violence. Hence, identity claims invariably informs interests. The call by fundamentalist Islamists for a Jihad on Western nations for example is a realisation of both interests and identities simultaneously. In this sense, identities and interests are mutually reinforcing concepts and incapable of being pursued separately ([Hughes, 2004](http://www.socresonline.org.uk/13/1/17.html#hughes2004), p.7). 4.8 Identity negotiation highlights the political nature of social identifications of Self and Others within and between groups. Contestation arises out of those ascribed social or collective identities that do not align with an individual’s or group’s self-definition, highlighting global and national tensions, as well as power dynamics which frequently underplay such identification processes. Hence Self/Other struggles are ultimately struggles of legitimacy and meaning, frequently enacting and fuelling conflict. Indeed, it is in the creation of Self and an all-threatening Other that the state, or prominent figures within terrorist networks like Al Qaeda, use their power and available resources for legitimated violence ([Grondin, 2004](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22grondin2004)). Enemies and Others 4.9 Identity boundaries are functional in that they allow us to distinguish humans from animals, culture from nature, as well as differences between classes and nations. Using identity to distinguish in this way is the foundation for insecurity and conflict. Such boundaries allow the demarcation of ‘Us’ versus ‘Them’ and ‘domestic’ versus ‘foreign.’ Without the creation of these distinctions, the ‘enemy’ could not be identified ([Campbell, 1998](http://www.socresonline.org.uk/13/1/17.html#campbell1998) cited in [Hughes 2004](http://www.socresonline.org.uk/13/1/17.html#hughes2004)). 4.10 Sociology of the enemy examines the social process of constructing enemies, and within the context of identity politics and negotiation, creating Others for advantageous reasons. Politicians, other charismatic leaders, social elites, and the military alike, are in prime positions to construct particular representations of the enemy. In turn, these representations are also influenced by a host of other actors (academics and intellectuals, advisors), and array of sources and representations at their disposal. The proliferation of these representations through the internet, media reports, government documents, books, articles, and film has led to an expansion of an enemy discourse (as part of a deliberate and incidental public diplomacy[3](http://www.socresonline.org.uk/13/1/17.html#fn3)), assisting the articulation of a dualistic collective moral righteousness which attempts to legitimate the destruction of the Other ([Aho, 1994](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22aho1994); cited in [Cerulo 1997](http://www.socresonline.org.uk/13/1/17.html#cerulo1997); [Berry, 2006](http://www.socresonline.org.uk/13/1/17.html#berry2006); [Hansen, 2004](http://www.socresonline.org.uk/13/1/17.html#hansen2004)). 4.11 Orientalist and occidentalist inspired representations of ‘enemies’ can be seen at work within the current terrorism discourse. The Australian and US national security ideology for example frames the terrorism discourse within a system of representations that defines Australian and US national identities through their reference to the Un-Australian, Un-American, Un-Western Other, usually confined to a Muslim/Islamic centre located in the Middle East, but also extending by association to Muslim/Islamist global diasporas. Similarly, representations of the Un-Eastern, Un-Muslim or Non-Islamic Other are employed by some Islamic fundamentalist groups to assert their identity and cause. Both parties construct an enemy that reflect and fuel ideological strains within the American/Australian body politic and Islamist terrorist networks ([Grondin, 2004](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22grondin2004), pp.15-16). The use of dichotomous logic in these representations fails to account for degrees of ‘Otherness’ and ‘Usness,’ or diversity, within both populations. In this sense, the homogenising effects of such a discourse fails to acknowledge an ‘other – Other,’ namely, a more moderate Muslim population located within an Islamic centre and its periphery. Similarly, distinctions can be drawn between an Australian ‘Us’ and her United States counterpart. In either case, the discursive construction of a homogenous West and ‘Rest’ has the effect of silencing dissenting voices residing within both camps. 4.12 Using simple dichotomies like ‘Us’ and ‘Them’ or ‘friend’ or ‘foe’ ignore the multidimensionality of identity and fail to recognise the interconnectedness and complexity of modern life. The use of such terms also highlights the emotional underpinnings for issues of security. With their use of an enemy discourse which incorporates notions of religiosity, good versus evil, and right and wrong, both the Taliban and US led ‘coalition of the willing’ appeal to beliefs over empiricism (what is knowable, measurable and debatable) – belief systems grounded in notions of faith where it is important to believe things to be true, rather than actually being true ([Berry, 2006](http://www.socresonline.org.uk/13/1/17.html#berry2006), p.5). Similarly, claim making of this nature appeals to emotions (like hatred, revenge and fear) in contrast to logic in the sense that they encourage communities to feel in particular ways which are less likely to be challenged than appeals to think in particular ways ([Loseke, 2003](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22loseke2003), p.76). Hence, Berry ([2006](http://www.socresonline.org.uk/13/1/17.html#berry2006)) contends, that because definitions of enemies are often not empirically based, they can fluctuate according to the needs of the definers. 4.13 With the creation of ‘identifiable’ enemies, defining ‘Us’ automatically entails defining ‘Them,’ with ‘Them’ being the social foe or ‘evil’ ([Huntington, 1996](http://www.socresonline.org.uk/13/1/17.html#huntington1996)). As Burman and MacLure ([2005](http://www.socresonline.org.uk/13/1/17.html#burmanmaclure2005)) remind us, ‘there is always a hierarchy in these oppositions’ for there is an essence of a higher principle or ideal articulated in one, and something lesser, or subordinate in the other (p.284). Thus, within this hierarchical value system of prioritised logic, good is seen as coming before evil, positive before negative, Us before Them, and real over the written. Moreover, to label a population as evil is to render the other ‘sub-human.’ We are told of the ‘Evil doers,’ Axis of evil,’ Osama Bin Laden the evil, America the evil, capitalism the evil, and terrorism the evil, and evil acts ([Davetian, 2001](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22davetian2001)). The ensuing pursuit and eradication of this evil within the context of calls for jihad and a corresponding ‘war on terror’ also implies a ‘promotion of war more willingly than accommodation’ ([Armitage, 2003](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22armitage2003), p.202). However, as is the case with dichotomous logic, good and evil are two sides of the same coin, or mutually sustaining concepts. Thus, to speak of eradicating evil in this context is a nonsensical pursuit. As Baudrillard explains: ‘We believe naively that the progress of the Good, its advance in all fields (the sciences, technology, democracy, human rights), corresponds to a defeat of Evil. No one seems to have understood that Good and Evil advance together, as part of the same movement…Good does not conquer Evil, nor indeed does the reverse happen: they are once both irreducible to each other and inextricably interrelated’ ([2002](http://www.socresonline.org.uk/13/1/17.html#baudrilard2002), p.13). Dichotomous logic can be applied to an examination of security and associated threat discourses. Threats and (in)security 4.14 Stern defines terrorism as ‘an act or threat of violence against non-combatants with the objective of exacting revenge, intimidation, or otherwise influencing an audience’ ([2003](http://www.socresonline.org.uk/13/1/17.html#stern2003), p.xx). One of the aims of this act of violence is to instil fear in the target audience. However, to better understand this notion of terrorism and threat, one also needs to understand the discursive power of claim makers, and those in positions of authority (whether they be political parties, clerics and other elites or the military for that matter) in shaping or co-constituting them so. As Campbell ([1998](http://www.socresonline.org.uk/13/1/17.html#campbell1998)) alludes: ‘[d]anger is not an objective condition. It is not a thing which exists independently of those to whom it may become a threat…nothing is a risk in itself;…it all depends on how one analyses the danger, considers the event’ (pp.1-2). 4.15 To this end, the securitization school of thought developed by the Copenhagen School examines the socially constructed dimension of security threats by looking at the ways in which processes like social interaction form as well as alter interests, and in the process, construct or constitute security. By using an inter-subjective lens to look at security, proponents of this school explore the extent to which power relationships and language as expressed through discourse shape understandings of threatsand subsequent security responses. They argue that by labelling something a security issue or threat, actors invoke the right to use whatever means to stop that threat. Here language is akin to a ‘speech act,’ or in other words, relates to the act of speaking in a way that gets someone else to act ([Hughes, 2004](http://www.socresonline.org.uk/13/1/17.html#hughes2004), p.14). 4.16 Labelling something as a security issue, or some group or community as a threat can therefore be seen as a powerful political tool in terms of the behaviour of governments and other interest groups. Indeed, to label a problem a ‘security’ issue or a ‘threat’ gives this problem a special status, and one which can legitimate extraordinary measures to tackle it. Within the current climate of terrorism, threats to security are often characterised as emanating from Others who view their global neighbours rapaciously and are ready to pounce at first sign of weakness. 4.17 The following discussion examines the relational and socially constructed nature of identity and its relevance to various discursive representations of terrorism through its analysis of polarised collective identities and intractable conflict. Polarised collective identities and conflict 5.1 Protracted conflicts have dominated the international arena and have resulted in much of the violence and terrorism witnessed today. These types of conflict usually centre on deep-rooted issues such as struggles over material, human needs, or an historical grievance. The relationships which feature in these forms of conflict comprise of self-perpetuating spiral of violent interactions in which each party develops a vested interest in the continuation of the conflict. They also characteristically entail ‘polarised perceptions of hostility and enmity’ ([Bercovitch, 2003](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22bercovitch2003)). 5.2 In the case of polarised collective identities and protracted conflict, conflict invariably centres on identity struggles, categorisation, and perceived difference (and related issues concerning values and beliefs). Social and collective identity construction is by nature a source of indirect and direct threat. As Hughes explains: ‘[i]ndirectly, identity construction contains the possibility for identity threat since the adoption and practice of one identity necessarily precludes the fulfilment of another by the same audience’ ([2004](http://www.socresonline.org.uk/13/1/17.html#hughes2004), p.24). 5.3 Direct threats are expressed in terms of an identity’s stance toward the existence and identification of ‘others.’ These stances can occur along a continuum ranging from accepting to eliminating ([Hughes, 2004](http://www.socresonline.org.uk/13/1/17.html#hughes2004), p.24). It is important to note, however that identity contains the potential for, rather than the inevitability of conflict. Nevertheless, an examination of the literature and theories concerning identity, Self-Other differentiation, highlights the extent to which individuals not only display a tendency for assigning people with whom they interact into a class of Self/Other, but also show how individuals treat more favourably other individuals whom they consider Self, than those who they regard as Other. ‘Inclusive fitness’ and social identity theories for example have shown how sharing ‘genetic material,’ or having similar observable characteristics such as looks, religion, ethnicity (markers of ‘in-group’ and ‘out-group’ status) informs behaviour between groups/others ([Ben-ner, McCall, Stephane, and Wang, 2006](http://www.socresonline.org.uk/13/1/17.html#ben-ner2006)). 5.4 The concept collective identity refers to a ‘shared place’ in the social world, or the ‘we’ aspect of identity that develops through a process of self-categorization, identification and social interaction. Moreover, whilst these identities can be chosen freely by individuals, they can also be imposed by others who have the resources and authority to do so (as is the case with labelling Others evil, a threat, or enemies through the discursive practices highlighted above). Collective identities serve many symbolic, practical and normative functions such as fulfilling needs for belonging, distinctiveness, respect, unity and status. They also provide a justification for claims and a focus for the maintenance of a distinctive culture or way of life ([Coleman, 2004](http://www.socresonline.org.uk/13/1/17.html#coleman2004)). Such a position presumes or utilises a sense of ‘we-ness,’ or group homogeneity, which discounts levels of heterogeneity that may exist. 5.5 As stated above, protracted conflicts are rooted in the perceived threat to basic human needs and values, as well as concerns over group dignity, recognition, security and distributive justice. When these aspects of collective identities are denied or threatened in some way, intractable conflict occurs. As the conflict intensifies, antagonistic groups become increasingly polarised through an in-group discourse and out-group hostilities focussed on the negation, defamation and vilification of the out-group ([Druckman, 2001](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22druckman2001); [Fordham and Ogbu, 1984](http://www.socresonline.org.uk/13/1/17.html#fordhamogbu1984); [Hicks, 1999](http://www.socresonline.org.uk/13/1/17.html#hicks1999); [Kelman, 1999](http://www.socresonline.org.uk/13/1/17.html#kelman1999) cited in [Coleman, 2004](http://www.socresonline.org.uk/13/1/17.html#coleman2004)). 5.6 In his review of the literature, Coleman ([2004](http://www.socresonline.org.uk/13/1/17.html#coleman2004)) highlights a series of conditions, processes and structural issues that are conducive to the development and maintenance of polarised collective identities and related conflict. Eight of these conditions include: 1. ‘Situations where there is a pervasive belief in enduring hostilities where the disputants feel locked – into the intensity and oppression of the conflict relationship’ ([Coleman, 2004](http://www.socresonline.org.uk/13/1/17.html#coleman2004), p.11; [Fordham and Ogbu, 1984](http://www.socresonline.org.uk/13/1/17.html#fordhamogbu1984)). 5.7 During his speech to the National Guard in February 2006, President George [Bush](http://www.socresonline.org.uk/13/1/17.html#bush2006) talks of the ongoing nature and progress of the War on Terror: …On September the 11th, 2001, our nation saw that vast oceans and great distances could no longer keep us safe. I made a decision that day -- that America will not wait to be attacked again. (Applause.) And since that day, we've taken decisive action to protect our citizens against new dangers. We're hunting down the terrorists using every element of our national power -- military, intelligence, law enforcement, diplomatic, and financial. We're clarifying the choice facing every nation: In this struggle between freedom and terror, every nation has responsibilities -- and no one can remain neutral… 5.8 Implied within this discourse is the notion that if you are not with us, then you are against us, and thus a potential enemy. The discussion also makes it clear that there is no room for negotiation with, or accommodation to, the enemy. The view that terrorists are also locked into a zero-sum battle has also been reported. R. James Woolsey has been quoted in the National Commission of terrorism as saying, “today’s terrorists don’t want a seat at the table, they want to destroy the table and everyone sitting at it” ([Morgan, 2004](http://www.socresonline.org.uk/13/1/17.html#morgan2004), pp.30-31). 2. The involvement of ‘salient aspects of identity’ (cultural differences) ‘where the in-group and out-group can be easily differentiated’ ([Coleman, 2004](http://www.socresonline.org.uk/13/1/17.html#coleman2004), p.12; [Gurr, 2000](http://www.socresonline.org.uk/13/1/17.html#gurr2000)). 5.9 The representation of the Muslim/Islamic Other with its emphasis on radically different values systems, becomes evident in references to religious motivations for terrorist attacks – religious ideals which are positioned in opposition to more ‘moderate’ Christian values. As argued above, both often use religious justifications as part of their claims making and their respective calls for a ‘Jihad’ on the US and her Allies, and the US led ‘War on Terror.’ Similarly, Esmer ([2002](http://www.socresonline.org.uk/13/1/17.html#esmer2002)) and Norris and Inglehart ([2002](http://www.socresonline.org.uk/13/1/17.html#norrisinglehart2002)) note how hallmarks of Western democracies which are built upon principles of rights (the ‘Land of the Free’), gender equality, sexual liberation pose a threat to traditional values extant in some Islamic cultures. Representations of this kind accentuate perceived cultural differences. In this sense, culture can be viewed as having three components: an empirical aspect (culture understood as communities with their own sets of identifiable, observable, and transferable cultural traits); an analytical aspect (culture used as a conceptual tool) and more significantly a strategic aspect (instrumentalisation of culture/religion to advance identity claims) (LCC, 2001, p.4). 3. ‘Where there exists the perception of negative treatment or threat to an identity group of high centrality and importance’ ([Coleman, 2004](http://www.socresonline.org.uk/13/1/17.html#coleman2004), p.12; [Fordham and Ogbu, 1984](http://www.socresonline.org.uk/13/1/17.html#fordhamogbu1984)). 5.10 There will be in most issues concerning security, a structure of two basic discourses, which articulate radically differing representations of identity (whether they be the humiliated other, the freedom fighting champion, or fanatical terrorist). Many ethnic and religious conflicts that cover the globe are fuelled by stories of humiliation, which in turn, are the basis for stories of revenge. Authors like Hassan ([2004](http://www.socresonline.org.uk/13/1/17.html#hassan2004)), Bendle ([2002](http://www.socresonline.org.uk/13/1/17.html#bendle2002)), Cobb, ([2004](http://www.socresonline.org.uk/13/1/17.html#cobb,2004)) and Davetian ([2001](http://www.socresonline.org.uk/13/1/17.html#davetian2001)) have noted how (suicide) terrorist attacks offer self empowerment in the face of powerlessness, redemption in the face of damnation and honour in the face of humiliation. 5.11 Group boundaries are also often delineated according to symbolic, spatial, religious and social referents, ensuring collective identification within, while simultaneously ensuring the exclusion of outsiders. In this respect, the symbolic attacks on the Pentagon, Twin Towers, and the planned attack on the Whitehouse, represent an attack on the pillars of Western democracy and capitalism, and as such, threats to ‘ways of life’ and identity. 4. ‘High mortality salience where death-related anxieties motivate people to become more deeply committed to their cultural groups as a means of buffering such anxiety’ ([Coleman, 2004](http://www.socresonline.org.uk/13/1/17.html#coleman2004), p.12; [McCauley, 2001](http://www.socresonline.org.uk/13/1/17.html#mccauley2001)). 5.12 Humphrey argues that the impact of September 11th as reported by real time coverage on international television networks, “was seductive in conjuring up the sense that we are living in an era of ubiquitous and even world-ending violence” ([2004](http://www.socresonline.org.uk/13/1/17.html#humphrey2004): 3). The fear of apocalyptic violence posed by WMD was a major justification for pursuing a pre-emptive war against Afghanistan and Iraq. In turn, a ‘death-related anxiety’ was felt by Western nations with the prospect of Weapons of Mass Destruction (WMD) falling into the hands of Osama Bin Laden and Al Qaeda terrorist networks. These fears were not alleviated when George W. Bush for example asserted the ‘terrorist groups’ would use WMD ‘without a hint of conscience’ ([Bullimer 2002](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22bullimer2002)). By linking these two issues (terrorism and WMD) political discourses of this kind reified terrorism and WMD, setting into action a series of actions designed to control their proliferation. 5.13 Structural issues which act to reinforce and maintain polarised collective identities include: 5. ‘A negation of the Other’ ([Coleman, 2004](http://www.socresonline.org.uk/13/1/17.html#coleman2004), p.17). 5.14 This, according to Coleman is the ‘fundamental aspect of the in-group’s identity’ (17). Identity creation through negation entails making a statement of in-group’ identity with reference to what it is not, or does not consist of, for example ‘I am a Christian, not a Muslim.’ Strategies employed in the negation of the Other also include: marginalisation of ethnic and religious groups through naming; racialisation; criminalisation; and stigmatisation. Response strategies of the ‘out-group’ include: collective resistance to ascribed identities; group empowerment; demands for collective group rights (territorial claims) in an attempt to secure greater autonomy, legitimisation and social control ([Rummens, 2001](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22rummens2001), p.18). 6. ‘The outgroup images become negative, homogeneous, abstract and stereotypical’…particularly in regards to the productions of ‘enemy images’ which ‘contain an emotional dimension of strong dislike…these images tend to become self-fulfilling and self-reinforcing, serving important interests and needs’ ([Coleman, 2004](http://www.socresonline.org.uk/13/1/17.html#coleman2004), pp.17-18; [Stein, 1999](http://www.socresonline.org.uk/13/1/17.html#stein1999); [Toscano, 1998](http://www.socresonline.org.uk/13/1/17.html#toscano1998)). 5.15 Implicit within ‘Us/Them,’ ‘East/West,’ ‘Good/Bad’ and ‘Self/Other’ binaries is the notion that opposing identities are relatively homogenous. The use of these non-specific yet all-inclusive tags also serves to dehumanise and depersonalise a highly abstracted Other. In turn, depersonalisation allows social stereotyping, group cohesiveness and collective action to occur. The construction of absolutist discourses of this kind are an important vehicle for understanding conflict: ‘[a]lthough generally described as integrated and homogensous, communities as loci of production, transmission, and evolution of group membership foster conflict through the negotiation and manipulation of social representations’ (LCC, 2001, p.6). 5.16 Here, the demarcation of the common enemy/Other assists with the mobilisation of one group against another ([Aho, 1994](http://www.socresonline.org.uk/13/1/17.html%22%20%5Cl%20%22aho1994)). Identity demarcation of this kind further allows the mobilisation of audiences to carry out conflict. President Bush for example has made many references to ‘evil doers’. He has been quoted as saying ‘we're on the hunt...got the evildoers on the run...we're bringing them to justice’ and ‘they kill without mercy because they hate our freedoms...’ ([Sample, 2006](http://www.socresonline.org.uk/13/1/17.html#sample2006), [The White House, 2001](http://www.socresonline.org.uk/13/1/17.html#the%20white%20house2001)). The emotive language used in ‘speech acts’ of this kind are designed to elicit ‘in-group’ distinctiveness and cohesion through the negation and disparagement of the ‘out-group’ (terrorist organisations). The use of terms ‘evil doers,’ ‘them,’ and ‘they’ are interesting however in the sense that they refer to an enemy that extends beyond the confines of terrorist organisations like Al Qaeda. 7. ‘A clear and simplified depiction of good (us) and evil (them) that serves many functions’ ([Brown and Gaertner, 2001](http://www.socresonline.org.uk/13/1/17.html#browngaertner2001); [Coleman, 2004](http://www.socresonline.org.uk/13/1/17.html#coleman2004), p.18). 5.17 By framing their conflict within a discourse which accentuates a struggle between good and evil, both religious terrorist groups and their Western-led protagonists, view non-members of either camp to be ‘infidels’ or ‘apostates’ ([Cronin, 2003](http://www.socresonline.org.uk/13/1/17.html#cronin2003)) and ‘immoral’ or ‘fanatical’ respectively. The maintenance of such a discourse can be seen as serving a dual purpose; namely, to dehumanise the respective victims on both sides of the conflict, and sustain in-group and out-group identities. 8. ‘In extreme cases, pain and suffering for one’s group and one’s cause come to be considered meritorious’ ([Coleman, 2004](http://www.socresonline.org.uk/13/1/17.html#coleman2004), p.19; [Zartman, 2001](http://www.socresonline.org.uk/13/1/17.html#zartman2001)). 5.18 Martyrdom is a well documented motivation for engaging in terrorist activity. From 1996-1999, Nasra Hassan, a United Nations relief worker in Gaza interviewed 250 aspiring suicide bombers. In one interview, the late spiritual leader of Hamas, Sheikh Yasin, told her that martyrdom was a way of redemption, "[l]ove of martyrdom is something deep inside the heart. But these rewards are not in themselves the goal of the martyr. The only aim is to win Allah's satisfaction. That can be done in the simplest and speediest manner by dying in the cause of Allah. And it is Allah who selects martyrs" ([Hassan, 2004](http://www.socresonline.org.uk/13/1/17.html#hassan2004), p.1). Conclusion 6.1 This paper has explored some of the issues concerned with identity formation, construction and negotiation. In doing so, this paper has focussed on the socially constructed aspects of identity, and in particular, the extent to which social identities are subjectively constructed according to perceived differences in comparison to others. Hansen contends, identity is “always a relational concept, and it is constructed within discourses, not given by the thing itself” ([2004](http://www.socresonline.org.uk/13/1/17.html#hansen2004), p.4). 6.2 Meaning is therefore also relational, for the identification of/with difference between imagined communities like the East and West denotes, or holds meaning. Consequently, identity construction involves a degree of ‘Othering’, and within this context, social identities can be constructed and understood as being more or less threatening and different. Issues of Otherness are central to understanding terrorist activity, and are a feature of security discourses girding the current ‘war on terror.’ To this end, this paper has examined the relationship between power and the formation, emergence, and mobilisation of culturally-based collective identities and their expression through representation, narratives, discourse and language. 6.3 Using a social constructionist and a somewhat postcolonialist inspired analysis, this paper questions the utility of dichotomies like Self/Other, insider/outsider, Us/Them, Good/Evil used within terrorist discourses. The ensuing discursive formation shapes the ways in which terrorism can be meaningfully talked about, understood, and tackled. In the process of defining and establishing difference, the discourse of the Other is also highlighted, since such definitions invariably allude to an object in terms of what it is not. Such a practice entails the social construction of some other person, group, culture or nation as being different and deficient from one’s own. Hence as Simon Dalby ([1997](http://www.socresonline.org.uk/13/1/17.html#dalby1997)) observes, “specifying difference is a linguistic, epistemological and, most importantly, a political act; it constructs a space for the other distanced and inferior from the vantage point of the person specifying the difference” (cited in [Grondin, 2004](http://www.socresonline.org.uk/13/1/17.html#grondin2004), p.5-6). For Said, accentuating difference in this way is central to dichotomous representations of the Self and Other, and through the lens of Orientalism, the creation of a self serving discourse which privileges the world-view of the West. 6.4 When examining issues concerning what is terrorism, who practices it and why, as well as appropriate responses to this activity, this paper contends that such issues are often clouded by a rhetoric (discourse) that has deflected attention away from political and moral concerns underlying political violence. This paper has also argued that utilising dichotomous logic in the construction of an enemy is a counterproductive strategy for grappling with terrorism. The use of binaries like Good/Evil and Us/Them assist with the construction of a dehumanised Other who cannot be reasoned with, thus repudiating calls for negotiation, and in the process, reducing incentives to understand difference. Demonising the enemy in such a manner, amplifies fear and alarm, and perpetuates cycles of revenge and retaliation which necessitate more violent responses to perceived injustices. In this sense, the production and maintenance of a West and Rest dichotomy, a dichotomy which characterises current terrorist and security discourses, has also lead to the creation of mutually sustaining antagonisms ensuring further conflict. 6.5 Consequently, it is important to rethink the binary oppositions employed within the social constructions of other socio-cultural groups, enemies or threats, and national identities. When employed within a national security context, these dichotomies not only serve to reify imagined differences between communities, but also may inflame hostilities through the continuation of oppositional identities and relations which are viewed as being fixed, and thus resistant to change. A way around this binary impasse is the construction of counter-discourses which contain dual positions for both parties as victims and as agents of conflict. As long as both sides represent themselves as being victims, rather than perpetrators of violence, more violence will ensue. Moreover, another way to challenge the legitimacy of dichotomous logic is to create a counter-discourse highlighting the diversity extant within ‘so-called’ homogenous populations.

#### Role of the ballot is to either accept or reject the affs securitization—prior to action

**Saltera 8** (Securitization and desecuritization: a dramaturgical analysis of the Canadian Air Transport Security Authority Mark B Saltera School of Politics, University of Ottawa, Ottawa, Ontario, Canada K1N 6N5. E-mail: msalter@uottawa.ca, , 2008

This model of settings for securitizing moves fits cleanly with Paris School interventions on the trope of risk (Aradau and van Munster 2007; Aradau et al. 2008). However, it is precisely because security plays differently to each audience, is used differently by different speakers, and changes in its meaning that we need to expand our analysis of how securitizing moves are accepted or rejected. Bigo (2006: 7) uses the notion of 'field' to demonstrate how 'these professions do not share the same logics of experience or practice and do not converge neatly into a single function under the rubric of security. Rather, they are both heterogeneous and in competition with each other'. This article offers a way into that field analysis of securitization, that is not reduced to linguistic analysis, through a dramaturgical analysis of setting: within each securitizing move, we must consider who may speak, what may be spoken, and what is heard. Top of page Securitization Securitization theory has been an incredibly fruitful approach for the study of security. Having disaggregated 'state security' into several sectors (military, political, societal, economic, and ecological), Buzan argues that 'the question of when a threat becomes a national security issue depends not just on what type of threat it is, and how much the recipient state perceives it, but also on the intensity with which the threat operates' (1991: 133–4). This was expanded by Buzan, Waever, and de Wilde in the formal model of securitization: 'the intersubjective establishment of an existential threat to have substantial political effects...to break free of procedures or rules he or she would otherwise be bound by...' (1998: 25). The attempt at securitization is called a 'securitizing move', which must be 'accepted' or rejected by the target audience. The authors argue that the conditions for success are (1) the internal grammatical form of the act, (2) 'the social conditions regarding the position of authority for the securitizing actor — that is, the relationship between the speaker and the audience and thereby the likelihood of the audience accepting the claims made in a securitizing attempt, and (3) features of the alleged threats that either facilitate or impede securitization' (1998: 33). There is room within the original cast of the theory to expand the notion of facilitating conditions or impediments for securitizing moves — but little direction as to what those might be. In this reading, the second factor — these social conditions — is under-determined and must be explored further. In the debate between the CS, so named in a response by McSweeney (1996, 1998), subsequent replies (Buzan and Waever, 1997), and a provocative intervention by Williams (2003), a number of critiques of the model of securitization were raised. The CS was faulted by McSweeney for appearing to give an ontological pre-existence to the 'speaker' and 'audience' that is at odds with a more processual or constructivist perspective of identity (1996: 83). Williams argued that different kinds of speech might constitute an act, and made an important theoretical connection to Schmittian politics of sovereign exceptionality. Williams wrote that the CS process of securitization — notably that securitization implies depoliticization — can be found in other theories of sovereign authority, and that securitizing moves are an attempt by the sovereign to decide the exception and thus remove the sector from democratic debate (2003). Buzan, presented a spectrum of how issues might be weighted: 'nonpoliticized... through politicized... or securitized' (1998: 23). Within this account, the CS appears to represent securitization as a threshold — particularly within a democratic society. Either a threat is represented and then accepted as a security issue, or it remains contested within the realm of normal, deliberative politics. Successful securitization is at root a political process, but the actual politics of the acceptance are left radically under-determined by this model. The authors argue that 'the issue is securitized only if and when the audience accepts it as such... (it must) gain enough resonance for a platform to be made from which it is possible to legitimize emergency measures...' (1998: 25). It is precisely the dynamics of this acceptance, this resonance, this politics of consent that must be unpacked further. The Copenhagen School, certainly open their model to consideration of the 'external, contextual, and social roles and authorized speakers' of the speech act 'and, not least, under what conditions (i.e. is the securitization successful)' (1998: 32). But, within their model, there is no frame for how securitizations are successful or fail. A subsidiary point that is worth noting: these external and internal conditions for securitization appear to work in reverse for the process of desecuritization (Wæver 1995). The speaker proposes that there is not a threat, or at least not a threat that is existential, and that the problem can be comprehended or managed within the rubric of normal politics. There are a number of assumptions within articles about securitization theory about the differential ease or difficulty of securitization and desecuritization. These unexplored assumptions arise because there is no theory for the actual process of the success or failure for a securitizing or desecuritizing move. The statist model of securitization does not match the complexity of contemporary social dynamics of security. First, other non-state actors must be included in the model, as demonstrated by Bigo (2006) and others. Security is not contained solely within the traditional boundaries of the state and the authority to make securitizing moves not limited to state actors. Second, two temporal dimensions must be added to considerations of securitization and desecuritization: the duration of the securitization and the entropy of the public imagination. Some issues, such as the war on drugs, rose and faded in the public imagination, largely independent from the 'actual' or empirical degree of threat (Campbell 1993; Aradau 2001). Third, securitization is not an instantaneous or irrevocable act. Rather securitization reflects the complex constitution of social and political communities and may be successful and unsuccessful to different degrees in different settings within the same issue area and across issues. Floyd demonstrates convincingly that desecuritization is entirely 'issue-dependent rather than static' (2007: 349). Nor is securitization an act that removes an issue from deliberative politics forever. Rather, studies of securitization need to account for the movement of issues into and out of the security sector over time. An issue that has faded from the public view may rest within the security frame or enjoy a kind of 'entropy' where the public, elite, technocratic, or scientific communities assume that exceptional security measures have lapsed in the face of a threat that no longer seems pressing or relevant. Hysteria over the presence of communists and homosexuals within government departments no longer seems a national security threat, in the way that McCarthy and others described. For example, a securitization act may be successful with a scientific or technocratic community, and yet fail in the elite and popular realm, such as the debate over global warming during the 1980s and 1990s. A process of desecuritization may occur within popular politics, while elites and professionals remain unconvinced, such as transportation safety. Doty examines how the Minutemen along the US–Mexico border consider themselves to be acting in a 'decisionist' mode, even though they are not sovereign actors (2007: 129–31). A particular group has successfully securitized illegal migration at the border for a segment of the population, while simultaneously human rights groups — by placing water in the desert and advocating for amnesty — act as if the issue is politicized. John McCain (Arizona Senator and Republican Presidential nominee) proposed legislation (with Democratic Senator Edward Kennedy, for whom 'all politics are local') that would provide a 'path to citizenship' and border security — only to withdraw it in the face of public criticism. In this case, the issue was the subject of intense 'normal' political debate, and the securitizing move was incomplete and heterogeneous across the political landscape. The model provided by the CS gives us no way to measure the success or failure of a securitizing move. In this article, I gauge the success or failure of a securitizing move by ranking the degree to which policies, legislation, and opinion accords with the prescriptions of the speech act: 1. To what degree is the issue-area discussed as part of a wider political debate? 2. Is the description of the threat as existential accepted or rejected? 3. Is the solution accepted or rejected? 4. Are new or emergency powers accorded to the securitizing agent? Unfortunately we are unable to provide accessible alternative text for this. If you require assistance to access this image, please contact help@nature.com or the author This scale of success–failure is particularly useful in assessing the persistence of a security issue within different audiences. A more nuanced notion of success and failure also gives us a purchase on whether an issue remains securitized over time so that we may develop a theory of the public imagination in the future. Two recent contributions to securitization theory stand out for my analysis.1 Balzacq and Stritzel share my excitement about the potential of the CS, and my worry about the under-developed social aspect of securitization. Stritzel leads the theoretical debate, and provides a strong grounding for this present article. He argues 'too much weight is put on the semantic side of the speech act articulation at the expense of its social and linguistic relatedness and sequentiality' (2007: 358). He critiques the under-theorization of the speaker–audience relations, stating that 'in empirical studies one cannot always figure out clearly which audience is when and why most relevant, what implications it has if there are several audiences, and when exactly an audience is "persuaded"' (2007: 363). Stritzel proposes an embedded analysis of securitization: '(1) the performative force of the articulated threat texts, (2) their embeddedness in existing discourses, and (3) the positional power of actors who influence the process of defining meaning' (2007: 370). By this, he argues, the discourse of securitization must be understood as situated within a relationship between speaker–audience and within a context that predates the actual securitizing act. What makes a securitizing move successful is, for Stritzel, the extent to which the actor has the power to make the threat and the discursive weight of that threat (has it been well established, or is this a new threat?). Stritzel's general model of embedded securitization is productive, but does not explain the success or failure of securitizing moves with any greater clarity than the CS. It is a useful framework that can guide empirical work, but it does not allow us to generate any hypotheses about the politics of securitization and, in particular, about securitizing moves that fail to garner acceptance or resonance. Adding the range of success/failure, as detailed above, helps Stritzel's embedded analysis disaggregate 'persuasion' into multiple steps of audience acceptance. Balzacq also offers a model of the social aspect of securitization that includes 'the context, the psycho-cultural disposition of the audience, and the power that both the speaker and the listener bring to the interaction' (2005: 172). In posing the question of strategic or pragmatic practice, Balzacq argues that 'the positive outcome of securitization, whether it be strong or weak, lies with the securitizing actor's choice of determining appropriate times within which the recognition, including the integration of "imprinting" object — a threat — by the masses is facilitated' (2005: 182). His examples demonstrate that these choices are constrained by history, memory, and discursive tropes. What a dramaturgical analysis adds is the notion that — just as there are different national and psycho-cultural contexts — so too are there different sociological, political, bureaucratic, and organizational contexts within a populace. A popular audience will 'accept' securitization of threats differently to an elite or scientific audience. Global warming as an environmental securitization, for example, has had creeping success — but on radically different grounds with scientists, bureaucrats, elite politicians, and the populace (both within states and between states). It is unclear to me if 'securitizing agents always strive to convince as broad an audience as possible' (2005: 185), particularly within the context of security professionals (Balzacq 2008). In the case study below, the securitization of Canadian civil aviation security was pitched to narrow, specific audiences — and there was little effort to securitize the issues for the general public. At a base level, popular politics (at least in democratic societies) operates differently than scientific politics; technocratic politics from elite politics. In short, in addition to the 'régime of truth, [a society's] "general politics" of truth' (Foucault 1980: 131), there are also specific politics of truth. Foucault hints at these specific regimes of truth in discussing the relationship between the specific intellectual and 'direct and localised relation[s] to scientific knowledge and institutions' (1980: 128). I return to these notions of direct and localized relations in the case study. This is why a dramaturgical approach to the actual evolution of particular securitizing moves is so productive; the language and political games at stake in each setting are radically different. Balzacq has gone on to argue that 'securitization sometimes occurs and produces social and political consequences without the explicit assent of an audience' (2008: 76). He uses the new governance literature to propose a new investigation into policy tools that are 'instruments of securitization' (2008: 79). Both Balzacq's work and this article are attempting to remedy the same flaw in the CS's methodology: an overreliance on speech acts to the neglect of the social. A dramaturgical analysis of setting, however, provides the audience that Balzacq displaces. It is crucial to our analysis that the audience is determinative of the form of securitizing move. Even if those audiences are internal or organizational, as Goffman explains: 'no audience, no performance' (1974: 125). He argues, "if one individual attempts to direct the activity of others by means of example, enlightenment, persuasion, exchange, manipulation, authority, threat, punishment, or coercion, it will be necessary, regardless his power position, to convey effectively what he wants done, what he is prepared to do to get it done and what he will do if it is not done. Power of any kind must be clothed in effective means of displaying it, and will have different effects depending upon how it is dramatized. (1959: 241, emphasis added)" Viewing securitizing moves as a kind of performance, we can see the importance of 'front' and 'backstage': that the same securitizing speech acts may be framed differently within the professional team and in front of an audience. Among themselves, (security) agents may speak in one way, but use other ways to conform to the expectations of a popular audience — and there are some that are always totally excluded from the securitizing process (1959: 145). The audience is not always the public. There is a network of bureaucrats, consultants, parliamentarians, or officials that must be convinced that securitization is appropriate, efficient, useful, or effective. Balzacq identifies a series of backstage securitizing moves that have public effects, though are never securitized publicly. Rather than disappear the audience, a more flexible notion of the setting of securitization allows for micro-sociologies of the particular securitizing moves. Top of page Dramaturgical Analysis Dramaturgical analysis uses the vocabulary of the theatre to understand social settings, roles, and performances of identity. Sociologist Goffman also introduced the notion of the 'framing' of identities and issues, to which much critical scholarship is indebted (1974).2 Much post-structuralist work relies on notions of performance, and critical work in international relations often assumes that key political divisions such as inside/outside, order/anarchy, self/other must be continually performed and reinforced to have effect. In this research programme, I am interested less in the national application of Butler's notion of the performativity of gendered and other identities (1990), Campbell's (1993) notion of foreign policy as an articulation of danger that acts as an identity function, Sylvester's analysis of 'dramaturgies of violence' (2003a) or 'development' (2003b), important and provocative though they may be. Instead, this dramaturgical theory argues that the setting of a securitizing move is determined by the actors and their roles, the rules of the discourse permissible within that space, and the expectations of the audience. When we push this theatrical metaphor, we can classify the different types of securitizing moves that all share similar conventions, narratives, characters, and tropes. The use of specialized language, procedural forms, and common conventions all suggest a common setting.3 For example, terms, precedents, or issues whose specialized meanings both speaker and audience share.4 Buzan et al. themselves use dramatic language: 'the staging of existential issues in politics to lift them above politics...an issue is dramatized and presented as an issue of supreme priority...' (1998: 26). Huysmans alludes to the 'security drama' and leads to this focus on 'the processes of security' (1995: 66). Rather than classify securitizing moves as comedies, tragedies, and histories, we can classify them according to the setting: popular, elite, technocratic, and scientific settings. Each of these settings structures the speaker–audience relationship of knowledge and authority, the weight of social context, and the success of the securitizing move. The setting of a securitizing act includes the stage on which it is made, the genre in which it is made, the audience to which it is pitched, and the reception of the audience. What is particularly useful about Goffman's dramaturgical analysis is precisely the mutual constitution of self and audience. The characters in the drama must use information to convince the audience of a particular story: 'the over-communication of some facts and the under-communication of others... a basic problem for many performances, then, is that of information control' (1959: 141). The setting of a performance, then, communicates the ground-rules for who may speak, what may be said, and what is heard. For example, when Shakespeare was originally staged, groundlings, who paid little admission and sat in the stalls below the stage, might speak to and throw food at the actors — something probably frowned upon at Stratford-upon-Avon today. British pantomime has a particularly interactive audience–actor relationship (oh no it doesn't, oh yes it does), as does the Rocky Horror Picture Show, both of which rely on the audience knowing the call-and-answer structure of the drama. This is to say that in addition to an awareness of the language, tropes, metaphor, plots, and devices that are embedded in the process of securitization, dramaturgical analysis also directs our attention to the constitution of the actor–audience in a particular discursive relationship. Also, Goffman argues that the presentation of the self changes from different social settings, and that an understanding of the setting can illuminate the exigencies of different performances. For him, the character and audience join together in a 'working consensus' to create 'the belief that ([he performer] is related to [the audience] in a more ideal way than is always the case' (1959: 48). Any social scene, such as the setting of securitizing moves, involves the presentation of a self, the setting for that narrative, and audience reception. Speech-act models of securitizing miss the crucial aspect of the 'setting' of the narrative. In particular, the setting of a political speech act includes the stage upon which the securitization is attempted (national, organizational, bureaucratic, or scientific) and also the past narrative history of failed and successful securitizations by lauded or derided characters (Merelman 1969: 225).5 Securitizing moves in popular, elite, technocratic, and scientific settings are markedly different — they operate according to different constitutions of actor and audience. A securitizing move is not the same in all contexts, because it is not simply made up of the internal grammatical elements. Krebs and Jackson analyse the importance of public rhetoric, while bracketing the questions of motivation (2007: 41). Whether the intention of the speaker is entirely calculative or emotive, the rules of the setting remain the same (Goffman 1959: 66). A securitizing move made for political gain or from fear adheres to the same logic, but the effect of the message may be different. This focus on the reflexive relationship between speaker and audience is particularly important for theories of securitization. Securitizing moves follow an internal grammar that is determined not simply by internal rules (i.e. the invocation of an emergency or exception to normal politics), but also to a common, social grammar (i.e. the universe of tropes, images, metaphors, histories that can be invoked). Securitizing moves occur within the universe of the audience imagination. It is not simply a power relationship — but a knowledge-authority game. A popular securitizing move may be prompted by an informal authority such as a civil society group (like the Minutemen along the US–Mexico border); but, civil society groups may be ineffective in scientific settings (Minutemen and similar groups do not participate in academic or professional arguments about border security). A scientist will use different authority to convince her colleagues than her bureaucratic counterparts. For example, the case for the presence of weapons of mass destruction in the lead-up to the most recent American invasion of Iraq illustrates how ambiguity was leeched from the technocratic discourse as it was marshalled in the popular sphere. Uncertainty was purged as the reports were summarized, as technocrats aimed to convince the political elite, and in turn as the elite aimed to convince the general populace. In short, the 'acceptance' of the audience and the 'resonance' of an existential threat is different within different spheres. I argue that we can distinguish these distinct settings by the grand narratives by which truth is authorized, the characters who are empowered to speak, and the relationships between characters and audience. Within the security sphere, different narratives are deployed for security threats in different sectors; different characters may attempt a securitizing speech act; and the relationship between the audience and the performer structure how those speech acts are made and received. This model of different settings for securitization stems from research into the widening of public security in post-9/11 politics. There is a consensus among critical scholars that the amount of social life that is governed by 'security' claims has increased since 9/11 — but not all securitizing moves have been successful. In studying the evolution of civil aviation security, it was clear that the rules of the speech act were different in different settings: who could speak, who could hear, and what could be said all varied radically — even on the same issue within the same sector. Using the case of the CATSA below, I argue that there are four key settings for these securitizing moves. This is not to say that, in other contexts, more settings are not possible, but rather that the four settings are the fewest number of categories that allow for significant differentiation within this case. The changing nature of perceptions of the aviation sector over the past 40 years demonstrates the importance of time and entropy within securitization studies. The gradual and increasing securitization of international aviation has been a long process, one in which terrorist groups rather than government elites have been the organizational and discursive entrepreneurs. The travelling public has a short memory, politicians aim at the next election cycle, and bureaucrats are risk averse. Securitization has occurred at once or necessarily as a result of one speech act that is accepted or rejected but often through the imposition of new regulations or international standards. The setting of securitization is clearly crucial. The success of a securitization act is dependent not exclusively on the formal syntax or on the informal social context, but also on the particular history, dominant narrative, constitutive characters, and the structure of the setting itself. A popular appeal to national security is often effective in popular and elite politics, but may be less convincing in a scientific realm. The restrictions of mandate and bureaucratic thinking will predominate in technocratic politics in (at least potentially) different ways to the decision making of elites bent on maintaining power or gaining reelection. The setting also determines the characters that may attempt a securitizing speech act. Imams and ministers have an authority to name cultural and moral threats to society within the setting of popular politics, but there is a different stage presence about scientific truths. For example, American librarians had a surprise entry onto the popular scene due to their perceived scientific interest in privacy and free speech, which trumped elite policy demands in the realm of popular politics during the debate surrounding the total information awareness proposal (Abdolian and Takooshian 2003; Monahan 2006). The disproportionate effect of librarians in this public debate cannot be explained simply by power differentials as in Stritzel or Balzacq. Different actors possess different authorizations to speak in different political settings. In the following case, the same securitizing move (to expand aviation security and airport passenger security) was made by different actors, to different audiences, with different claims to authority, in different languages, with different effects. This was evident over time as the securitizing move was accepted or rejected by the target audience. Top of page Securitization and CATSA CATSA provides an excellent case for dramaturgical analysis.6 There is a clear and accepted securitizing move in response to the attacks of 9/11: the creation of CATSA. Because the 9/11 attacks were directly connected to failures in airport security, specifically passenger screening, the securitization of civil aviation was relatively straightforward: the external threat of terrorists using planes as weapons of mass destruction had a deep resonance across the populace, political elite, technocrat, and scientific audiences.7 In particular, the real-time broadcast of the second plane hitting the World Trade center, and the repetition of those images, gave aviation security a dominant position in the public imagination of homeland security. Previous to 9/11, in Canada (and the United States) aviation passenger screening was done by airlines according to national standards set by the transportation authority. Airport security was not a realm of emergency or crisis, and could be handled by non-state entities (like airlines or airport authorities). It was depoliticized, expressed in terms of cost and regulations and technical standards. To nationalize airport security — make it part of the governmental structure, through CATSA — represented an expansion of governmental powers that was due to a perceived emergency and existential threat.8 The securitizing move was successful, even easy. However, this does not tell us enough about the process of securitization. During 2004–2007, there were several other securitizing and desecuritizing moves. There are clear popular, elite, technocratic, and scientific communities that engaged in these (de)securitization processes. Popular sentiment can be evaluated through public media, particularly in 2006. Furthermore, in 2004, CATSA engaged the scientific community in an examination of its security strategy, the proceedings of which were then published in 2006. Elite, technocratic, and scientific settings are evidenced through a 5-year governmental review of the CATSA Act in 2005–2007 and an Auditor-General Special Examination of CATSA in 2006. In these reviews, experts, bureaucrats, and policy-makers evaluated the security function of CATSA. In particular, the CATSA Act Review, conducted by Transport Canada with a wide range of public consultations, provides a thick slice of public, scientific, technocratic, and elite opinion after 5 years of operation. During these two critical reviews, the CATSA executive attempted to convince the elite of the need for an expansion of their mandate. In other words, a further securitization of airport security was called for. This was rejected by the technocrats, experts, and the elite. The CATSA case thus provides us with a clear sector that is successfully securitized, popular and expert challenges to that securitization, and a rejection of an expansive securitizing move. There is thus a prima facie case for a successful securitization move in the area of aviation security in Canada. Before 9/11, passenger screening was done by airports and airlines according to standards set by Transport Canada. Despite Vancouver-based attacks on Air India in 1985, there had been a general trend towards the depoliticization of airport security. It was a subject accessible to public debate, but not politically salient (referenced in political campaigns or in parliamentary debates). Transport Canada was the owner/operator of the majority of airports, and consequently was responsible for passenger screening. Airport policing, which had been the responsibility of the federal police force (RCMP), was conducted by regional forces. Following the 9/11 attacks, Finance Minister Paul Martin submitted a budget that included the creation of the CATSA. The CATSA Act received royal assent on 27 March, 2002, as a new crown corporation responsible for 'effective, efficient and consistent screening of persons accessing aircraft or restricted areas through screening points, the screening of the property in their possession or control, and the screening of the belongings or baggage they give to the air carrier for transport' (CATSA Act Review 2006: 13).9 On 31 December 2002, CATSA undertook responsibility for all passenger screening. The creation of CATSA and its initial responsibilities was supported by the Minister of Transport and Finance Minister Paul Martin, who shortly thereafter became the Prime Minister and issued Canada's first National Security Strategy. There was a clear case for securitization: the threat of terrorism particularly to civil aviation was acute, the previous system of privatized or deregulated screening might lead to inconsistencies among Canadian airports which fundamentally threatened the integrity of the system, and, finally, running counter to the trend towards deregulation in civil aviation, the government had a security role. This opinion was exemplified in the National Security Strategy (Canada. Office of the Auditor General 2006: 36). In the following sections, this article parses the four settings of securitizing moves in the civil aviation security sector during 2004–2007. The traditional CS explanation would go this way: the Canadian state made a securitizing move to define the terror threat to civil aviation as an existential threat that required extraordinary action; this move was accepted by the public, and CATSA was formed in 2001–2002 with new powers and authorities (in evidence through the changes to the Aeronautics Act). The Canadian state has not attempted any significant securitizing moves since the formation of CATSA. However, a close reading of the evolution of CATSA, and, in particular, the reviews in 2005–2006, demonstrates a much more complex picture of securitizing moves and counter-moves. Within the elite setting, political and bureaucratic actors actively debated the roles and responsibilities of CATSA and attempted to increase or decrease the powers and authorities of the organization. Within the popular scene, CATSA became the subject of a number of journalistic and public government reports by a Senate committee that questioned the nature of the threat to aviation security and the appropriate policy responses. Within the scientific setting, academics and experts attempted to desecuritize the work of CATSA through a critical appraisal of the risk management approach. Within a technocratic setting, the ability of CATSA to provide and measure security was radically questioned by the Auditor-General, leading to a desecuritizing move. Running throughout all of these settings, there is a common thread: the CATSA executive wanted to increase its mandate, including more counter-terror operations in its operational purview. This particular securitizing move followed the same pattern: existential threat and new powers needed. However, this same securitizing move was made in different ways in different settings. Elite The CATSA Act Review provides a productive snapshot of the securitizing moves in play between 2005 and 2006. The Minister of Transport, later Transport, Infrastructure and Communities, appointed an expert advisory panel in November 2005 to report on CATSA after 5 years of operation, which was tabled in Parliament on 12 December 2006.10 The Advisory Panel had a wide remit to 'examine the provisions and operations of the CATSA Act to ensure that the legislation provides a sound and adequate statutory basis for CATSA's aviation security mandate, provide advice on future aviation security requirements and other developments that may impact on CATSA's future operations...on other important issues that come to [the Panel's] attention' (CATSA Act Review 2006: 15). In the preparation of their report, the panel conducted a number of public consultations and received submissions from over 40 agencies, institutions, airports, organizations, and individuals. CATSA itself also prepared a number of position papers. This is a complex situation for the study of securitization: the three experts on the advisory panel are the primary authors of the report; they are guided and supported by a bureaucracy from Transport Canada; the final audience is the Minister of Transport. Because the audience of this legislative review was the Minister of Transport, Communities and Infrastructure (and other political decision-makers), I analyze this process as part of the elite process. The Auditor-General's Special Examination, though it occurred in a similar timeframe and with consequences for CATSA's Board, was conducted with reference to the Office of the Auditor-General which has a defined mandate. Thus, I examine the Special Examination below as part of the technocratic audience. It was clear that the mandate of CATSA was in contention. There was a potential within the social space for a securitizing move. The Panel notes: 'it is apparent to the Panel and to many stakeholders that clarification is needed concerning the operation mandate of CATSA and Transport Canada... CATSA thinks it should determine the "hows" [of security functions], while Transport Canada insists they are to be determined within the [Security Screening Order]' (CATSA Act Review 2006: 146). CATSA argued in their submissions that Transport Canada's Security Screening Order was extremely detailed in its prescription, and made security screening inflexible. CATSA made a clear securitizing move: a threat, which was existential, that required extraordinary action — in this case the expansion of its mandate and the transformation of an aviation screening corporation into a counter-terrorism agency (CATSA 2006a: 4). In particular, it was argued before the Advisory Panel that the CATSA Act, Canadian Aviation Security Regulations, and the security screening order, gave CATSA an extremely clear, but restricted mandate in its passenger screening. CATSA screeners were responsible for and authorized to detect and to interdict prohibited items only, or to validate the identity of some non-passengers entering into secure air-side operations. In other words, CATSA could not use any profiling, risk-management, or policing methods in their security screening. CATSA argued that its ability to use these tools — such as behavioural profiling or risk management — would make the civil aviation security system much more secure. CATSA sought increased access to intelligence, a greater flexibility in screening-point staffing, and screening procedures. These moves were rejected by the expert panel and the Minister in the CATSA Act Review.11 In 'Our vision for aviation security', submitted to the Review, CATSA makes its case for an expanded mandate. CATSA can provide 'a national approach and consistency', 'public security', 'accountability', 'access to intelligence', and 'international networks' (CATSA 2006b: 5–6). The desire for national consistency among Canadian airports was one of the chief reasons for the creation of CATSA. The form of the organization balances accountability across a Board of Directors, the Minister for Transport, Infrastructure and Communities, and the Treasury Board (which approve, among other aspects, CATSA's budget and corporate plans). However, these other three priorities (public security, access to intelligence, and international networks) represent an expansion of its mandate. Airports, in their submissions to the CATSA Act Review, argue that screening can be handled efficiently and effectively by their own private security staff — essentially a desecuritizing move (Aéroports de Montréal 2006; Canadian Airports Council 2006). They argue that security screening is not an existential threat and does not require additional powers or authorities. Aéroports de Montreal concludes: 'ADM strongly opposes any expansion of CATSA's mandate to encompass, for example, access control or policing functions, since this could be a further infringement of airports' control over their operations. Furthermore, the Minister should not be able to grant CATSA new responsibilities without consulting the airports' (2006: 3). The Canadian Airports Council writes: 'With the exception possibly of cargo security, airports are not in favour of an expanded mandate for CATSA, and airports should be consulted thoroughly before any expansion to CATSA's mandate takes place. Some airports have expressed an interest in taking over or sharing some of CATSA's functions at airports' (2006: 1). Against the argument that airports might be able to provide security screening, CATSA argues 'public security is the #1 priority — CATSA's legislated mandate is air transport security — period. We are not in the business of operating parking, leasing space to businesses, airport cleaning and maintenance, or other areas of interest to airport authorities. Public security is compromised when screening operations are "cross-collateralized" with other airport operations' (5). Within this complex discursive environment, securitization/desecuritization is not simply a binary (on/off) condition but more processual. An examination of the submissions to the Advisory Panel illustrates who 'counts' as a stakeholder for the process, who counts as expert, whose voice is heard. While CATSA, the Advisory Panel, and the Review Secretariat clearly had primary speaking roles (with stakeholders in supporting roles) in this particular securitization drama, the important audience was the Minister. This is a failed securitizing move: CATSA attempted to expand their mandate, to widen their security footprint, to convince the political elite that, due to the terror threat, more powers should accrue to the security service. CATSA publications emphasize the threat of terror, memorialize past attacks, and have instituted a training programme on terror for senior staff (David 2006). The attempt by CATSA to expand their mandate and securitize other areas of airport security was rejected by both the expert panel and the political elite. Both elite and experts were convinced of the threat, but none were convinced that special or expanded powers were needed. The Minister argued specifically that 'Responsibility for aviation security will continue to rest with the Minister of Transport, Infrastructure and Communities... CATSA's activities will be focused on its core aviation security-screening role: the effective and efficient screening of persons who access aircraft or restricted areas through screening points, the property in their possession or control, and the belongings or baggage that they give to an air carrier for transport' (Cannon 2007). Experts and elites argued that the public–private system, structured by rules from Transport Canada, could secure the system. In other words, the existential threat was accepted by the audiences, but not an expansion of powers. Consequently, the securitizing move was not accepted by the key audiences, the Advisory Panel and the Minister. Popular Within popular politics, the securitization of airport screening was easy to accomplish, particularly in countries that had 'focusing events' such as 9/11 (Birkland 1997, 2004). As Lyon observes, 'apart from short-term responses to some notorious hijackings over the past 30 years, airport security was never a topic that engaged the public imagination in Canada (or elsewhere for that matter)' (2006: 398). In 1985, the attack on Air India flight originated in Canada. Investigations determined that it was a result of weak baggage screening and the lack of reconciliation between passengers and luggage. However, passenger screening was not seen as such an important issue — the majority of hijacking or terror attacks occurred in the United States, particularly with reference to Cuba, or in Europe and the Middle East.12 In January 2003, the Standing Senate Committee on National Security and Defence tabled a report in Parliament titled The Myth of Security at Canada's Airports that called for a reinstatement of the RCMP presence and a wide-ranging overhaul of the system. Despite frequent interviews in the popular press by its author, this report did not resonate with the public, the policy, or the political audiences: it represents another failed securitizing move.13 However, the success of the securitization of aviation security can be seen in the popular reaction to two cases of investigative journalism. First, a journalist from the French-language paper Journal de Montréal infiltrated the secure, air-side areas at Trudeau airport in Montreal on a number of occasions through different access points. The journalist entered a catering company's facilities (Cara Foods) and gained access to restricted areas through a disused hanger. The reporter 'found a place to slip under the airport's perimeter fence, but there's no need to get your knees dirty: he also just walked in, repeatedly, as if he belonged. In prohibited zones he gained easy access to the outside of aircraft, to carts full of meals about to be loaded onto planes, and to a truck used to provide water to aircraft' (Gazette 2006). Though none of the checkpoints he passed were staffed by CATSA employees, or indeed the actual regulatory responsibility of CATSA, it was CATSA that was held publicly responsible. While CATSA has responsibility for key elements of aviation security, such as passenger and non-passenger screening at identified checkpoints, it is not responsible for overall perimeter security or security of air-side services. An editorial opined: 'Transport Minister Lawrence Cannon and CATSA chief Maurice Baril have got some explaining to do. Security can't be perfect, but it should surely be better than this'. Minister Cannon summoned Maurice Baril (who was CATSA's Chairman of the Board of Directors, who subsequently resigned) and CATSA President and CEO Jacques Duchesneau to Ottawa 'for further discussions' (Cannon 2006). In Canada, the responsibility for airport security, and the maintenance of air-side security, is shared among a number of different players in the airport and coordinated by Transport Canada through the Aviation Security Regulations. Thus, CATSA is responsible only for its six stated tasks, mandated in the CATSA Act. However, the popular response was that CATSA should be responsible for all of airport security — that all aspects of airport security were the responsibility of the government, because of the existential threat, because of the need for emergency powers. The (inappropriate) critique of CATSA — for, in essence, having a restricted mandate — is a clear demonstration that the public expected that CATSA would be responsible for all airport security (perhaps because of its much larger American counterpart the Transportation Security Administration or a 'misleading' corporate identity). For securitization theory, this implies that the audience, in this case the popular audience, may not simply accept securitization but also initiate an expansion of government powers. The second popular case that demonstrates how the wider public may not simply support, but widen securitization, is the 'revelation' by a Canadian television news programme that CATSA itself had security problems. CBC's investigative journalism programme, The Fifth Estate, broadcast 'Fasten Your Seatbelt' on 5 November 2005 (CBC 2005). A whistle-blower argued that 'customer service' was prioritized over security in passenger screening, and then a security expert, Steve Elson, demonstrated how to circumvent screening points (CBC 2006). The 'security expert' was described as being a former TSA inspector who currently consults on security matters (validating his expertise in both government and liberal economic terms). Once again, a complex web of regulations and responsibilities was simplified (and misconstrued). The whistle-blower was a CATSA employee, and the programme highlighted the role of CATSA in passenger screening and the random nature of non-passenger screening. Within the programme, there was little discussion of the role of the actual regulator and ministry responsible for aviation security: Transport Canada. However, in an unaired portion of the interview with Senator Colin Kenny, one of the authors of The Myth of Security at Canada's Airports said, 'The problem is with Transport Canada. They set the regulations, CATSA simply follows them' (CBC n.d.). CATSA has specifically mentioned their attention to public pressure (Auditor-General 2006), and continuously measures passenger satisfaction rates. Within the popular realm, journalists and government representatives had the roles as experts to 'speak authoritatively'. In these cases, CATSA representatives — who were experts on the legislated mandate of CATSA — were unable to convince the populace through press releases, interviews, etc. that CATSA was not responsible for the security breeches. The socio-political context of Canada also determined 'what might be said'. In particular, the extremely complex interplay of authorities and responsibilities at the airport was radically simplified: CATSA was represented as being solely responsible for aviation security. Any failures of airport security, by themselves or their subcontractors, were laid at the feet of CATSA — as demonstrated by the Minister of Transport calling the President of CATSA back to Ottawa immediately after the Montreal incidents. The success of the securitization of aviation security within this realm is clear in the public criticism of CATSA for not using enough emergency measures to contain this existential threat. The travelling public, which is frequently surveyed by CATSA about its customer service, plays a large role in CATSA's internal discussions, but a smaller role in its discussions with external agencies. These conclusions demonstrate why more nuance is needed in current models of securitization. More is going on than a simple politics of blame or bureaucratic infighting, although plainly some of those dynamics are in play. Rather, CATSA was being responsibilized for all of aviation security in Canada, despite its limited mandate. The popular pressure, I argue, is a representation of the 'facilitating conditions' in the popular imagination: the public was open to securitizing moves by the government. There is also the restriction of 'what might be said': in short, an over-simplification of complex regulatory systems and a misrepresentation of the level of attainable security. No system is completely secure — a fact that is often and easily acknowledged among experts in aviation security. But, this was not portrayed in the popular scene. Investigative journalists, in this case, had the position to speak authoritatively in a way that a Senator and other security experts did not. The public could only express their satisfaction with CATSA's screening as a customer service to CATSA, or in the popular media as a policing and counter-terrorism agency. The failure of the expansion of the security mandate of CATSA in the elite realm and the simultaneous popular critique of CATSA's mandate indicate that the setting matters. Scientific In addition to a set of technical debates, CATSA is also engaged with the scientific community on how to effectively and efficiently screen passengers. I want to focus on the primary adoption of the risk management model, since this has been examined in the Auditor-General's Special Examination and CATSA Act Review process. CATSA was responsible for the purchase and implementation of a wide-scale technological upgrade to explosive detection systems, to meet Canadian and international standards. It has also won awards for its technological innovation for the RAIC programme that uses biometric identification.14 There is also a robust debate in expert circles regarding the use of private firms for security screening, whether airport security can be left to the private sector or should be provided by the government (Frederickson and Laporte 2002; Hainmüller and Lemnitzer 2003; Seidenstat 2004).15 CATSA is mandated to secure key elements of the civil aviation infrastructure through passenger screening. CATSA, however, provides screening according to the 'Security Screening Order', under the Aeronautics Act and the Canadian Aviation Security Regulations. As a crown corporation, CATSA is also bound by government policy to implement a 'risk management strategy', the key elements of which are the evaluation of potential impact and frequency of exposures to different risks. It then formulates a strategy that accepts, avoids, transfers, or mitigates that risk. Within this framework, 'It is government policy to identify, and reduce or eliminate risks to its property, interests and employees, to minimize and contain the costs and consequences in the event of harmful or damaging incidents arising from those risks, and to provide for adequate and timely compensation, restoration and recovery' (Canada. Treasury Board of Canada 2001). CATSA actively engaged the academic and expert communities in formulating its risk management strategy (Brodeur 2006),16 and its proposed Security Management Systems approach (Salter 2007). The CATSA executive asked for training in risk management and, in 2005, the International Centre for Comparative Criminology organized two seminars (in Paris and in Montréal) on risk management. The academic experts at these workshops represented the fields of surveillance studies, criminology, sociology, public health, environmental studies, and risk management itself. The core issues for the experts were the following: 'uncertainty theoretically supersedes risk and rule-based and risk-based models are not mutually exclusive in the promotion of security. Not only can they be reconciled in practice, but they must' (Brodeur 2006: 324). This poses two problems for CATSA, which later became evident in the CATSA Act Review and the Auditor-General's Special Examination: uncertainty within the public security fields makes measurement impossible; following security regulations alone would be insufficient to demonstrate risk management. Among the social scientists represented at the Montréal seminar, there was a consensus that the tactic of risk management, used often in environmental planning and other scientific realms, cannot be easily transferred to the social realm (Zedner 2006: 424). Ericson, an internationally renowned criminologist who pioneered the critical study of risk management, argued, 'risk management systems can restrict freedom, invade privacy, discriminate, and exclude populations. Such self-defeating costs and the uncertainties they entail can be minimized only by infusing risk management systems with value questions about human rights, well-being, prosperity, and solidarity' (2006: 346). These experts questioned not only the empirical reliability of risk management (Manning 2006: 457), but also the ideological function of screening by risk (O'Malley 2006: 420). These experts agreed that the move to a risk-based model of airport screening would require more specific intelligence and the widening of CATSA's mandate. But, they also stressed that because of the radical incalculability of the threat of terror, risk-based security screening had to be combined with rules-based screening. Since risk management could not prevent terror, and may cause potential problems, the problem of airport security had to be made explicitly political. Within these seminars, the setting was academic: experts were selected because of their scholarly credentials and the discourse was in an academic mode.17 At root, the experts attempted a desecuritizing move: since uncertainty trumps risk, the lack of metrics makes measurement (and thus management of risk) impossible. Thus, the security screening process must be political. Since a risk-based approach cannot guarantee security, and the risk- and rule-based systems were in some conflict, CATSA (and by implication Transport Canada, the regulator) must deal with these uncertainties and risks, sensitive to the politics of the situation. Screening procedures could not be an emergency, existential threat that required extraordinary powers or policies. Because security was unobtainable, the process had to remain steadfastly political. Though there was a consensus among the scientific field, this desecuritizing move failed — none of the other audiences were convinced, as demonstrated below in the review of the technocratic setting. Technocratic While the CATSA Act Review had the political elite as its audience, the Auditor-General's Special Examination had only the Office of the Auditor-General as its audience. It was also presented to the CATSA Board of Directors, with clear implications for the Minister — but the authors of the report were a team of auditors not politicians. A Special Examination of CATSA was undertaken by the Auditor-General of Canada during November 2005–June 2006 (a similar time period to the CATSA Act Review process). The Auditor-General appraised the extent to which CATSA was fulfilling and measuring its mandate, as well as other financial and management standards.18 It is beyond the mandate of the Auditor-General's Special Examination to analyse the mandate of the organization (Canada. Office of the Auditor General 2006: 9). CATSA tried to use the Special Examination as another venue to expand its mandate, which, as I argue above, is a securitizing move — accruing more governmental power to manage an existential threat. Just as CATSA attempted this with respect to the elite audience of the CATSA Act Review, they also attempted this in the technocratic setting. As the report concludes: 'CATSA does not wish to be constrained by its limited mandate. CATSA would like to have more control over the way screening operations are conducted, the allocation of screening staff, and the selection of screening equipment; and it would like direct access to intelligence information' (3). The case for the expansion of CATSA's mandate is made in terms of security, emergency, and extraordinary powers: it satisfies the internal criteria for a securitizing move. Here is the key moment: 'CATSA's view is that counterterrorism is a key aspect of its work. This is evident in CATSA documents. Transport Canada has stated that CATSA's current mandated responsibilities do not specifically include counter-terrorism' (14). The CATSA Act Review Advisory Panel also notes this troubled relationship: 'there appears to be a high level of frustration and mistrust between Transport Canada and CATSA at the national level' (CATSA Act Review 2006: 137). The Auditor-General's report is relatively neutral in this bureaucratic in-fighting but that neutrality stands as a rejection of the securitizing move. In short, the securitizing move fails because it does not accept 'security' as a legitimate justification for reevaluating the mandate of CATSA: 'This Special Examination did not question CATSA's mandate; rather it assessed CATSA's systems and practices within its mandate and the regulations that govern the aviation security system' (9). Despite the best efforts of CATSA to make the mandate part of the audit, in order to use the report as a tool in their securitizing move, the Auditor-General did not accept the move. Within the Auditor-General's review, who may speak and what may be said is radically different. CATSA officials prepared reports for the Auditor-General's team who also consulted with an expert team.19 The terms of reference for the report, however, were specific to the crown corporation model and its relevant legislation regarding financial administration. Essentially, security was not the object of study: however, risk management was under scrutiny. Thus, while similar messages were made by CATSA and Transport Canada, they were expressed in different, more managerial language. The audience for this report was primarily the Board of Directors, and indirectly the responsible Minister, Treasury Board Secretariat, and the Parliament of Canada to which the Auditor-General reports. However, the review results were also marshalled in the CATSA Act Review process, in order to bolster the case for a refusal of the securitizing move to increase CATSA's mandate. Thus, the same securitizing/desecuritizing moves are played out, but in a totally different register within different sectors. Settings for Canadian Aviation Security This dramaturgical analysis of CATSA during the crucial 2005–2006 period has demonstrated the need for an analytical disaggregation of the actor–audience model in securitization theory. Within different settings (popular, elite, scientific, and technocratic), different actors were empowered to speak, and different audiences constituted — the rules of those discursive relationships were also impacted by setting. Stakeholders from the CATSA Act Review had no voice in the experts' academic workshop; reports on the measurement of security for the Advisory Panel were not used in the Auditor-General's Special Examination. These different settings also defined the content of securitizing moves: though there was a common desire to expand CATSA's security mandate, it was done with different arguments in the expert workshop, the Special Examination, and the CATSA Act Review. Finally, the CATSA case demonstrates the need to parse the success/failure of securitizing moves in a more nuanced way. CATSA's securitizing move was premised on the acceptance of an existential threat (which is commonly believed), the description of a crisis or emergency (accepted by some and rejected by others), and the accrual of new executive power (which was completely rejected). Top of page Conclusion The CS model of securitization is provocative and productive of many political and research agendas. Making the model more sensitive to who may speak, who can hear, and what can be said within particular settings allows us to evaluate the politics of successful moves to securitize or desecuritize an issue. This kind of analysis necessarily involves an examination of a particular setting over time, a factor often downplayed in CS analysis. Sector studies in public safety, security studies, migration, trafficking, minority rights, and disease can all benefit from a clearer consideration of audience–speaker co-constitution of authority and knowledge, the weight of social context, and the degree of success of particular moves. Desecuritization is seen a priori as more politically preferable than securitization (Wæver 1999: 335). Deliberative politics are by definition more democratic than exceptional politics. This has led to the important debate led by Aradau (2001, 2004, 2006), Alker (2006), Taureck (2006), Behnke (2006), Huysmans (2006), and Floyd (2007) on the ethical relationship of emancipation and politicization to securitization. This follows from a productive discussion on the role of security experts (Eriksson 1999; Goldmann 1999; Wæver 1999; Williams 1999). While this article does not engage this debate extensively, we would argue that, tactically, analysts and experts must understand the political dynamics of successful securitization and desecuritization processes if they wish to intervene. In this, I once again take the lead from Foucault who says that his own analysis has sprung from his personal experiences and a kind of a malaise with objective, abstract, Archimedian theory. In building from his insider knowledge of and outsider status within institutions (such as the clinic, human sexuality, or the penal system), Foucault conducts a 'history of the present' — to ask not 'what does the prison mean' but 'how does the prison mean?' With particular experience in different realms of security studies, it seems that securitization theory might contribute to this kind of history of the present. This is to say that the process of successful securitization and desecuritization operates differently within different settings. If, as security experts, it is part of our role to intervene in the securitization/desecuritization process, then we must gain a tactical knowledge of the conditions for success and failure. There is an assumption in this debate about securitization/desecuritization that experts are significant or important voices. It is true that 'in writing or speaking security, the analyst him/herself executes a speech act, this speech act is successful if the problem raised becomes recognized as a security problem in the academy and/or in the wider policy making discourse' (Floyd 2007: 336).

### 4

#### The President of the United States should issue an Executive Order prohibiting the use of offensive cyber operations absent prior Congressional notification

#### Your author says we solve

**Brecher, 2012**. (Aaron, Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations, 111 Michigan Law Review, No 3, p 423, L/N)

III. Enacting the Covert Action Regime as Presumptive via Executive Order Cyberattacks present a challenge for U.S. policymakers: they are difficult to locate within a cl

ear legal category and there is a significant risk of uncontrollable consequences associated with their use. As a result, policymakers must choose a paradigm to govern their use that will ensure that the executive branch is held accountable and shares information with legislators. 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.

**Statutory restriction kill pres powers – causes terrorism, prolif and rogue state aggression**

John **Yoo**, Law professor, former official in the United States Department of Justice, 2-1-**2012**, ABA Journal, “War Powers Belong to the President”, http://www.abajournal.com/magazine/article/war\_powers\_belong\_to\_the\_president

The most important of the president’s powers are commander in chief and chief executive. As Alexander Hamilton wrote in Federalist 74, “The direction of war implies the direction of the common strength, and the power of directing and employing the common strength forms a usual and essential part in the definition of the executive authority.” Presidents should conduct war, he wrote, because they could act with “decision, activity, secrecy and dispatch.” In perhaps his most famous words, Hamilton wrote: “Energy in the executive is a leading character in the definition of good government. ... It is essential to the protection of the community against foreign attacks.” The framers realized the obvious. Foreign affairs are unpredictable and involve the highest of stakes, making them unsuitable to regulation by pre-existing legislation. Instead, they can demand swift, decisive action—sometimes under pressured or even emergency circumstances—that is best carried out by a branch of government that does not suffer from multiple vetoes or is delayed by disagreements. Congress is too large and unwieldy to take the swift and decisive action required in wartime. Our framers replaced the Articles of Confederation, which had failed in the management of foreign relations because they had no single executive, with the Constitution’s single president for precisely this reason. Even when it has access to the same intelligence as the executive branch, Congress’ loose, decentralized structure would paralyze American policy while foreign threats grow. Congress has no political incentive to mount and see through its own wartime policy. Members of Congress, who are interested in keeping their seats at the next election, do not want to take stands on controversial issues where the future is uncertain. They will avoid like the plague any vote that will anger large segments of the electorate. They prefer that the president take the political risks and be held accountable for failure. Congress’ track record when it has opposed presidential leadership has not been a happy one. Perhaps the most telling example was the Senate’s rejection of the Treaty of Versailles at the end of World War I. Congress’ isolationist urge kept the United States out of Europe at a time when democracies fell and fascism grew in their place. Even as Europe and Asia plunged into war, Congress passed the Neutrality Acts designed to keep the United States out of the conflict. President Franklin Roosevelt violated those laws to help the Allies and draw the nation into war against the Axis. While pro-Congress critics worry about a president’s foreign adventurism, the real threat to our national security may come from inaction and isolationism. Many point to the Vietnam War as an example of the faults of the “imperial presidency.” Vietnam, however, could not have continued without the consistent support of Congress in raising a large military and paying for hostilities. And Vietnam ushered in a period of congressional dominance that witnessed American setbacks in the Cold War and the passage of the ineffectual War Powers Resolution. Congress passed the resolution in 1973 over President Richard Nixon’s veto, and no president, Republican or Democrat, George W. Bush or Obama, has ever accepted the constitutionality of its 60-day limit on the use of troops abroad. No federal court has ever upheld the resolution. Even Congress has never enforced it. Despite the record of practice and the Constitution’s institutional design, critics nevertheless argue for a radical remaking of the American way of war. They typically base their claim on Article I, Section 8, of the Constitution, which gives Congress the power to “declare war.” But these observers read the 18th century constitutional text through a modern lens by interpreting “declare war” to mean “start war.” When the Constitution was written, however, a declaration of war served diplomatic notice about a change in legal relations between nations. It had little to do with launching hostilities. In the century before the Constitution, for example, Great Britain—where the framers got the idea of the declare-war power—fought numerous major conflicts but declared war only once beforehand. Our Constitution sets out specific procedures for passing laws, appointing officers and making treaties. There are none for waging war because the framers expected the president and Congress to struggle over war through the national political process. In fact, other parts of the Constitution, properly read, support this reading. Article I, Section 10, for example, declares that the states shall not “engage” in war “without the consent of Congress” unless “actually invaded, or in such imminent danger as will not admit of delay.” This provision creates exactly the limits desired by anti-war critics, complete with an exception for self-defense. If the framers had wanted to require congressional permission before the president could wage war, they simply could have repeated this provision and applied it to the executive. Presidents, of course, do not have complete freedom to take the nation to war. Congress has ample powers to control presidential policy, if it wants to. Only Congress can raise the military, which gives it the power to block, delay or modify war plans. Before 1945, for example, the United States had such a small peacetime military that presidents who started a war would have to go hat in hand to Congress to build an army to fight it. Since World War II, it has been Congress that has authorized and funded our large standing military, one primarily designed to conduct offensive, not defensive, operations (as we learned all too tragically on 9/11) and to swiftly project power worldwide. If Congress wanted to discourage presidential initiative in war, it could build a smaller, less offensive-minded military. Congress’ check on the presidency lies not just in the long-term raising of the military. It can also block any immediate armed conflict through the power of the purse. If Congress feels it has been misled in authorizing war, or it disagrees with the president’s decisions, all it need do is cut off funds, either all at once or gradually. It can reduce the size of the military, shrink or eliminate units, or freeze supplies. Using the power of the purse does not even require affirmative congressional action. Congress can just sit on its hands and refuse to pass a law funding the latest presidential adventure, and the war will end quickly. Even the Kosovo war, which lasted little more than two months and involved no ground troops, required special funding legislation. The framers expected Congress’ power of the purse to serve as the primary check on presidential war. During the 1788 Virginia ratifying convention, Patrick Henry attacked the Constitution for failing to limit executive militarism. James Madison responded: “The sword is in the hands of the British king; the purse is in the hands of the Parliament. It is so in America, as far as any analogy can exist.” Congress ended America’s involvement in Vietnam by cutting off all funds for the war. Our Constitution has succeeded because it favors swift presidential action in war, later checked by Congress’ funding power. If a president continues to wage war without congressional authorization, as in Libya, Kosovo or Korea, it is only because Congress has chosen not to exercise its easy check. We should not confuse a desire to escape political responsibility for a defect in the Constitution. A radical change in the system for making war might appease critics of presidential power. But it could also seriously threaten American national security. In order to forestall another 9/11 attack, or to take advantage of a window of opportunity to strike terrorists or rogue nations, the executive branch needs flexibility. It is not hard to think of situations where congressional consent cannot be obtained in time to act. Time for congressional deliberation, which leads only to passivity and isolation and not smarter decisions, will come at the price of speed and secrecy. The Constitution creates a presidency that can respond forcefully to prevent serious threats to our national security. Presidents can take the initiative and Congress can use its funding power to check them. Instead of demanding a legalistic process to begin war, the framers left war to politics. As we confront the new challenges of terrorism, rogue nations and WMD proliferation, now is not the time to introduce sweeping, untested changes in the way we make war.

#### Prez flexibility solves alliances, heg, indo-pak/china war- extinction

Ben Coes 11, a former speechwriter in the George H.W. Bush administration, managed Mitt Romney’s successful campaign for Massachusetts Governor in 2002. His latest book, Coup D’Etat, has just been released. “The disease of a weak president” Read more: http://dailycaller.com/2011/09/30/the-disease-of-a-weak-president/#ixzz2cqY7Y7e0

Unfortunately, President Obama’s weakness in his response to Israel and Iran is a cause for real concern, not only for our Israeli allies, but for other American allies as well. A weak U.S. president emboldens our enemies. A good example of this is what happened the last time we had a weak president, namely Jimmy Carter. The disease of a weak president usually begins with the Achilles’ heel all politicians are born with — the desire to be popular. It leads to pandering to different audiences, people and countries and creates a sloppy, incoherent set of policies. Ironically, it ultimately results in that very politician losing the trust and respect of friends and foes alike. In the case of Israel, those of us who are strong supporters can at least take comfort in the knowledge that Tel Aviv will do whatever is necessary to protect itself from potential threats from its unfriendly neighbors. While it would be preferable for the Israelis to be able to count on the United States, in both word and deed, the fact is right now they stand alone. Obama and his foreign policy team have undercut the Israelis in a multitude of ways. Despite this, I wouldn’t bet against the soldiers of Shin Bet, Shayetet 13 and the Israeli Defense Forces. But Obama’s weakness could — in other places — have implications far, far worse than anything that might ultimately occur in Israel. The triangular plot of land that connects Pakistan, India and China is held together with much more fragility and is built upon a truly foreboding foundation of religious hatreds, radicalism, resource envy and nuclear weapons. If you can only worry about preventing one foreign policy disaster, worry about this one. Here are a few unsettling facts to think about: First, Pakistan and India have fought three wars since the British de-colonized and left the region in 1947. All three wars occurred before the two countries had nuclear weapons. Both countries now possess hundreds of nuclear weapons, enough to wipe each other off the map many times over. Second, Pakistan is 97% Muslim. It is a question of when — not if — Pakistan elects a radical Islamist in the mold of Ayatollah Khomeini as its president. Make no mistake, it will happen, and when it does the world will have a far greater concern than Ali Khamenei or Mahmoud Ahmadinejad and a single nuclear device. Third, China sits at the northern border of both India and Pakistan. China is strategically aligned with Pakistan. Most concerning, China covets India’s natural resources. Over the years, it has slowly inched its way into the northern tier of India-controlled Kashmir Territory, appropriating land and resources and drawing little notice from the outside world. In my book, Coup D’Etat, I consider this tinderbox of colliding forces in Pakistan, India and China as a thriller writer. But thriller writers have the luxury of solving problems by imagining solutions on the page. In my book, when Pakistan elects a radical Islamist who then starts a war with India and introduces nuclear weapons to the theater, America steps in and removes the Pakistani leader through a coup d’état. I wish it was that simple. The more complicated and difficult truth is that we, as Americans, must take sides. We must be willing to be unpopular in certain places. Most important, we must be ready and willing to threaten our military might on behalf of our allies. And our allies are Israel and India. There are many threats out there — Islamic radicalism, Chinese technology espionage, global debt and half a dozen other things that smarter people than me are no doubt worrying about. But the single greatest threat to America is none of these. The single greatest threat facing America and our allies is a weak U.S. president. It doesn’t have to be this way. President Obama could — if he chose — develop a backbone [strength] and lead. Alternatively, America could elect a new president. It has to be one or the other. The status quo is simply not an option.

### Cyber Attacks

#### Nuke war outweighs cyber attack

Jason **Healey**, 3-30-**2013**, “No, Cyberwarfare Isn't as Dangerous as Nuclear War,” US News and World Report, http://www.usnews.com/opinion/blogs/world-report/2013/03/20/cyber-attacks-not-yet-an-existential-threat-to-the-us

**America does not face an existential cyberthreat today, despite recent warnings.** Our **cybervulnerabilities are** undoubtedly **grave and the threats** we face **are severe but far from comparable to nuclear war**. The most **recent** alarms come in a Defense Science Board **report** on how to make military cybersystems more resilient against advanced threats (in short, Russia or China). It **warned** that the "**cyber threat is serious, with potential consequences similar** in some ways **to the nuclear threat** of the Cold War." Such fears were also expressed by Adm. Mike Mullen, then chairman of the Joint Chiefs of Staff, in 2011. **He called cyber** "**The single biggest existential threat** that's out there" because "cyber actually more than theoretically, can attack our infrastructure, our financial systems." While it is true that cyber attacks might do these things, it is also **true they have not only never happened but are far more difficult to accomplish than mainstream thinking believes**. The **consequences from cyber threats may be similar in some ways to nuclear**, as the Science Board concluded**, but mostly, they are incredibly dissimilar**. [See a collection of political cartoons on defense spending.] Eighty years ago, the generals of the U.S. Army Air Corps were sure that their bombers would easily topple other countries and cause their populations to panic, claims which did not stand up to reality. **A study of the 25-year history of cyber conflict**, by the Atlantic Council and Cyber Conflict Studies Association**, has shown** a similar dynamic where **the impact of disruptive cyberattacks has been consistently overestimated**. Rather than theorizing about future cyberwars or extrapolating from today's concerns, **the history of cyberconflict that have actually been fought, shows that cyber incidents have so far tended to have effects that are either widespread but fleeting or persistent but narrowly focused.** **No attacks**, so far**, have been both widespread and persistent. There have been no authenticated cases of anyone dying from a cyber attack**. Any widespread disruptions, even the 2007 disruption against Estonia, have been short-lived causing no significant GDP loss. Moreover, as with conflict in other domains, cyberattacks can take down many targets but keeping them down over time in the face of determined defenses has so far been out of the range of all but the most dangerous adversaries such as Russia and China. Of course, if the United States is in a conflict with those nations, cyber will be the least important of the existential threats policymakers should be worrying about. **Plutonium trumps bytes in a shooting war.** [Read the U.S. News Debate: Should There Be an International Treaty on Cyberwarfare?] This is not all good news. Policymakers have recognized the problems since at least 1998 with little significant progress. Worse, the threats and vulnerabilities are getting steadily more worrying. Still, **experts have been warning of a cyber Pearl Harbor for 20** of the 70 **years** since the actual Pearl Harbor. The transfer of U.S. trade secrets through Chinese cyber espionage **could someday accumulate into an existential threat. But it doesn't seem so** seem just **yet,** with only handwaving estimates of **annual losses of 0.1 to 0.5 percent** to the total U.S. GDP of around $15 trillion. That's bad, but **it doesn't add up to an existential crisis or "economic cyberwar**." [See a collection of political cartoons on the economy.] Instead, the true existential cyberdanger is likely to come after America connects the electrical grid and other infrastructure to the Internet. An interconnected Smart Grid connects things made not just of bytes and silicon but of concrete and steel. It is all too likely that America will take its overstretched and insecure electrical system and connect it to the Internet. In this future our electric supply is no more or less reliable than the Internet and the years when no one died because of cyberattacks will seem like the quaint good ol' days. There are still **practical solutions** to avoid today's serious threats become tomorrow's existential ones but these **are often overshadowed by the rhetoric of cyberwar, the push for ever better U.S. cyberoffense**, and other distractions. Focusing on actual fixes, like securing the Smart Grid, will be the best ways to avoid future existential attacks.

#### Cyber war infeasible

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

The Department of Homeland Security worries that our critical infrastructure and key resources (CIKR) may be exposed, both directly and indirectly, to multiple threats because of CIKR reliance on the global cyber infrastructure, an infrastructure that is under routine cyberattack by a “spectrum of malicious actors” (National Infrastructure Protection Plan 2009). CIKR in the extremely large and complex U.S. economy spans multiple sectors including agricultural, finance and banking, dams and water resources, public health and emergency services, military and defense, transportation and shipping, and energy (National Infrastructure Protection Plan 2009). The disruption and destruction of public and private infrastructure is part of warfare, without this infrastructure conflict cannot be sustained (Geers 2011). Cyber-attacks are desirable because they are considered to be a relatively “low cost and long range” weapon (Lewis 2010), but prior to the creation of Stuxnet, the first cyber-weapon, the ability to disrupt and destroy critical infrastructure through cyber-attack was theoretical. The movement of an offensive cyber-weapon from conceptual to actual has forced the United States to question whether offensive cyber-attacks are a significant threat that are able to disrupt or destroy CIKR to the level that national security is seriously degraded. It is important to understand the risk posed to national security by cyber-attacks to ensure that government responses are appropriate to the threat and balance security with privacy and civil liberty concerns. The risk posed to CIKR from cyber-attack can be evaluated by measuring the threat from cyber-attack against the vulnerability of a CIKR target and the consequences of CIKR disruption. As the only known cyber-weapon, Stuxnet has been thoroughly analyzed and used as a model for predicting future cyber-weapons. The U.S. electrical grid, a key component in the CIKR energy sector, is a target that has been analyzed for vulnerabilities and the consequences of disruption predicted – the electrical grid has been used in multiple attack scenarios including a classified scenario provided to the U.S. Congress in 2012 (Rohde 2012). Stuxnet will serve as the weapon and the U.S. electrical grid will serve as the target in this risk analysis that concludes that there is a low risk of disruption or destruction of critical infrastructure from a an offensive cyber-weapon because of the complexity of the attack path, the limited capability of non-state adversaries to develop cyber-weapons, and the existence of multiple methods of mitigating the cyber-attacks. To evaluate the threat posed by a Stuxnet-like cyber-weapon, the complexity of the weapon, the available attack vectors for the weapon, and the resilience of the weapon must be understood. The complexity – how difficult and expensive it was to create the weapon – identifies the relative cost and availability of the weapon; inexpensive and simple to build will be more prevalent than expensive and difficult to build. Attack vectors are the available methods of attack; the larger the number, the more severe the threat. For example, attack vectors for a cyberweapon may be email attachments, peer-to-peer applications, websites, and infected USB devices or compact discs. Finally, the resilience of the weapon determines its availability and affects its usefulness. A useful weapon is one that is resistant to disruption (resilient) and is therefore available and reliable. These concepts are seen in the AK-47 assault rifle – a simple, inexpensive, reliable and effective weapon – and carry over to information technology structures (Weitz 2012). The evaluation of Stuxnet identified malware that is “unusually complex and large” and required code written in multiple languages (Chen 2010) in order to complete a variety of specific functions contained in a “vast array” of components – it is one of the most complex threats ever analyzed by Symantec (Falliere, Murchu and Chien 2011). To be successful, Stuxnet required a high level of technical knowledge across multiple disciplines, a laboratory with the target equipment configured for testing, and a foreign intelligence capability to collect information on the target network and attack vectors (Kerr, Rollins and Theohary 2010). The malware also needed careful monitoring and maintenance because it could be easily disrupted; as a result Stuxnet was developed with a high degree of configurability and was upgraded multiple times in less than one year (Falliere, Murchu and Chien 2011). Once introduced into the network, the cyber-weapon then had to utilize four known vulnerabilities and four unknown vulnerabilities, known as zero-day exploits, in order to install itself and propagate across the target network (Falliere, Murchu and Chien 2011). Zero-day exploits are incredibly difficult to find and fewer than twelve out of the 12,000,000 pieces of malware discovered each year utilize zero-day exploits and this rarity makes them valuable, zero-days can fetch $50,000 to $500,000 each on the black market (Zetter 2011). The use of four rare exploits in a single piece of malware is “unprecedented” (Chen 2010). Along with the use of four unpublished exploits, Stuxnet also used the “first ever” programmable logic controller rootkit, a Windows rootkit, antivirus evasion techniques, intricate process injection routines, and other complex interfaces (Falliere, Murchu and Chien 2011) all wrapped up in “layers of encryption like Russian nesting dolls” (Zetter 2011) – including custom encryption algorithms (Karnouskos 2011). As the malware spread across the now-infected network it had to utilize additional vulnerabilities in proprietary Siemens industrial control software (ICS) and hardware used to control the equipment it was designed to sabotage. Some of these ICS vulnerabilities were published but some were unknown and required such a high degree of inside knowledge that there was speculation that a Siemens employee had been involved in the malware design (Kerr, Rollins and Theohary 2010). The unprecedented technical complexity of the Stuxnet cyber-weapon, along with the extensive technical and financial resources and foreign intelligence capabilities required for its development and deployment, indicates that the malware was likely developed by a nation-state (Kerr, Rollins and Theohary 2010). Stuxnet had very limited attack vectors. When a computer system is connected to the public Internet a host of attack vectors are available to the cyber-attacker (Institute for Security Technology Studies 2002). Web browser and browser plug-in vulnerabilities, cross-site scripting attacks, compromised email attachments, peer-to-peer applications, operating system and other application vulnerabilities are all vectors for the introduction of malware into an Internetconnected computer system. Networks that are not connected to the public internet are “air gapped,” a technical colloquialism to identify a physical separation between networks. Physical separation from the public Internet is a common safeguard for sensitive networks including classified U.S. government networks. If the target network is air gapped, infection can only occur through physical means – an infected disk or USB device that must be physically introduced into a possibly access controlled environment and connected to the air gapped network. The first step of the Stuxnet cyber-attack was to initially infect the target networks, a difficult task given the probable disconnected and well secured nature of the Iranian nuclear facilities. Stuxnet was introduced via a USB device to the target network, a method that suggests that the attackers were familiar with the configuration of the network and knew it was not connected to the public Internet (Chen 2010). This assessment is supported by two rare features in Stuxnet – having all necessary functionality for industrial sabotage fully embedded in the malware executable along with the ability to self-propagate and upgrade through a peer-to-peer method (Falliere, Murchu and Chien 2011). Developing an understanding of the target network configuration was a significant and daunting task based on Symantec’s assessment that Stuxnet repeatedly targeted a total of five different organizations over nearly one year (Falliere, Murchu and Chien 2011) with physical introduction via USB drive being the only available attack vector. The final factor in assessing the threat of a cyber-weapon is the resilience of the weapon. There are two primary factors that make Stuxnet non-resilient: the complexity of the weapon and the complexity of the target. Stuxnet was highly customized for sabotaging specific industrial systems (Karnouskos 2011) and needed a large number of very complex components and routines in order to increase its chance of success (Falliere, Murchu and Chien 2011). The malware required eight vulnerabilities in the Windows operating system to succeed and therefore would have failed if those vulnerabilities had been properly patched; four of the eight vulnerabilities were known to Microsoft and subject to elimination (Falliere, Murchu and Chien 2011). Stuxnet also required that two drivers be installed and required two stolen security certificates for installation (Falliere, Murchu and Chien 2011); driver installation would have failed if the stolen certificates had been revoked and marked as invalid. Finally, the configuration of systems is ever-changing as components are upgraded or replaced. There is no guarantee that the network that was mapped for vulnerabilities had not changed in the months, or years, it took to craft Stuxnet and successfully infect the target network. Had specific components of the target hardware changed – the targeted Siemens software or programmable logic controller – the attack would have failed. Threats are less of a threat when identified; this is why zero-day exploits are so valuable. Stuxnet went to great lengths to hide its existence from the target and utilized multiple rootkits, data manipulation routines, and virus avoidance techniques to stay undetected. The malware’s actions occurred only in memory to avoid leaving traces on disk, it masked its activities by running under legal programs, employed layers of encryption and code obfuscation, and uninstalled itself after a set period of time, all efforts to avoid detection because its authors knew that detection meant failure. As a result of the complexity of the malware, the changeable nature of the target network, and the chance of discovery, Stuxnet is not a resilient system. It is a fragile weapon that required an investment of time and money to constantly monitor, reconfigure, test and deploy over the course of a year. There is concern, with Stuxnet developed and available publicly, that the world is on the brink of a storm of highly sophisticated Stuxnet-derived cyber-weapons which can be used by hackers, organized criminals and terrorists (Chen 2010). As former counterterrorism advisor Richard Clarke describes it, there is concern that the technical brilliance of the United States “has created millions of potential monsters all over the world” (Rosenbaum 2012). Hyperbole aside, technical knowledge spreads. The techniques behind cyber-attacks are “constantly evolving and making use of lessons learned over time” (Institute for Security Technology Studies 2002) and the publication of the Stuxnet code may make it easier to copy the weapon (Kerr, Rollins and Theohary 2010). However, this is something of a zero-sum game because knowledge works both ways and cyber-security techniques are also evolving, and “understanding attack techniques more clearly is the first step toward increasing security” (Institute for Security Technology Studies 2002). Vulnerabilities are discovered and patched, intrusion detection and malware signatures are expanded and updated, and monitoring and analysis processes and methodologies are expanded and honed. Once the element of surprise is lost, weapons and tactics are less useful, this is the core of the argument that “uniquely surprising” stratagems like Stuxnet are single-use, like Pearl Harbor and the Trojan Horse, the “very success [of these attacks] precludes their repetition” (Mueller 2012). This paradigm has already been seen in the “son of Stuxnet” malware – named Duqu by its discoverers – that is based on the same modular code platform that created Stuxnet (Ragan 2011). With the techniques used by Stuxnet now known, other variants such as Duqu are being discovered and countered by security researchers (Laboratory of Cryptography and System Security 2011). It is obvious that the effort required to create, deploy, and maintain Stuxnet and its variants is massive and it is not clear that the rewards are worth the risk and effort. Given the location of initial infection and the number of infected systems in Iran (Falliere, Murchu and Chien 2011) it is believed that Iranian nuclear facilities were the target of the Stuxnet weapon. A significant amount of money and effort was invested in creating Stuxnet but yet the expected result – assuming that this was an attack that expected to damage production – was minimal at best. Iran claimed that Stuxnet caused only minor damage, probably at the Natanz enrichment facility, the Russian contractor Atomstroyeksport reported that no damage had occurred at the Bushehr facility, and an unidentified “senior diplomat” suggested that Iran was forced to shut down its centrifuge facility “for a few days” (Kerr, Rollins and Theohary 2010). Even the most optimistic estimates believe that Iran’s nuclear enrichment program was only delayed by months, or perhaps years (Rosenbaum 2012). The actual damage done by Stuxnet is not clear (Kerr, Rollins and Theohary 2010) and the primary damage appears to be to a higher number than average replacement of centrifuges at the Iran enrichment facility (Zetter 2011). Different targets may produce different results. The Iranian nuclear facility was a difficult target with limited attack vectors because of its isolation from the public Internet and restricted access to its facilities. What is the probability of a successful attack against the U.S. electrical grid and what are the potential consequences should this critical infrastructure be disrupted or destroyed? An attack against the electrical grid is a reasonable threat scenario since power systems are “a high priority target for military and insurgents” and there has been a trend towards utilizing commercial software and integrating utilities into the public Internet that has “increased vulnerability across the board” (Lewis 2010). Yet the increased vulnerabilities are mitigated by an increased detection and deterrent capability that has been “honed over many years of practical application” now that power systems are using standard, rather than proprietary and specialized, applications and components (Leita and Dacier 2012). The security of the electrical grid is also enhanced by increased awareness after a smart-grid hacking demonstration in 2009 and the identification of the Stuxnet malware in 2010; as a result the public and private sector are working together in an “unprecedented effort” to establish robust security guidelines and cyber security measures (Gohn and Wheelock 2010).

#### Cyberattacks impossible – empirics and defenses solve

Rid 12 (Thomas Rid, reader in war studies at King's College London, is author of "Cyber War Will Not Take Place" and co-author of "Cyber-Weapons.", March/April 2012, “Think Again: Cyberwar”, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full)

"Cyberwar Is Already Upon Us." No way. "Cyberwar is coming!" John Arquilla and David Ronfeldt predicted in a celebrated Rand paper back in 1993. Since then, it seems to have arrived -- at least by the account of the U.S. military establishment, which is busy competing over who should get what share of the fight. Cyberspace is "a domain in which the Air Force flies and fights," Air Force Secretary Michael Wynne claimed in 2006. By 2012, William J. Lynn III, the deputy defense secretary at the time, was writing that cyberwar is "just as critical to military operations as land, sea, air, and space." In January, the Defense Department vowed to equip the U.S. armed forces for "conducting a combined arms campaign across all domains -- land, air, maritime, space, and cyberspace." Meanwhile, growing piles of books and articles explore the threats of cyberwarfare, cyberterrorism, and how to survive them. 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. "A Digital Pearl Harbor Is Only a Matter of Time." 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. "Cyberattacks Are Becoming Easier." Just the opposite. U.S. Director of National Intelligence James R. Clapper warned last year that the volume of malicious software on American networks had more than tripled since 2009 and that more than 60,000 pieces of malware are now discovered every day. The United States, he said, is undergoing "a phenomenon known as 'convergence,' which amplifies the opportunity for disruptive cyberattacks, including against physical infrastructures." ("Digital convergence" is a snazzy term for a simple thing: more and more devices able to talk to each other, and formerly separate industries and activities able to work together.) Just because there's more malware, however, doesn't mean that attacks are becoming easier. In fact, potentially damaging or life-threatening cyberattacks should be more difficult to pull off. Why? Sensitive systems generally have built-in redundancy and safety systems, meaning an attacker's likely objective will not be to shut down a system, since merely forcing the shutdown of one control system, say a power plant, could trigger a backup and cause operators to start looking for the bug. To work as an effective weapon, malware would have to influence an active process -- but not bring it to a screeching halt. If the malicious activity extends over a lengthy period, it has to remain stealthy. That's a more difficult trick than hitting the virtual off-button. Take Stuxnet, the worm that sabotaged Iran's nuclear program in 2010. It didn't just crudely shut down the centrifuges at the Natanz nuclear facility; rather, the worm subtly manipulated the system. Stuxnet stealthily infiltrated the plant's networks, then hopped onto the protected control systems, intercepted input values from sensors, recorded these data, and then provided the legitimate controller code with pre-recorded fake input signals, according to researchers who have studied the worm. Its objective was not just to fool operators in a control room, but also to circumvent digital safety and monitoring systems so it could secretly manipulate the actual processes. Building and deploying Stuxnet required extremely detailed intelligence about the systems it was supposed to compromise, and the same will be true for other dangerous cyberweapons. Yes, "convergence," standardization, and sloppy defense of control-systems software could increase the risk of generic attacks, but the same trend has also caused defenses against the most coveted targets to improve steadily and has made reprogramming highly specific installations on legacy systems more complex, not less.

#### Zero impact to cyber arms race --- 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.

#### xxGrid is resilient and sustainable

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

In 2003, a simple physical breakdown occurred – trees shorted a power line and caused a fault – that had a cascading effect and caused a power blackout across the Northeast (Lewis 2010). This singular occurrence has been used as evidence that the electrical grid is fragile and subject to severe disruption through cyber-attack, a disruption that could cost billions of dollars, brings business to a halt, and could even endanger lives – if compounded by other catastrophic events (Brennan 2012). A power disruption the size of the 2003 blackout, the worst in American history at that time (Minkel 2008), is a worst case scenario and used as an example of the fragility of the U.S. energy grid. This perceived fragility is not real when viewed in the context of the robustness of the electrical grid. When asked about cyber-attacks against the electrical grid in April of 2012, the intelligence chief of U.S. Cyber Command Rear Admiral Samuel Cox stated that an attack was unlikely to succeed because of the “huge amounts of resiliency built into the [electrical] system that makes that kind of catastrophic thing very difficult” (Capaccio 2012). This optimistic view is supported by an electrical grid that has proven to be robust in the face of large natural catastrophes. Complex systems like the electrical grid in the U.S. are prone to failures and the U.S. grid fails frequently. Despite efforts to reduce the risk out power outages, the risk is always present. Power outages that affect more than 50,000 people have occurred steadily over the last 20 years at a rate of 12% annually and the frequency of large catastrophes remains relatively high and outages the size of the 2003 blackout are predicted to occur every 25 years (Minkel 2008). In a complex system that is always at risk of disruption, the effect is mitigated by policies and procedures that are meant to restore services as quickly as possible. The most visible of these policies is the interstate Emergency Management Assistance Compact, a legally binding agreement allowing combined resources to be quickly deployed in response to a catastrophic disaster such as power outages following a severe hurricane (Kapucu, Augustin and Garayev 2009). The electrical grid suffers service interruptions regularly, it is a large and complex system supporting the largest economy in the world, and yet commerce does not collapse (Lewis 2010). Despite blizzards, earthquakes, fires, and hurricanes that cause blackouts, the economy is affected but does not collapse and even after massive damage like that caused by Hurricane Katrina, national security is not affected because U.S. military capability is not degraded (Lewis 2010). Cyber-security is an ever-increasing concern in an increasingly electronic and interconnected world. Cyber-security is a high priority “economic and national security challenge” (National Security Council n.d.) because cyber-attacks are expected to become the top national security threat (Robert S. Mueller 2012). In response to the threat Congress is crafting legislation to enhance cyber-security (Brito and Watkins 2012) and the Department of Homeland Security budget for cyber-security has been significantly increased (U.S. Senate Committee on Homeland Security and Governmental Affairs 2012).

#### xxThe grid is air-gapped

Michael Tanji 10, spent 20 years in the US intelligence community; veteran of the US Army; served in strategic and tactical assignments worldwide; participated in national and international analysis and policy efforts for the NIC, NSC and NATO; Claremont Institute Lincoln Fellow and Senior Fellow at the Center of Threat Awareness; lectures on intelligence issues at The George Washington University, 7/13/10, “Hacking the Electric Grid? You and What Army?,” <http://www.wired.com/dangerroom/2010/07/hacking-the-electric-grid-you-and-what-army/>

Grid-hacking is back in the news, with the unveiling of “Perfect Citizen,” the National Security Agency’s creepily named effort to protect the networks of electrical companies and nuclear power plants. People have claimed in the past to be able to turn off the internet, there are reports of foreign penetrations into government systems, “proof” of foreign interest in attacking U.S. critical infrastructure based on studies, and concerns about adversary capabilities based on allegations of successful critical infrastructure attacks. Which begs the question: If it’s so easy to turn off the lights using your laptop, how come it doesn’t happen more often? The fact of the matter is that it isn’t easyto do any of these things. Your average power grid or drinking-water system isn’t analogous to a PC or even to a corporate network. The complexityof such systems, and the use of proprietary operating systems and applications that are not readily available for study by your average hacker, make the development of exploits for any uncovered vulnerabilitiesmuch more difficult than using Metasploit. To start, these systems arerarely connected directly to the public internet. And that makes gaining access to grid-controlling networks a challenge for all but the most dedicated, motivated and skilled — nation-states, in other words.

#### No grid collapse—decentralization, major power users have backups and your evidence is just alarmism

Gosh 9 Bobby, “How Vulnerable Is the Power Grid?” [http://www.time.com/time/nation/article/0,8599,1891562,00.html] April 15

As bad as all that may sound, there are several reasons not to panic about our power grid's vulnerability.

•No national power grid anywhere in the world has been brought down by a cyberattack.And it's worth keeping in mind that most countries have much fewer defenses from cyberattacksthan the U.S. "It's virtually impossible to bringdown the entireNorth American grid," says Major General (Rtd) Dale Meyerrose, a cybersecurity expert who recently retired as chief information officer for the Director of National Intelligence. The electricity-distribution system is highly decentralized, and there's no central control system; at worst, cyberattackers may be able to damage sections of the grid.•The most critical power users — the military, hospitals, the banking system, phone networks, Google's server farms — have multiple contingencies for uninterrupted power supply and backup generation. In the event of a cyberattack on the grid, they would beable to operatefor long periods — days, weeks and, in some cases, indefinitely — without much difficulty.•The power grid is far from perfect. On any given day, 500,000 Americans experience an outage, says ArshadMansoor of the Electric Power Research Institute, which is funded by the utility industry. Why is this a good thing? Because it means the grid deals with breakdowns all the time, and the industry knows how to fix them. The grid has built-in redundancies and manual overrides that allow for restoration of supply. Mansoor is careful to point out that these are "not defenses against cyberattacks, but for dealing with the consequence of such attacks." •The larger point is that in most cases, damage done to the power supply can be undone. "In the banking system, if someone hacks the system and steals information about 500,000 credit cards, it's incredibly tough to undo that damage," says Mansoor. "But if a section of the power grid goes down, we start it up again." Of course, every power outage comes with a cost, not least to the economy. Mansoor would not discuss how long it would take to recover from a cyberattack — there are too many variables involved — but said the longest delays in restoring power are typically caused not by technological glitches but by major acts of God, like hurricanes and earthquakes that destroy physical infrastructure. (Read a TIME blog on China and hacking.) This is not to suggest that the power grid can't be hacked into. In 2007, CNN reported that researchers working for the Department of Energy had mounted an experimental cyberattack against a power generator and were able to get it to self-destruct. Details of the experiment were kept from the public at the request of the Department of Homeland Security.While Meyerrose, Mansoor and other experts agree that the utility industry's vulnerability will grow as its command-and-control systems rely ever more on computer networks, those concerns are not new. Some security experts have cautioned against the growing use of "smart grid" technology — which relies even more on computer networks to allow both utilities and individual consumers to monitor and reduce power usage. There are already 2 million smart meters in use in the U.S., and the Obama Administration's 2010 budget includes $4.5 billion in spending on such technology. The fear is that these meters may allow hackers access to the grid's control systems. But smart-grid backers say the opposite is true: the use of more-sophisticated monitoring systems makes the grid safer.The timing of the recent reports about the power grid's vulnerability to cyberattacks may have more to do with politics than anything else. The news flurry coincided with the introduction of a new bill, by Senators Jay Rockefeller and Olympia Snowe, to impose cybersecurity standards on private industry — regulations that would likely affect the utilities and other vital infrastructure. And this week marks the end of a 60-day review by the National Security Council of the nation's cybersecurity polices and practices; the results will be submitted to President Obama any day now, and will likely be made public later this month.

#### Microgrids solve DOD vulnerability

Pike Research 11, market research and consulting firm that provides in-depth analysis of global clean technology markets, 9/16/’11

(<http://www.pikeresearch.com/newsroom/military-microgrid-capacity-to-experience-more-than-700-growth-by-2017>)

Military Microgrid Capacity to Experience More than 700% Growth by 2017 September 16, 2011 The United States Department of Defense (DOD) is the single largest consumer of petroleum in the world. U.S. military operations are also the largest consumer of all forms of energy globally. Microgrids, which enable distributed energy generation at a localized scale including the ability to “island”themselves from larger utility grids, can shrink the amount of fossil fuels consumed to create electricity by networking generators as a system to maximize efficiency. Microgrids enable military bases – both stationary and tactical – to sustain operations no matter what is happening on the larger utility grid or in the theater of war. According to a new report from Pike Research, the capacity of military microgrids will grow at a rate of 739% between 2011 and 2017, increasing from 38 megawatts (MW) to 316 MW during that period, under a baseline forecast scenario. The cleantech market intelligence firm expects that, under a more aggressive adoption scenario, stationary and mobile military microgrid capacity could reach as high as 817 MW during the same timeframe. “The military’s primary concern is disruption of service from utility transmission and distribution lines,” says senior analyst Peter Asmus. “The lack of control and ownership of these lines – and the uneven quality of power service regionally throughout the United States – has prompted the DOD to reexamine the existing electricity service delivery model. This analysis has led the DOD to the inevitable conclusion that the best wayto bolster its ability to secure power may well be through microgrid technology it can own and control.” Asmus adds that, as awareness about the electrical grid’s vulnerability to terrorist attacks has increased in recent times, the U.S. military has become one of the strongest proponents of microgrids, which offer the ultimate secure power supply for fixed base mobile operations. Many army, navy, air force, and other related bases and offices already have vintage microgrids in place. What is new, says Asmus, is that these facilities are looking to envelop entire bases with microgrids and integrate distributed energy generation on-site. These resources, when capable of safe islanding from the surrounding grid, offer the ultimate security since fuel never runs out with renewable energy resources such as solar or wind. The opportunity to help develop these microgrids has attracted a number of powerful technology companies including Lockheed Martin, GE, Honeywell, Boeing, and Eaton.

#### xxBackup capacity solves blackouts

Aimone 9-12 (Dr. Michael, Director of Business Enterprise Integration – Office of the Deputy Under Secretary of Defense (Installations and Environment), “Statement Before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies,” 2012, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Aimone.pdf)

DoD’s facility energy strategy is also focused heavily on grid securityin the name of mission assurance. Although the Department’s fixed installations traditionally served largely as a platform for training and deployment of forces, in recent years they have begun to provide direct support for combat operations, such as unmanned aerial vehicles (UAVs) flown in Afghanistan from fixed installations here in the United States. Our fixed installations also serve as staging platforms for humanitarian and homeland defense missions. These installations are largely dependent on a commercial power grid that is vulnerable to disruption due to aging infrastructure, weather-related events, and potential kinetic, cyber attack. In 2008, the Defense Science Board warned that DoD’s reliance on a fragile power grid to deliver electricity to its bases places critical missions at risk. 1 Standby Power Generation Currently, DoD ensures that it can continue mission critical activities on base largely through its fleet of on-site power generation equipment. This equipment is connected to essential mission systems and automatically operates in the event of a commercial grid outage. In addition, each installation has standby generators in storage for repositioning as required. Facility power production specialists ensure that the generators are primed and ready to work, and that they are maintained and fueled during an emergency.With careful maintenance these generators can bridge the gap for even a lengthy outage. As further back up to this installed equipment, DoD maintains a strategic stockpile of electrical power generators and support equipment that is kept in operational readiness. For example, during Hurricane Katrina, the Air Force transported more than 2 megawatts of specialized diesel generators from Florida, where they were stored, to Keesler Air Force Base in Mississippi, to support base recovery.

#### xxVenture capital shifting to grid modernization now

NBC 12 [Dinah WisenbergBrin, award-winning writer with a strong background producing financial, healthcare, government news, “Clean Tech Investing Shifts, With Lower-Cost Ventures Gaining Favor” March 1, http://www.cnbc.com/id/46222448/Clean\_Tech\_Investing\_Shifts\_With\_Lower\_Cost\_Ventures\_Gaining\_Favor]

For many investors, that change means shifting funds from capital-intensive alternative-energy technologies, such as solar panels, to lower-cost ventures focused on energy efficiency and “smart grid” technologies that automate electric utility operations. “We continue to be very optimistic about things like the smart grid and the infusion of information technologies and software services” into old lines like electricity, agriculture and the built environment," says Steve Vassallo, general partner in Foundation Capital. “We’re very bullish on what I would consider the nexus of information technology and clean tech.” Foundation, based in Menlo Park, Calif., reflects this in investments such as Sentient Energy Inc., a smart-grid monitoring company that allows utilities to remotely find power outages, and Silver Spring Networks, which provides utilities a wireless network for advanced metering and remote service connection. Another holding, EnerNOC [ENOC 10.13 -0.22 (-2.13%) ], a demand-response business with technology to turn off noncritical power loads during peak periods, went public in 2007. EMeter, a one-time Foundation investment, was recently acquired by Siemens Industry [SI 93.09 0.23 (+0.25%) ]. To be sure, investors have not abandoned costlier technologies with longer-term horizons, but many — put off, in part, by last year’s bankruptcy and shutdown of solar power firm Solyndra — now favor smaller infusions in businesses with a quicker potential payoff. Rob Day, partner in Boston-based Black Coral Capital, says his cleantech investment firm maintains some solar holdings, but he sees a shift from an emphasis on those types of plays to more “intelligence-driven, software-driven, web-driven businesses.” These technologies can be used to improve existing businesses, he says. One Black Coral smart-technology investment is Digital Lumens of Boston, which makes high-efficiency, low-cost LED lighting for warehouses and factories. Software and controls are embedded in the fixtures, which can cut lighting bills by 90 percent, providing customers a two-year payback, says Day. U.S. venture capital investment in cleantech companies hit $4.9 billion last year, down 4.5 percent in dollar terms but flat in the number of transactions, according to Ernst & Young LLP, which analyzed data from Dow Jones VentureSource. Cleantech companies raised 29 percent more capital last year than in 2009, E&Y said recently. Most of that decline, however, came from less investment in sectors that were once hot. Investment in energy and electric generation, including solar businesses, fell 5 percent to $1.5 billion, while that of industry products and services companies plunged 34 percent to $1 billion, according to E&Y's analysis of equity investments from venture capital firms, corporations and individuals. The energy efficiency category leads the diverse industry in deals with 78 transactions worth $646.9 million. Energy-storage companies raised $932.6 million, a 250 percent increase and 47 percent deal increase. “Cleantech is … a maturing industry. I think people are beginning to have worked through the early stages, figured out where the more attractive opportunities are and those less so, and meanwhile lots and lots of changes have occurred in the broader world,” says Dan Reicher, executive director of Stanford University’s Center for Energy Policy and Finance, and a faculty member of the university’s business and law schools. Cleantech investment in 2011 brought a number of other important changes: Most of the money went to companies already generating revenue, the emergence of innovative contributions from the IT industry and extraordinary interest by the Chinese in large-scale, capital-intensive technology, such as energy hardware. Many U.S. companies can’t get domestic backing for what they call the “valley of death” phase: between the VC-backed pilot plant and the fully commercialized facility. As a result, they are increasingly turning to China, says Reicher. “There are clearly economic implications," he adds. "The wonderful fruits of our innovation in this country are increasingly being consumed in China, and that has implications for job creation here, for a whole host of things that are important to our economy and our security." Stanford is developing a financing vehicle to address that valley, but Reicher says he couldn’t provide details yet. “You really want to see big impacts; you’ve got to put big money in,” says Kilambi, the serial entrepreneur, who has experience raising large sums of investment capital. Federal funding for cleantech is facing more political resistence in the wake of the Solyndra collapse. President Obama has requested $2.27 billion in his 2013 budget, versus $3.2 billion the previous year. Congress, however, has approved less than the president's requests for the last three fiscal years, notes Reicher. Black Rock’s Day, who laments the politicization of the cleantech sector, suggests that investors look beyond Solyndra or the next election to what will happen over the next 20- or 50-year cycle.

#### US conventional capabilities suck

David P. **Calleo**, University Professor, Johns Hopkins University, "Unipolar Illusions," SURVIVAL v. 49 n. 3, Autumn 20**07**, pp. 73-78.

Given our future's high potential for discord and destruction, having a hegemonic superpower already installed might seem a great good fortune. Yet, recent experience also reveals that America's global predominance has been seriously overestimated. Put to the test, American power counts for less than expected. While the United States is lavishly outfitted for high-technology warfare, pursuing a hegemonic agenda in today's world requires different capabilities for more primitive forms of combat, like countering guerrilla warfare and suicidal terrorism. The American military loathes this kind of fighting and, to date, has not been very good at it. Greater success would seem to require a different sort of military - with more and cheaper troops, trained for intimate contact with the enemy, and prepared for high casualties. Controlling hostile populations will demand extensive linguistic and policing skills. The United States is now spending heavily to compensate for its deficiencies, but is still far short of the resources needed to prevail.

#### Offensive capabilities are key to deterrence – without offensive policy flexibility the US will be vulnerable to attack

Jarno Limnéll October 9 2012 “Offensive Cyber Capabilities Need to be Built and Exposed Because of Deterrence”, <http://www.infosecisland.com/blogview/22534-Offensive-Cyber-Capabilities-Need-to-be-Built-and-Exposed-Because-of-Deterrence.html>

Within the next couple of years the world will experience more intentionally executed and demonstrated cyberattacks while the development of offensive cyberweapons will become fiercer and publicly more acceptable.¶ Today, cyber capabilities are essential for nation-states and armed forces that want to be treated as credible players**.** Cyberspace, the fifth dimension of warfare, has already become an important arena of world politics, especially since we are living in a time in which the lines between war and peace have blurred. The digital world has become a domain where strategic advantage can be either lost or won.¶ To succeed in the cyber domain is not merely a question of defense, even if we would like to think of it that way – at least not for the nation-states. Naturally, defense capabilities have to be as preventive as possible in order to reduce the effectiveness of the adversary´s – whoever it might be –cyber attack. However, despite the best defensive efforts, intrusions will occur. In the cyber domain, you must also be resilient, i.e. have the ability to withstand attacks and failures, to mitigate harm, more so than what is needed in other domains. Creating cyber defense capabilities and resilience are fairly easy for the public to accept. But they are not enough. Deterrence is also needed, that is, the capabilities and policies to convince others not to launch a cyber attack against you. Deterrence will only be effective if you can build and demonstrate offensive cyber capabilities. To put it clearly: cyber offensive capabilities are an essential element for nation-states to succeed in the current and future reality of both international and security policies. Defense, resilience, and offense contribute to a country’s overall ability to protect itself. You need them all.¶ From nuclear to cyber deterrence¶ Deterrence theory was developed in the 1950s, primarily to address the new strategic challenges posed by nuclear weapons. During the Cold War, nuclear deterrence was able to keep the United States and the Soviet Union in check. Nuclear deterrence was the art of convincing an enemy not to take a specific action by threatening it with intolerable punishment or unacceptable failure. The theory worked well**.**¶ Based on that logic, cyber deterrence should play a similar role in the digitalized world. However, the anonymity, the advantage of attacks, and the global reach and interconnectedness greatly reduce the efficiency of cyber deterrence. At the same time, there are suspicion and rumors surrounding the kind of capabilities others have and how they are already using those capabilities.¶ In the kinetic world, it is much simpler to evaluate an opponent’s capabilities. It is typically quite easy to accurately estimate how many tanks, interceptors, or submarines a given country possesses. Countries also openly expose their arsenal, in military parades for example, or their operational skills, by organizing large military exercises. In the logic of deterrence, even more important than having the actual capability is the perception of having that capability.

#### Reactors won’t meltdown

**NEI 12**, Nuclear Energy Institute, “U.S. Reactors Add Safety Equipment”, Spring, http://www.nei.org/resourcesandstats/publicationsandmedia/insight/insightspring2012/us-reactors-add-safety-equipment/

The U.S. nuclear energy industry has implemented a far-reaching program to ensure that America’s 104 reactors will remain safe even if a site loses electrical power for an extended period. Even though a nuclear energy facility generates electricity, it depends on power from the grid to operate. As one lesson learned from last year’s accident at Japan’s Fukushima Daiichi nuclear energy facility, all U.S. nuclear energy companies have ordered pumps, generators, fire trucks and other portable equipment to provide electricity and cooling capability in an extreme event. The industry also will develop regional centers stocked with safety equipment and supplies that can be rushed to a reactor site, if needed. “We can provide an indefinite supply of electrical power, enabling plant operators to prevent fuel damage,” said Anthony Pietrangelo, senior vice president and chief nuclear officer at the Nuclear Energy Institute. The loss of electricity to power reactor cooling systems after the 2011 earthquake and tsunami resulted in damage to four reactors at the Fukushima Daiichi plant on Japan’s coastline. When a massive earthquake struck the facility, the reactors shut down safely, but the ensuing tsunami disabled backup generators and left the plant without power to cool the reactors. The fuel overheated and melted, which led to the release of radiation. The U.S. nuclear energy industry’s lessons learned from that event focus on ensuring backup supplies of power and cooling after an extreme event of any kind. “We said, never mind how we got there, never mind debating how likely it could be or how extreme it could be,” said Charles Pardee, chief operating officer for Exelon Generation and chairman of the industry’s Fukushima Response Steering Committee. Instead, the industry’s diverse and flexible coping approach, or “FLEX,” focuses on preventing the loss of power and cooling. All U.S. energy companies that operate reactors have ordered backup portable equipment to position at strategic locations on site and at regional centers. FLEX is designed to meet new requirements from the U.S. Nuclear Regulatory Commission on emergency equipment.

#### Impact is inevitable- their author

Lendman 11
– Research Associate of the Centre for Research on Globalization (Stephen, 03/ 13, “Nuclear Meltdown in Japan,” http://www.thepeoplesvoice.org/TPV3/Voices.php/2011/03/13/nuclear-meltdown-in-japan)

Further, the combined effects of allowable radiation exposure, uranium mining, milling operations, enrichment, and fuel fabrication can be devastating to those exposed. Besides the insoluble waste storage/disposal problem, nuclear accidents happen and catastrophic ones are inevitable. Inevitable Meltdowns Caldicott and other experts agree they're certain in one or more of the hundreds of reactors operating globally, many years after their scheduled shutdown dates unsafely. Combined with human error, imprudently minimizing operating costs, internal sabotage, or the effects of a high-magnitude quake and/or tsunami, an eventual catastrophe is certain. Aging plants alone, like Japan's Fukushima facility, pose unacceptable risks based on their record of near-misses and meltdowns, resulting from human error, old equipment, shoddy maintenance, and poor regulatory oversight. However, under optimum operating conditions, all nuclear plants are unsafe. Like any machine or facility, they're vulnerable to breakdowns, that if serious enough can cause enormous, possibly catastrophic, harm.

#### Timeframe is 200 years and adaptation solves

**Mendelsohn 9** – Robert O. Mendelsohn 9, the Edwin Weyerhaeuser Davis Professor, Yale School of Forestry and Environmental Studies, Yale University, June 2009, “Climate Change and Economic Growth,” online: <http://www.growthcommission.org/storage/cgdev/documents/gcwp060web.pdf>

These statements are largely alarmist and misleading. Although climate change is a serious problem that deserves attention, society’s immediate behavior has anextremely low probabilityof leading tocatastrophic consequences. The science and economics of climate change is quite clear that emissions over the next few decades will lead to only mild consequences. The severe impacts predicted by alarmists require a century (or two in the case of Stern 2006) of no mitigation. Many of the predicted impacts assume there will be no or little adaptation. The net economic impacts from climate change over the next 50 years will be small regardless. Most of the more severe impacts will take more than a century or even a millennium to unfold and many of these “potential” impacts will never occur because people will adapt. It is not at all apparent that immediate and dramatic policies need to be developed to thwart long‐range climate risks. What is needed are long‐run balanced responses.

#### It’s too late

Andreas **Souvaliotis 12** (3-20, “Is It Too Late to Change Climate Change?” <http://www.huffingtonpost.ca/andreas-souvaliotis/climate-change_b_1365449.html>

The alarm bells were going off 20 years ago at the Rio Summit but few of us were listening. Six years ago, Al Gore raised the volume much higher with his film and we started paying a lot more attention, but we still didn't do much about it. And now the evidence is mounting that we might, in fact, be too far gone already. Climate change is happening much faster than we anticipated; feedback loops are kicking in everywhere, totally dwarfing any of our own greenhouse gas contributions. Skyrocketing property damage from climate volatility is obliterating livelihoods, panicking insurance companies, and draining government funds. And the OECD just released a frightening study this week, suggesting that our constant debate, dithering, and lack of real response are now setting us up for a severe economic and lifestyle nosedive in the coming decades. Maybe some of the cynics are right: No matter how much we curb our emissions now, the damage is already done and the climate will continue to destabilize. Maybe that whole "mitigation" concept was pure fantasy and we were a few decades too late. But should we just give up, enjoy the irresponsible partying a little bit longer, and then simply brace ourselves for whatever comes next -- or should we refocus our attention and energy on the things we can still affect?

#### ecosystems are resilient

**NIPCC 11**. Nongovernmental International Panel on Climate Change. Surviving the unprecedented climate change of the IPCC. 8 March 2011. http://www.nipccreport.org/articles/2011/mar/8mar2011a5.html

In a paper published in *Systematics and Biodiversity*, Willis *et al*. (2010) consider the IPCC (2007) "predicted climatic changes for the next century" -- i.e., their contentions that "global temperatures will increase by 2-4°C and possibly beyond, sea levels will rise (~1 m ± 0.5 m), and atmospheric CO2will increase by up to 1000 ppm" -- noting that it is "widely suggested that the magnitude and rate of these changes will result in many plants and animals going extinct," citing studies that suggest that "within the next century, over 35% of some biota will have gone extinct (Thomas *et al*., 2004; Solomon *et al*., 2007) and there will be extensive die-back of the tropical rainforest due to climate change (e.g. Huntingford *et al*., 2008)." On the other hand, they indicate that some **biologists and climatologists have pointed out that "many of the predicted increases in climate have happened before, in** terms of **both magnitude and rate of change** (e.g. Royer, 2008; Zachos et al., 2008), and yet **biotic communities** have **remained remarkably resilient** (Mayle and Power, 2008) **and in some cases thrived** (Svenning and Condit, 2008)." But they report that those who mention these things are often "placed in the 'climate-change denier' category," although the purpose for pointing out these facts is simply to present "a sound scientific basis for understanding biotic responses to the magnitudes and rates of climate change predicted for the future through using the vast data resource that we can exploit in fossil records." Going on to do just that, **Willis** et al**. focus on "intervals in time in the fossil record when atmospheric CO2 concentrations increased up to 1200 ppm, temperatures in mid- to high-latitudes increased by greater than 4°C within 60 years, and sea levels rose by up to 3 m higher than present,"** **describing studies of past biotic responses that indicate "the scale and impact of the magnitude and rate of such climate changes on biodiversity**." And **what emerges** from those studies, as they describe it, "**is evidence for rapid community turnover, migrations, development of novel ecosystems and thresholds from one stable ecosystem state to anoth**er." And, most importantly in this regard, they report "**there is** very little **evidence for broad-scale extinctions due to a warming world.**" In concluding, the Norwegian, Swedish and UK researchers say that "based on such evidence **we urge some caution in assuming broad-scale extinctions of species will occur due solely to climate changes of the magnitude and rate predicted for the next centur**y," reiterating that "**the fossil record indicates remarkable biotic resilience to wide amplitude fluctuations in climate."**

#### \*\*China overwhelms

Richard **Heinberg**, senior fellow, "China Coal Update," Post Carbon Institute, 3--8--**12**, <http://www.postcarbon.org/blog-post/747521-china-coal-update>, accessed 4-9-12.

Second, can the world save itself from a climate apocalypse unless China leads the way? Talk of “climate justice” (which emphasizes the higher per-capita emissions of wealthy nations) is all well and good, but the harsh reality is that even drastic emissions cuts by the US will mean relatively little unless China also cuts soon and fast. So far, indications are that Beijing is keeping the carbon pedal to the metal, despite concurrent efforts to become a world leader in renewable energy. Barring a dramatic global emissions policy breakthrough, resource limits and economic contraction seem to offer the main hope for keeping climate change to merely “catastrophic” levels.

### Solvency

#### Restricting ability to use force causes Israeli panic

Malka 11 Haim Malka is deputy director and senior fellow in the Middle East Program at CSIS and#34;Uncertain Commitment: Israeli Assessments of US Powerand#34; csis.org/files/publication/110613\_malka\_CapacityResolve\_Web.pdf

Israelis believe the United States is projecting weakness in a region that has no mercy for the weak. The Israeli elite do not doubt U.S. power and military capabilities as much as they question how the United States will use its assets to shape regional trends and events that directly affect Israeli interests. They fear that America’s political influence is declining and its unwillingness to use unilateral military action to solve regional threats will come at their expense. Moreover, U.S. demands for the ouster of the Egyptian president, Hosni Mubarak, a longtime ally and pillar of regional stability, stunned many Israelis who fear that U.S. support for popular Arab protests fundamentally destabilizes the region. Israeli assessments reflect a deep sense of uncertainty and anxiety over the trajectory of U.S. policy and its potential impact on Israeli security and interests. More specifically, Israelis see America’s unwillingness to threaten Iran with military force not only strengthening Iran’s resolve but making a nuclear-armed Iran inevitable. The United States has the capability to stop Iran’s nuclear weapons program, but Israelis doubt whether the United States has the “stomach” for such a fight. The question lies at the center of Israeli strategic calculations, and in many ways Israelis see U.S. resolve on Iran as the test of U.S. global power. They fear the United States will fail the test, leaving Israel alone to face the burden of a nuclear Iran. Although most Israelis are confident that the United States will remain the world’s dominant military power for the foreseeable future, many see rising powers like China, Russia, and Turkey increasingly challenging U.S. policy on a range of issues. Some even point to the slow evolution of a multipolar international order in which the United States has less influence to shape trends and outcomes. This poses serious diplomatic constraints for Israel, which relies on strong U.S. diplomatic support, especially in international forums. Israelis fear a U.S. shift toward multilateralism may become irreversible and will further deepen their own international isolation. More broadly, U.S. indecision and passivity raise fundamental Israeli questions about the longterm U.S. commitment to Israel’s security. For nearly half a century, America has sustained a level of political and military support that has guaranteed Israel’s security. If U.S. support is in doubt, then Israeli decisionmakers believe they will have to rely even more on their own military strength and assets to protect Israeli interests. The consequences could be destabilizing for both Israel and the United States. Obama’s Worldview As most Israelis see it, America’s passivity stems largely from President Barack Obama’s strategic orientation, which emphasizes multilateralism and dialogue over unilateral military action and traditional alliances.1 The president’s talk of engagement with U.S. adversaries and his outreach to the Muslim world early in his presidency contrasted sharply with the language of preemptive force and unilateralism with which Israelis identified during the George W. Bush years. Israelis had grown accustomed to U.S. presidents showering them with attention and friendship. The contrast was stark, and it created a deep uncertainty about how Obama’s different approach would affect Israel. Bush’s friendship and strong moral support were reassuring to Israelis. His public affection for Ariel Sharon, whom he called a “man of peace,” complemented strategic outlooks that saw Israel’s battle against Hamas and Hezbollah as the same as the U.S. war against al Qaeda. Bush’s warm embrace eased Israeli concerns about the negative strategic consequences of his policies, many of which undermined Israeli interests. Bush’s democratization policy helped bring Hamas to power in 2006, and the execution of the war in Iraq raised many questions about U.S. judgment and capability in the Middle East. The release of the National Intelligence Estimate in November 2007, which concluded that Iran had halted its nuclear weapons program in 2003, was another blow to Israeli confidence that the Bush administration was taking the Iranian threat seriously. But for all of Bush’s strategic shortcomings, Israelis took comfort not only in his unflinching support but also in his projection of U.S. strength. To most Israelis, President Obama is different. He displays an inherent sympathy for a vague notion of global equality that has shaped his attitudes toward the Israeli-Palestinian conflict and, more important, toward the U.S.-Israeli relationship. Whereas George W. Bush unapologetically identified with Israel’s challenges, Barack Obama sympathizes with both the Palestinian and Israeli narratives. The president’s early position on the siege of Gaza, his public demand for a settlement construction freeze, and his Cairo speech were three critical moments that shaped Israeli attitudes and perceptions of Obama in his first half year in office. The encounter was tense from President Obama’s first days in office. Obama celebrated his inauguration in the aftermath of the Israel-Hamas war, which clouded an unprecedented occasion in U.S. history. Two days later at the State Department the president announced a new peace envoy to promote Israeli-Palestinian talks. More alarming for many Israelis, his talk about Palestinian suffering in Gaza seemed to hint at a nuanced shift in policy toward the Hamas-controlled territory as he declared, “As part of a lasting cease-fire, Gaza’s border crossings should be open to allow the flow of aid and commerce, with an appropriate monitoring regime. . . .”2 That was just the beginning. The Palestinian issue and Israeli settlement construction quickly became key sources of bilateral tension between the Obama administration and Netanyahu government. President Obama’s approach to restarting direct talks by focusing on an Israeli settlement construction freeze in the West Bank and East Jerusalem was seen by many Israelis as not only overly ambitious and idealistic, but ultimately counterproductive. Ironically, even those Israelis who supported negotiations toward a Palestinian state believed that U.S. actions made an agreement less likely.3 More egregious for many Israelis was the Obama administration’s argument that the IsraeliPalestinian conflict was undermining broader U.S. security and national interests, a concept that Israelis overwhelmingly rejected. “The absence of peace between Palestinians and Israelis is an impediment to a whole host of other areas of increased cooperation and more stable security for people in the region, as well as the United States,” Obama said.4 Israelis became fixated on this “linkage” that Obama and his national security team articulated between the Israeli-Palestinian conflict and America’s broader interests in the Middle East.5 This idea later spurred a broader debate over Israel’s strategic value to the United States, which alarmed many Israelis.6 By mid-2009 the crisis of trust in U.S.-Israeli relations was unmistakable. Many Israelis were convinced that the Obama administration was trying to orchestrate the collapse of Prime Minister Benjamin Netanyahu’s coalition in the hopes of bringing about a Kadima-led government that would be more willing to negotiate a Palestinian agreement. In an interview with National Public Radio, President Obama explicitly admitted that he was taking an approach to Israel different from that of his predecessors. “Part of being a good friend is being honest,” he said. “And I think there have been times where we are not as honest as we should be about the fact that the current direction, the current trajectory, in the region is profoundly negative, not only for Israeli interests but also U.S. interests.”7 The interview was a rare display of public frankness in U.S.-Israeli dialogue. It deepened Israeli concerns that President Obama sought to fundamentally change the relationship. Then came the president’s Cairo speech, which marked a turning point that convinced many Israelis that President Obama was intent on rebuilding U.S. ties with the Muslim world at their expense and that he was hostile toward Israel and Israeli interests. The speech equated Jewish suffering in the Nazi Holocaust with Palestinian suffering and displacement. For Israelis the Cairo speech was a double blow: not only did it raise Palestinian displacement on equal moral ground with the Holocaust, but the president, who was only 250 miles from Tel Aviv, chose not to visit Israel. Despite these concerns, most Israeli critics could not point to any concrete examples of how President Obama’s approach directly undermined their security or interests. Indeed, despite unprecedented political tension during the first 18 months of the Obama administration, strategic cooperation continued growing as the president pledged additional funds for Israeli defense systems and granted Israel access to the F-35 Joint Strike Fighter, which the Bush administration delayed. While the majority was critical, dissenting Israeli voices took a more balanced approach, and some Israeli government professionals privately acknowledged that President Obama’s outreach to the Muslim world made sense from the U.S. perspective and that it was counterproductive for Israelis to raise such loud protests regarding U.S. policy.8 Such sentiment was the exception, and relations deteriorated further still. In March 2010 Vice President Joseph Biden visited Israel to reassure Israelis and repair ties. Instead, the Jerusalem Planning Committee issued an ill-timed announcement that Israel would build 1,600 housing units for Jewish families in East Jerusalem, which sparked a major political crisis between the two governments. In the aftermath both sides recognized that such deep political tension was counterproductive, and they worked hard to repair damaged ties. President Obama firmly backed Israel’s position after the Gaza flotilla incident and announced plans to provide an additional $205 million to fund Israel’s development of the Iron Dome short-range rocket defense system.9 In July 2010, President Obama warmly welcomed Prime Minister Netanyahu to the White House and publicly reinforced his administration’s commitment to Israel’s security. Prime Minister Netanyahu seemed to grudgingly accept America’s strategy for confronting Iran through United Nations Security Council (UNSC) sanctions, and some commentators argued that U.S. and Israeli positions on Iran were converging.10 Most important, the strong relationship built between Admiral Michael G. Mullen, chairman of the Joint Chiefs of Staff, and Gabi Ashkenazi, then chief of the General Staff of the Israel Defense Forces (IDF), played a crucial role in maintaining close strategic cooperation during a period of heightened political tension. Yet, if Israelis had grown more accustomed to President Obama toward the close of 2010, their public criticisms reemerged during the waves of public protest that swept Tunisia and then Egypt in January and February 2011. Many Israelis blamed Obama for supporting the ouster of Hosni Mubarak as president of Egypt. For three decades Mubarak had been one of Israel’s most important strategic partners and anchor of regional stability. Mubarak’s departure created a new set of uncertainties for Israeli policymakers. More broadly, they feared that the president’s support for popular Arab uprisings would create hostile regimes on Israel’s borders and beyond. In a public gathering, Amos Gilead, director for political-military affairs at Israel’s Ministry of Defense, expressed Israeli concerns, stating, “Look around the Middle East: If there is a democratic process here, it will bring, for sure, hell.”11 Ramifications for Israel Ongoing Israeli mistrust of President Obama’s policy approach directly influences Israeli policy debates in three critical ways. First, if Israeli decisionmakers believe the United States is reluctant to use force, or at least the threat of force, to solve regional security threats—most importantly stopping Iran’s nuclear weapons program—then it raises the urgency of decisive and perhaps even unilateral actions to protect Israeli interests. Second, Israelis believe U.S. policy is facilitating a slow evolution toward a multilateral international order, where the United States is increasingly constrained diplomatically and challenged by regional powers. Third, U.S. policy fuels Israeli doubts about America’s reliability as a strategic ally and raises difficult questions about its longterm commitment to Israel’s security. The deep uncertainty has significant ramifications not only for Israeli decisionmaking but for U.S. interests as well.

The plan’s perception of non-commitment radicalizes Israeli foreign policy and causes greater self-reliance

Malka 11 Haim Malka is deputy director and senior fellow in the Middle East Program at CSIS and#34;Uncertain Commitment: Israeli Assessments of US Powerand#34; csis.org/files/publication/110613\_malka\_CapacityResolve\_Web.pdf

More broadly, U.S. indecision and passivity raise fundamental Israeli questions about the longterm U.S. commitment to Israel’s security. For nearly half a century, America has sustained a level

of political and military support that has guaranteed Israel’s security. If U.S. support is in doubt,

then Israeli decisionmakers believe they will have to rely even more on their own military strength

and assets to protect Israeli interests. The consequences could be destabilizing for both Israel and

the United States.

#### That ensures miscalc and triggers biological and nuclear war

Beres 11 Louis René Beres is a professor of Political Science at Purdue University, an expert on Israeli security matters and the author of 10 major books and several hundred journal articles on international relations and international law. and#34;The unforeseen risks of Palestinian statehoodand#34; 6/9/11www.haaretz.com/print-edition/opinion/the-unforeseen-risks-of-palestinian-statehood-1.382766

In turn, such self-reliance would demand: (1) a more comprehensive and explicit nuclear strategy involving refined deterrence, preemption and war fighting capabilities; and (2) a corresponding and thoroughly updated conventional war strategy. The birth of Palestine could affect these two interpenetrating strategies in several important ways. Immediately, it would enlarge Israel's need for what military strategists call "escalation dominance" - namely, the capacity to fully determine sequential moves toward greater destructiveness. By definition, as any Palestinian state would make Israel's conventional capabilities far more complex and problematic, the Israel Defense Forces' national command authority would now need to make the country's still-implicit nuclear deterrent less ambiguous. Taking the presumed Israeli Bomb out of the "basement," could enhance Israel's overall security for a while; but over time, ending "deliberate ambiguity" could also heighten the chances of nuclear weapons use. With a Palestinian state in place, a nuclear war could arrive in Israel not only as a "bolt-from-the-blue" surprise missile attack, but also as a result, intended or inadvertent, of escalation. If an enemy state were to begin with "only" conventional and/or biological attacks upon Israel, Jerusalem might respond, sooner or later, with fully nuclear reprisals. Alternately, if this enemy state were to begin with solely conventional attacks upon Israel, Jerusalem's conventional reprisals might still be met, in the uncertain strategic future, with enemy nuclear counterstrikes

#### Only trust in US stops Israeli attack on Iran

Birnbaum 9/12/13, Ben Birnbaum is a writer living in Israel. http://www.newrepublic.com/article/114691/israel-strike-iran-how-obamas-syria-waffling-makes-it-more-likely

The second misconception is that there is a meaningful debate within the Israeli government and security establishment about whether to attack Iran’s nuclear program. There is not. Virtually all top Israeli officials agree that given the choice between “bomb or bombing,” bombing is the lesser of two evils. The debate instead has been over whether Israel has more time to wait for other measures to take their toll or whether, by waiting too long, it risks allowing Iran to enter what former defense minister Ehud Barak called the “zone of immunity,” when the Iranian nuclear program would be beyond Israel’s military reach. There are a number of factors at play here, from the amount of uranium Iran possesses to the number and quality of centrifuges, not to mention the measures Iran is taking to hide and fortify its program. But the major question before Israel has always been whether it could trust the U.S.—with its superior military capabilities—to strike in the event that its own window of military opportunity closes.

#### Attack on Iran causes extinction

Hindustan Times 9/24/12 http://www.hindustantimes.com/world-news/RestOfAsia/World-War-III-may-erupt-if-Israel-attacks-Iran-official/Article1-934709.aspx

A top Iranian official has said a World War III may erupt if his country is attacked by Israel, concerned over Tehran's controversial nuclear programme. Brigadier general Amir-Ali Hajizadeh, commander of the Aerospace Division of Iran's Islamic Revolution Guards Corps (IRGC), told Press TV that in case of the eruption of such a war, the situation would be out of control. "This war is likely to degenerate into the World War III," Hajizadeh was quoted as saying. Stating that some countries might enter the war in favour of or against Iran, the official said: "We see the US and the Zionist regime (of Israel) alongside one another and we can by no means imagine that the Zionist regime would initiate a war (against Iran) without US support." "The Islamic Republic of Iran considers US bases in the region as part of American soil and will definitely target them if a war breaks out," he added.

#### 1. Plan not enough—international efforts key

Oona A. Hathaway et al., 2012 (Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel, The Law of Cyber-Attack, [100 Calif. L. Rev. 817, 844 (2012)](http://www.lexisnexis.com.ezp1.lib.umn.edu/lnacui2api/mungo/lexseestat.do?bct=A&risb=21_T17852526755&homeCsi=7346&A=0.810545954009541&urlEnc=ISO-8859-1&&citeString=100%20Calif.%20L.%20Rev.%20817,at%20844&countryCode=USA&_md5=00000000000000000000000000000000), L/N)

Cyber-attacks on vital infrastructure are already becoming widespread. Cyber-security professionals report that the computer infrastructure has become more vulnerable even in just a year. [n331](http://www.lexisnexis.com.ezp2.lib.umn.edu/lnacui2api/frame.do?tokenKey=rsh-20.600841.7197208486&target=results_DocumentContent&returnToKey=20_T17900625919&parent=docview&rand=1375411392497&reloadEntirePage=true#n331) And yet, while the threat of cyber-  [\*885]  attacks has rapidly grown, the response has not kept pace. This Article has shown that both the U.S. government and the international community have thus far largely failed to update legal frameworks that might respond to cyber-attacks. To face new and growing threats, governments continue to rely on limited and piecemeal bodies of law not designed to meet the challenge of cyber-attacks.

It is past time to begin a conversation about the scope of the threat posed by cyber-attacks and the best ways to meet it. The United States should expand the reach of domestic law abroad and develop a system for utilizing limited countermeasures where appropriate to respond to certain types of cyber-attacks. Yet the United States is restricted in what it can accomplish alone. Cyber-attacks are often transnational - designed by authors in multiple countries, run through networks across the world, and used to undermine computer systems in countries where those designing the attack have never set foot. This global threat may only be effectively met by a global solution - by the international community working together to design a new law for cyber-attacks.

#### \*2. Alt Causes

#### \*A. Patriotic hackers

Owens et al 9

(William A. Owens, as an Admiral in the United States Navy and later Vice Chairman of the Joint Chiefs of Staff, \*\*Kenneth W. Dam, served as Deputy Secretary of the Treasury from 2001 to 2003, where he specialized in international economic development, \*\*Herbert S. Lin, Senior Scientist and Study, “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities” 4/27/2009, <http://www.lawfareblog.com/wp-content/uploads/2013/01/NRC-Report.pdf>)

Past experience strongly indicates that conflict or increased tension between two nations will result in the “patriotic hackers” of both nations (and perhaps their allies) taking action intended to harass or damage the other side. Such activities are not under the direct control of the national government, and as discussed in Section 7.2.3.3 may well interfere with the efforts of that government to manage the crisis vis-à-vis the other side.4 Indeed, the government of a targeted nation is likely to believe that a cyberattack conducted on it is the result of deliberate adversarial action rather than the actions of “unauthorized” parties. Thus, unauthorized activities of the patriotic hackers of Zendia against the United States may lead the United States to believe that the Zendian government has launched a cyberattack against it. A U.S. cyberattack against Zendia may be seen by the Zendian government as a cyber first strike against it. Yet another complication involving patriotic hackers is the possibility that they might be directed by, inspired by, or tolerated by their government (or a rogue section within it), but in ways in which the government’s hand is not easily visible. Under such circumstances, hostile acts with damaging consequences could continue to occur (with corresponding benefits to the nation responsible) despite official denials. At the very least, the possibility that patriotic hackers may be operating could act as a plausible cover for government-sponsored cyberattacks, even if there were in fact no patriotic hackers doing anything.

#### \*B. Lack of doctrine

Mark Young, Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence, 2010 (Journal of National Security Law & Policy, 4 J. Nat'l Security L. & Pol'y 173, Cybersecurity Symposium: National Leadership, Individual Responsibility: National Cyber Doctrine: The Missing Link in the Application of American Cyber Power, L/N)

Not only does each of the military services have its own personnel dedicated to cyber operations, but also - despite the lack of a unified U.S. government cyber doctrine - each of the individual armed forces has a disparate information operations doctrine and elements that manage and defend their information networks. In accordance with the doctrine, all of the armed forces view cyber operations as tools to affect the cognitive processes of adversaries. The majority of soldiers, sailors, airmen, and marines continue to see cyber operations only as an element to be governed by their service information operations doctrine. As noted by Director of the National Security Agency Keith Alexander, "the only doctrine that currently addresses operations within the cyberspace environment is contained within two subsets of information operations (IO) computer network operations and electronic warfare (EW)." n28 The individual armed forces computer network operations doctrines are incomplete. They fail to delineate the fundamental principles by which the services manage their computer network activities in support of national objectives. This lack of appropriate doctrine has not prevented the Departments of the Army, Navy, and Air Force from establishing individual organizations to address cyberspace issues. Similar to the DoD and the Cyber Command, the services have established these organizations without any governing principles. This lack of a government-wide cyber doctrine creates a potential for inadequate and ineffective responses to cyber threats. The outdated, maladapted doctrine and the various armed forces doctrines create confusion and could compromise highly sensitive attack techniques. The current doctrine lacks adequate interoperability principles to govern a joint cyber force. "In addition, different organizational structures are being implemented within each service to address this rapidly evolving source of both military opportunity and threat vulnerability. Further complicating the issue, "different voices within the individual Services present diverse visions of the role of cyberpower and of the Service's role ... within that vision." n29 These different voices may generate incompatible directives and result in the services managing their forces in an entirely inadequate and [\*181] incompatible manner. In a time of shrinking budgets and growing threats, cyber coordination must improve within the national security sector. Without a properly coordinated doctrine, the Cyber Command's capabilities might first be tested during an actual national emergency. Such a crisis may highlight the inadequacy of the command's organizational structure, gaps in its roles and missions, or insufficient intelligence authorities. Critical elements, "such as intelligence, logistics, airspace control, space operations, etc.," have yet to be addressed in any joint authoritative directives. n30 All DoD elements must acknowledge the realities of an environment that provides a powerful advantage but also presents significant vulnerabilities.

#### 3. Executive will ignore and/or courts will circumvent

Stephen Dycus (Proffesor at Vermont Law School) August 11 2010 “Congress’s Role in Cyber Warfare,” <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>

Congress’s active role in the development and implementation of cyber ¶ warfare policy is no guarantee of national security. The policy might be ¶ flawed in various ways. There is also a risk that whatever policy is adopted ¶ will not be properly executed or that its execution will have unintended ¶ results. The policy might be misunderstood or might not provide clear or ¶ appropriate guidance in the urgent circumstances facing its interpreter. The ¶ person charged with implementing the policy might make a mistake – for ¶ example, by interpreting a potential enemy’s electronic espionage as an ¶ attack. Available cyber weaponry might not work as planned. Or a purely ¶ defensive move by U.S. operators might be construed by another nation as ¶ offensive, and provoke an attack. Nor can the clearest policy, statutory or ¶ executive, guarantee compliance by an Executive determined to ignore it.71¶ The rules might be construed by the President in a way that reduces the ¶ importance of Congress’s role. Or they might be challenged in court.

#### 4. Doesn’t Solve – too fragmented

Clarke and Knake 2012 (Richard (former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States) and Robert (Cybersecurity and homeland security expert at the Council on Foreign Relations), Cyber War: The Next Threat to National Security and What to Do About It, Harper Collins Books, 2012, http://indianstrategicknowledgeonline.com/web/Cyber%20War%20-%20The%20Next%20Threat%20to%20National%20Security%20and%20What%20to%20Do%20About%20It%20(Richard%20A%20Clarke)%20(2010).pdf)

Congress is a federation of fiefdoms, subject to the vicissitudes of constant fund raising and the lobbying of those who have donated the funds. That situation has two adverse consequences with regard to congressional involvement in cyber war oversight. First, everyone wants his or her own fiefdom.

Congress has resisted any suggestion, such as was made by Senator Bob Bennett (Republican of Utah), that there be one committee authorized to examine cyber security. As a result there are approximately twenty-eight committees and subcommittees involved in the issue and none with jurisdiction to think holistically. Second, Congress “eschews regulation” and spits it out. The influential donors from the information technology, electric power, pipeline, and telecommunications industries have made the idea of serious cyber security regulations as remote as public financing of congressional campaigns or meaningful limits on campaign contributions.

#### 5. Plan doesn’t restrain the Executive

Lorber 2013(Eric, J.D. Candidate at the University of Pennsylvania Law School, and Ph. D candidate at Duke University, January, "Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?”, Journal of Constitutional Law, Vol. 15:3)

The lack of congressional oversight of offensive cyber operations under the Intelligence Authorization Act also likely does not seriously shift the balance between congressional and executive war-making powers. The reason is inherent in the limitations of the legislation itself: the Intelligence Authorization Act specifies reporting requirements, but does not require the non-use or withdrawal of forces.234 Further, these reports must be made in a “timely” fashion (the definition of which is undefined) and only to a small number of Congressmen (at most eight).235 Thus even if the President had to report offensive cyber operations to Congress, it is unclear he would have to do so in a way that gave Congress an effective check, as these reports would be made only to a small group of Congressmen (who would not be able to share the information, because of its classified nature, with other members of the legislature) and could be done well after the employment of these capabilities. The resulting picture is one of increased presidential flexibility; the War Powers Resolution and the Intelligence Authorization Act—while arguably ineffective in many circumstances—provide increased congressional oversight of presidential war-making actions such as troop deployments and covert actions. Yet these statutes do not cover offensive cyber operations, giving the President an increasingly powerful foreign policy tool outside congressional reach.

#### 6. US bans on offense weapons don’t dissuade other countries

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

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

# 2NC

## Cp

### PP Lx

**Statutory restriction kill pres powers**

**Restrictions snowball – partisanship**

Gary **Schmitt**, director of the Program on Advanced Strategic Studies, 1-13-**2009**, “The Myth of the (Bush) Imperial Presidency” AEI, http://www.aei.org/article/foreign-and-defense-policy/defense/the-myth-of-the-bush-imperial-presidency/

Since the 1970s there has been a good deal of confusion about the appropriate division of powers under the Constitution when it comes to foreign and defense affairs.[21] The Bush White House has been right in principle to push back against the idea that Congress is either its equal in this policy area or that it has the power to define exactly how a president may exercise his authorities. But could it have been more adroit in how it went about making that case? Almost certainly.[22] The cost has been new laws and new Supreme Court decisions that, instead of upholding precedents and authorities friendly to the exercise of presidential power, have begun to curtail them. Whether the issue is one of electronic surveillance, military commissions, due process rights for detainees, or even interrogation techniques, what the president once might have gotten without much compromise has become a partisan issue in which the president is given less discretion. Again, it is understandable why the administration took the positions it did. What is less certain is whether it was prudent to do so.

### A2 Syria

#### Presidential powers high – consulting Congress over Syria maximized Obama’s power

Posner 9-3 – Eric Posner, “Obama Is Only Making His War Powers Mightier,” SLATE, 9-3-13. http://www.slate.com/articles/news\_and\_politics/view\_from\_chicago/2013/09/obama\_going\_to\_congress\_on\_syria\_he\_s\_actually\_strengthening\_the\_war\_powers.html

President Obama’s surprise announcement that he will ask Congress for approval of a military attack on Syria is being hailed as a vindication of the rule of law and a revival of the central role of Congress in war-making, even by critics. But all of this is wrong. Far from breaking new legal ground, President Obama has reaffirmed the primacy of the executive in matters of war and peace. The war powers of the presidency remain as mighty as ever. It would have been different if the president had announced that only Congress can authorize the use of military force, as dictated by the Constitution, which gives Congress alone the power to declare war. That would have been worthy of notice, a reversal of the ascendance of executive power over Congress. But the president said no such thing. He said: “I believe I have the authority to carry out this military action without § Marked 16:04 § specific congressional authorization.” Secretary of State John Kerry confirmed that the president “has the right to do that”—launch a military strike—“no matter what Congress does.” Thus, the president believes that the law gives him the option to seek a congressional yes or to act on his own. He does not believe that he is bound to do the first. He has merely stated the law as countless other presidents and their lawyers have described it before him. The president’s announcement should be understood as a political move, not a legal one. His motive is both self-serving and easy to understand, and it has been all but acknowledged by the administration. If Congress now approves the war, it must share blame with the president if what happens next in Syria goes badly. If Congress rejects the war, it must share blame with the president if Bashar al-Assad gases more Syrian children. The big problem for Obama arises if Congress says no and he decides he must go ahead anyway, and then the war goes badly. He won’t have broken the law as he understands it, but he will look bad. He would be the first president ever to ask Congress for the power to make war and then to go to war after Congress said no. (In the past, presidents who expected dissent did not ask Congress for permission.) People who celebrate the president for humbly begging Congress for approval also apparently don’t realize that his understanding of the law—that it gives him the option to go to Congress—maximizes executive power vis-à-vis Congress. If the president were required to act alone, without Congress, then he would have to take the blame for failing to use force when he should and using force when he shouldn’t. If he were required to obtain congressional authorization, then Congress would be able to block him. But if he can have it either way, he can force Congress to share responsibility when he wants to and avoid it when he knows that it will stand in his way. This approach also empowers the president relative to Congress by giving him the ability to embarrass members of Congress when he wants to. Just ask Hillary Clinton, whose vote in favor of the 2003 Iraq War damaged her chances against Barack Obama in 2008, and the Democratic senators who could not enter the 1992 campaign for the presidency because their votes against the 1991 Iraq War rendered them unelectable. The best thing for individual members of Congress is to be able to carp on the sidelines—to complain about not being consulted and to blame the president if the war goes badly. That is why David Axelrod said, “Congress is now the dog that caught the car.” This is hardball politics, not a rediscovery of legal values.

## Case

### No Cyber

We don’t have to prove that a cyber attack is impossible, just that high costs will cause enemies to seek alternatives

Rid, reader in war studies – King's College London, and McBurney, professor – Agents and Intelligent Systems Group – Department of Informatics @ King's College, ‘12 (Thomas and Peter, “Cyber-Weapons,” *The RUSI Journal* Volume 157, Issue 1, p. 6-13)

A thorough conceptual analysis and a detailed examination of the empirical record corroborates our hypothesis: developing and deploying potentially destructive cyber-weapons against hardened targets will require significant resources, hard-to-get and highly specific target intelligence, and time to prepare, launch and execute an attack. Attacking secured targets would probably require the resources or the support of a state actor; terrorists are unlikely culprits of an equally unlikely cyber-9/11. The scant empirical record also suggests that the greatest benefit of cyber-weapons may be using them in conjunction with conventional or covert military strikes, as Israel did when it blinded the Syrian air defence in 2007. This leads to a second conclusion: the cost-benefit payoff of weaponised instruments of cyber-conflict may be far more questionable than generally assumed: target configurations are likely to be so specific that a powerful cyber-weapon may only be capable of hitting and acting on one single target, or very few targets at best. The equivalent would be a HARM missile that can only destroy one unique emitter, not a set of targets emitting at the same frequency. But in contrast to the missile – where only the seeker needs to be specifically reprogrammed and the general aviation and propulsion systems remain functional – the majority of modular components of a potent cyber-weapon, generic and specific, would have a rather short shelf-life after discovery. Two findings contravene the debate's received wisdom. One insight concerns the dominance of the offence. Most weapons may be used defensively and offensively. But the information age, the argument goes since at least 1996, has ‘offence-dominant attributes’.37 A 2011 Pentagon report on cyberspace again stressed ‘the advantage currently enjoyed by the offense in cyberwarfare’.38 But when it comes to cyber-weapons, the offence has higher costs, a shorter shelf-life than the defence, and a very limited target set.39 All this drastically reduces the coercive utility of cyber-attacks. Any threat relies on the offender's credibility to attack, or to repeat a successful attack. Even if a potent cyber-weapon could be launched successfully once, it would be highly questionable if an attack, or even a salvo, could be repeated in order to achieve a political goal. At closer inspection cyber-weapons do not seem to favour the offence. A second insight concerns the risk of electronic arms markets. One concern is that sophisticated malicious actors could resort to asymmetric methods, such as employing the services of criminal groups, rousing patriotic hackers, and potentially redeploying generic elements of known attack tools. Worse, more complex malware is likely to be structured in a modular fashion. Modular design could open up new business models for malware developers. In the car industry, for instance,40 modularity translates into a possibility of a more sophisticated division of labour. Competitors can work simultaneously on different parts of a more complex system. Modules could be sold on underground markets. But if our analysis is correct, potential arms markets pose a more limited risk: the highly specific target information and programming design needed for potent weapons is unlikely to be traded generically. To go back to our imperfect analogy: paintball pistols will continue to be commercially available, but probably not pre-programmed warheads of smart missiles.

#### That’s a key framing issue—the context of cyberwar requires you to evaluate it’s probability, not it’s magnitude—their experts agree

Cavelty, October 22, 2012 (Myriam Dunn, The Militarisation of Cyber Security as a Source of Global Tension, <http://isn.ch/Digital-Library/Articles/Special-Feature/Detail/?lng=en&id=153888&tabid=1453349960&contextid774=153888&contextid775=153887> )

Since the potentially devastating effects of cyber attacks are so scary, the temptation is very high not only to think about worst-case scenarios, but also to give them a lot of (often too much) weight despite their very low probability. However, most experts agree that strategic cyber war remains highly unlikely in the foreseeable future, mainly due to the uncertain results such a war would bring, the lack of motivation on the part of the possible combatants, and their shared inability to defend against counterattacks. Indeed, it is hard to see how cyber attacks could ever become truly effective for military purposes: It is exceptionally difficult to take down multiple, specific targets and keep them down over time. The key difficulty is proper reconnaissance and targeting, as well as the need to deal with a variety of diverse systems and be ready for countermoves from your adversary. Furthermore, nobody can be truly interested in allowing the unfettered proliferation and use of cyber war tools, least of all the countries with the offensive lead in this domain. Quite to the contrary, strong arguments can be made that the world’s big powers have an overall strategic interest in developing and accepting internationally agreed norms on cyber war, and in creating agreements that might pertain to the development, distribution, and deployment of cyber weapons or to their use (though the effectiveness of such norms must remain doubtful). The most obvious reason is that the countries that are currently openly discussing the use of cyber war tools are precisely the ones that are the most vulnerable to cyber warfare attacks due to their high dependency on information infrastructure. The features of the emerging information environment make it extremely unlikely that any but the most limited and tactically oriented instances of computer attacks could be contained. More likely, computer attacks could ‘blow back’ through the interdependencies that are such an essential feature of the environment. Even relatively harmless viruses and worms would cause considerable random disruption to businesses, governments, and consumers. This risk would most likely weigh much heavier than the uncertain benefits to be gained from cyber war activities. Certainly, thinking about (and planning for) worst-case scenarios is a legitimate task of the national security apparatus. Also, it seems almost inevitable that until cyber war is proven to be ineffective or forbidden, states and non-state actors who have the ability to develop cyber weapons will try to do so, because they appear cost-effective, more stealthy, and less risky than other forms of armed conflict. However, cyber war should not receive too much attention at the expense of more plausible and possible cyber problems. Using too many resources for high- impact, low-probability events – and therefore having less resources for the low to middle impact and high probability events – does not make sense, neither politically, nor strategically and certainly not when applying a cost-benefit logic.

#### No credible evidence confirms cyber risk—just conflation of threats

Jon R. Lindsay, 2013 (Stuxnet and the Limits of Cyber Warfare, Security Studies, Volume 22, Issue 3, 2013)

In the absence of evidence of strategic cyber warfare, many look to industrial accidents to illustrate its lethal potential. Gen. Keith Alexander, commander of us Cyber Command and the National Security Agency, points to events like Russia's Sayano-Shushenskaya dam catastrophe of 2009. In this instance a computer operator five hundred miles away mistakenly sent a command to start a hydro-turbine generator then undergoing maintenance; this human error resulted in a flood that killed seventy-five people and ruined eight of the remaining turbines. 29 Such examples are meant to show that because ics accidents can and do happen, they could also be triggered intentionally via cyber attack. They tell us little, however, about how hard or easy it is to cause such failures predictably at will, an important distinction between an unforeseen accident and a controlled attack, let alone the conditions under which it would make sense to employ such a weapon against an actual adversary. In the universe of cybersecurity, therefore, we observe a high frequency of low intensity cyber attacks resulting in computer crime, espionage, and hacktivism, but a remarkably low frequency of high intensity cyber warfare resulting in serious infrastructure damage. Thus in order to describe the phenomenon of cyber warfare, most Cyber Revolution proponents must either speculate deductively from the assumed properties of cyber technology or inductively through analogy with more prevalent cyber irritants. The first rhetorical option risks ignoring the effects of strategic context while the second risks ignoring the effects of increasing scale and complexity. As we shall see in the case of Stuxnet, context and complexity matter tremendously. In all of the diverse discourse on cyber warfare, three related beliefs about cyber warfare are often assumed but rarely evaluated. us Deputy Secretary of Defense William J. Lynn III lists them all in a recent article describing Pentagon cyber strategy: (1) “cyberwarfare is asymmetric,” (2) “the offense has the upper hand”, and (3) “deterrence models of assured retaliation do not apply to cyberspace, where it is difficult and time consuming to identify an attack's perpetrator.” 30 Before evaluating these propositions, I will first briefly summarize the conventional wisdom on each.

#### Their authors are paid off

Bruce Schneier, 12/21/10 (Book Review: Cyber War, Schneier on Security, <http://www.schneier.com/blog/archives/2010/12/book_review_cyb.html>)

Cyber War is a fast and enjoyable read. This means you could give the book to your non-techy friends, and they'd understand most of it, enjoy all of it, and learn a lot from it. Unfortunately, while there's a lot of smart discussion and good information in the book, there's also a lot of fear-mongering and hyperbole as well. Since there's no easy way to tell someone what parts of the book to pay attention to and what parts to take with a grain of salt, I can't recommend it for that purpose. This is a pity, because parts of the book really need to be widely read and discussed.

The fear-mongering and hyperbole is mostly in the beginning. There, the authors describe the cyberwar of novels. Hackers disable air traffic control, delete money from bank accounts, cause widespread blackouts, release chlorine gas from chemical plants, and -- this is my favorite -- remotely cause your printer to catch on fire. It's exciting and scary stuff, but not terribly realistic. Even their discussions of previous "cyber wars" -- Estonia, Georgia, attacks against U.S. and South Korea on July 4, 2009 -- are full of hyperbole. A lot of what they write is unproven speculation, but they don't say that.

Better is the historical discussion of the formation of the U.S. Cyber Command, but there are important omissions. There’s nothing about the cyberwar fear being stoked that accompanied this: by the NSA's General Keith Alexander -- who became the first head of the command -- or by the NSA's former director, current military contractor, by Mike McConnell, who’s Senior Vice President at Booz Allen Hamilton, and by others. By hyping the threat, the former has amassed a lot of power, and the latter a lot of money. Cyberwar is the new cash cow of the military-industrial complex, and any political discussion of cyberwar should include this as well.

### Warming

#### Warming irreversible - past the tipping point

Spaeth, 12/5/12 [“Why it's probably too late to roll back global warming”, Ryu,The Week News, <http://theweek.com/article/index/237392/why-its-probably-too-late-to-roll-back-global-warming>]

Two degrees Celsius. According to scientists, that's the rise in global temperature, measured against pre-industrial times, that could spark some of the most catastrophic effects of global warming. Preventing the two-degree bump has been the goal of every international treaty designed to reduce greenhouse gas emissions, including a new one currently being [hammered out](http://www.washingtonpost.com/business/ap-interview-un-chief-says-rich-countries-caused-climate-change-must-take-lead-in-fixing-it/2012/12/05/e7f5be46-3eb9-11e2-8a5c-473797be602c_story.html) at a United Nations summit in Doha, Qatar. But a new study published by the journal Nature Climate Change [shows](http://www.huffingtonpost.com/2012/12/02/climate-change-study-emissions_n_2228646.html) that it's incredibly unlikely that global warming can be limited to two degrees. According to the study, the world in 2011 "pumped nearly 38.2 billion tons of carbon dioxide into the air from the burning of fossil fuels such as coal and oil," [says Seth Borenstein at The Associated Press](http://www.huffingtonpost.com/2012/12/02/climate-change-study-emissions_n_2228646.html): The total amounts to more than 2.4 million pounds (1.1 million kilograms) of carbon dioxide released into the air every second. Because emissions of the key greenhouse gas have been rising steadily and most carbon stays in the air for a century, it is not just unlikely but "rather optimistic" to think that the world can limit future temperature increases to 2 degrees Celsius (3.6 degrees Fahrenheit), said the study's lead author, Glen Peters at the Center for International Climate and Environmental Research in Oslo, Norway. What happens when the two-degree threshold is crossed? Most notably, that's when the polar ice caps will begin to [melt,](http://www.nationaljournal.com/magazine/it-s-already-too-late-to-stop-climate-change-20121129) leading to a dangerous rise in sea levels. Furthermore, the world's hottest regions will be unable to grow food, setting the stage for mass hunger and global food inflation. The rise in temperature would also likely exacerbate or cause extreme weather events, such as hurricanes and droughts. There is a very small chance that the world could pull back from the brink. The U.N. could still limit warming to two degrees if it adopts a "radical plan," [says Peters' group](http://www.carbonbrief.org/blog/2012/12/can-we-still-limit-warming-to-two-degrees). According to a PricewaterhouseCoopers study, such a plan would entail cutting carbon emissions "by 5.1 percent every year from now to 2050, essentially slamming the breaks on growth starting right now," [says Coral Davenport at The National Journal](http://www.nationaljournal.com/magazine/it-s-already-too-late-to-stop-climate-change-20121129), "and keeping the freeze on for 37 years." However, the U.N. has set a deadline of ratifying a new treaty by 2015, and implementing it by 2020, which means the world is already eight years behind that pace. There are still major [disagreements](http://www.washingtonpost.com/business/ap-interview-un-chief-says-rich-countries-caused-climate-change-must-take-lead-in-fixing-it/2012/12/05/e7f5be46-3eb9-11e2-8a5c-473797be602c_story.html) between the U.S. and China over whether the developed world, which industrialized first, should bear the bulk of the cost of reducing carbon emissions. And there is, of course, a large contingent of Americans who don't even believe climate change exists,

putting any treaty's ratification at risk. Climate change is so politically toxic in America that Congress has prioritized the [fiscal cliff](http://dyn.politico.com/printstory.cfm?uuid=19D2674D-7D85-4BDC-B63E-E75C9D26AA3A) over — no exaggeration — untold suffering and the end of the world as we know it. In other words, it isn't happening. And if that's not bad enough, keep in mind that the two-degree mark is just the beginning, [says Davenport](http://www.nationaljournal.com/magazine/it-s-already-too-late-to-stop-climate-change-20121129): Michael Oppenheimer, a professor of geosciences and international affairs at Princeton University and a member of the Nobel Prize-winning U.N. Intergovernmental Panel on Climate Change, says that a 2-degree rise is not itself that point, but rather the beginning of irreversible changes. "It starts to speed you toward a tipping point," he said. "It's driving toward a cliff at night with the headlights off. We don't know when we'll hit that cliff, but after 2 degrees, we're going faster, we have less control. After 3, 4, 5 degrees, you spiral out of control, you have even more irreversible change." Indeed, at the current emissions rate, the world is expected to broach the four-degree mark by [2100](http://www.carbonbrief.org/blog/2012/12/can-we-still-limit-warming-to-two-degrees) — at which point, we can expect even worse environmental catastrophes.

# 1NR

### Debt: Overview 2NC

#### B. Timeframe ---- collapse by November if we don’t raise the debt ceiling

Sahadi 9/10 Jeanne, “Debt ceiling 'X date' could hit Oct. 18”, <http://money.cnn.com/2013/09/10/news/economy/debt-ceiling-bills-coming-due/index.html>, MCR

A new analysis by a think tank shows that **Washington's drop-dead deadline for the debt ceiling could hit as soon as Oct. 18**.¶ Estimating exactly when the Treasury Department will be unable to pay all the bills coming due if Congress fails to raise the nation's legal borrowing limit is notoriously difficult.¶ That's why, in an analysis released Tuesday, the Bipartisan Policy Center put the "X date" between Oct. 18 and Nov. 5.¶ Treasury Secretary Jack Lew has warned that **by mid-October the agency will have only $50 billion in cash on top of incoming revenue.**¶That may sound like a lot. But, as the Bipartisan Policy Center details, **it won't last very long**.¶ If the "X" date turns out to be Oct. 18, Treasury would run about $106 billion short of the money it owes between then and Nov.15. That means it wouldn't be able to pay the equivalent of a third of all the bills due during that period.¶ Here's why: Treasury handles about 80 million payments a month. Those payments are not evenly spaced out so on some days more is owed than on others. And the revenue flowing into federal coffers is unpredictable and varies from day to day.¶ Payments include IRS refunds, Social Security and veterans benefits, Medicare reimbursements for doctors and hospitals, bond interest owed investors, payments to contractors and paychecks for federal workers and military personnel.¶ If Congress fails to act in time, Treasury will have to make difficult -- and legally questionable -- decisions about who should get paid and who should be stiffed. It may decide to pay some bills in full and on time and not others.¶ Or it may decide to delay all payments due on a given day until it has sufficient revenue on hand to pay in full. in a Treasury Inspector General's report that this might be the most plausible and least harmful approach.¶ But under that scenario, **delays would grow over time from a day or two to several weeks**. For example, the payments due to seniors, veterans and active duty military personnel on Nov. 1 wouldn't go out until Nov. 13.¶ In any case, the expectation is that the agency will try to prioritize payments to bond investors over everyone else, lest the financial markets go haywire. Politically, of course, that carries risk, said Steve Bell, the senior director of the Bipartisan Policy Center's economic policy project.¶ "There's a political danger you'll be accused of paying bondholders over Social Security recipients," Bell said.¶ On both Oct. 23 and Nov. 14, $12 billion in Social Security benefits come due, while another $25 billion comes due on Nov. 1, according to the analysis.¶ Meanwhile, on Oct. 24, Treasury will have to roll over $57 billion in outstanding debt and another $115 billion on Oct. 31. Normally that's not a problem, because U.S. Treasury auctions attract a lot of buyers willing to purchase bonds at low rates.¶ But if those rollover dates come after the "X" date, and **the perception is that the United States is defaulting on some of its obligations, Treasury could have trouble finding enough buyers or investors could demand higher interest rates**.¶ The debt ceiling is currently set at $16.7 trillion. That ceiling was reached on May 19, and ever since Treasury has been using a host of special measures to keep the country's borrowing at or below that ceiling. But those measures will be exhausted by mid-October, according to Treasury.¶ If lawmakers want to raise the ceiling enough to get past the 2014 midterm elections in November, the Bipartisan Policy Center estimates they will have to raise it by $1.1 trillion to $17.8 trillion. To top of page

#### D. Turn – Gov shutdown allows cyber attacks

Eric **Chabrow**, Executive Director of Gov Info and Security, 4-7-**2011**, “Feds Face Infosec Challenges in Shutdown,” http://www.govinfosecurity.com/articles.php?art\_id=3512

A government **shutdown would** not only **cause a reduction in available staff,** **there would also** likely **be a** temporary **shutdown of** some **IT systems**, **creating a crisis of prioritization and the possibility that federal cyber security may suffer**. Regardless of well established contingency plans each federal agency maintains, the simple fact that **there will be fewer government employees at their posts** inherently **means there will be an increased level of vulnerability to federal networks**. "Because there are not enough people watching as there was before, **the risk profile will be higher if there's a** **government shutdown**," said the national director of U.S. Cyberchallenge, Karen Evans. The white House estimates that **more than three-quarters of a million federal workers may be off the job** if Congress fails to pass funding legislation by midnight Friday, but there are no official estimates of how many information networks may also be affected by a partial government shutdown. According to GovInfoSecurity, both the Office of Management and Budget and the Department of Homeland Security refused the opportunity to comment directly on the possible impact a shutdown might have on federal cyber security. The DHS did however issue an optimistic statement earlier this week regarding the likelihood there will even be a shutdown, and reitterated the fact that there are contingency plans for such an event in place. "As a matter of course, DHS plans for contingencies. In fact, since 1980, all agencies and departments have had to have a plan in case of a government shutdown, and these plans are updated routinely. All of this is beside the point since, as the bipartisan congressional leadership has said on a number of occasions and as the president has made clear, **no** **one anticipates** or wants **a** government **shutdown**," the DHS stated. **Others familiar with the possible effect a shutdown may have on federal cyber security were not** as **optimistic**, such as former **Interior** **Department Chief** Information Officer W. Hord **Tipton**, currently the executive director of the IT certification and education organization (ISC)2. "**When we put ourselves in state of chaos like this,** and this is what it will be, **think of the opportunities for striking through the APTs** (advanced persistent threats), **they can pick and choose the targets with much less security behind them,"** said Tipton.

### Line By Line

#### Causes nuclear war, turns warming and heg

O’Hanlon 12 — Kenneth G. Lieberthal, Director of the John L. Thornton China Center and Senior Fellow in Foreign Policy and Global Economy and Development at the Brookings Institution, former Professor at the University of Michigan, served as special assistant to the president for national security affairs and senior director for Asia on the National Security Council, holds a Ph.D. from Columbia University, and Michael E. O'Hanlon, Director of Research and Senior Fellow in Foreign Policy at the Brookings Institution, Visiting Lecturer at Princeton University, Adjunct Professor at Johns Hopkins University, holds a Ph.D. from Princeton University, 2012 (“The Real National Security Threat: America's Debt,” *Los Angeles Times*, July 10th, Available Online at http://www.brookings.edu/research/opinions/2012/07/10-economy-foreign-policy-lieberthal-ohanlon)

Lastly, American economic weakness undercuts U.S. leadership abroad. Other countries sense our weakness and wonder about our purported decline. If this perception becomes more widespread, and the case that we are in decline becomes more persuasive, countries will begin to take actions that reflect their skepticism about America's future. Allies and friends will doubt our commitment and may pursue nuclear weapons for their own security, for example; adversaries will sense opportunity and be less restrained in throwing around their weight in their own neighborhoods. The crucial Persian Gulf and Western Pacific regions will likely become less stable. Major war will become more likely. When running for president last time, Obama eloquently articulated big foreign policy visions: healing America's breach with the Muslim world, controlling global climate change, dramatically curbing global poverty through development aid, moving toward a world free of nuclear weapons. These were, and remain, worthy if elusive goals. However, for Obama or his successor, there is now a much more urgent big-picture issue: restoring U.S. economic strength. Nothing else is really possible if that fundamental prerequisite to effective foreign policy is not reestablished.

### Debt Uq: Will Pass 2NC

#### Debt ceiling will pass now—business lobby

Hartman, 9/19, (“Business lobby says don't shut down the government!”, 9/19/2013, <http://www.thomhartmann.com/forum/2013/09/business-lobby-says-dont-shut-down-government>)

Even the business lobbyists are against a government shutdown. The U.S. Chamber of Commerce is taking aim at House Republicans, and urging them to stop playing games with our economy. The Chamber's top lobbyist, Bruce Josten, said, “It is not in the best interest of the U.S. business community, or the American people, to risk even a brief government shutdown that might trigger disruptive consequences.” In a letter to to members, the Chamber called on the House to pass a three-month stopgap measure to keep government spending at current levels. Mr. Josten wrote, “It is readily apparent none of these important issues are ripe for resolution. We therefore urge the House to act promptly to pass a Continuing Resolution to fund the government and raise the debt ceiling, and then return to work on these other vital issues.” The U.S. Chamber of Commerce usually sides with big business, even when business interests collide with the will of the American people. But, the Chamber of Commerce knows that a government shutdown will hurt families and corporations alike. Hopefully, this warning will breakthrough to Republicans.

#### Will Pass—using health care as a bargaining chip won’t work

National Review, 9/19, (“Lowry: House Will Pass Clean Debt Limit Raise”, 9/19/2013, <http://www.nationalreview.com/corner/359030/lowry-house-will-pass-clean-debt-limit-raise-nro-staff>)

The effort to use the debt ceiling as leverage to defund Obamacare will come to naught, National Review editor Rich Lowry said tonight. During an appearance on Special Report’s All-Star Panel, Lowry predicted that the House would eventually pass a “clean” debt limit raise despite drama in the Senate related to the effort to defund Obamacare. “It goes to the Senate, there’ll be some theatrics, Harry Reid will strip out the defunding from the [continuing resolution], it’ll go back to the House and probably end up passed in a clean version,” Lowry said.

### PC Debate

#### Syria puts PC on the brink

Garrett, 9/19/13 - National Journal Correspondent-at-Large and Chief White House Correspondent for CBS News (Major, National Journal, “A September to Surrender: Syria and Summers Spell Second-Term Slump” <http://www.nationaljournal.com/all-powers/a-september-to-surrender-syria-and-summers-spell-second-term-slump-20130917>)

There are no “obstructionist” Republican fingerprints on the conspicuous and power-depleting defeats for Obama. He never sought a vote on Syria and therefore was not humiliated. The same is true for Summers. But Obama lost ground on both fronts and ultimately surrendered to political realities that, for the first time in his presidency, were determined by his own obdurate party.

This does not mean Obama will lose coming fights over the sequester, shutdown, or debt ceiling. But he is visibly weaker, and even his sense of victory in Syria is so unidimensional, it has no lasting sway in either Democratic cloakroom. More important, Democrats are no longer afraid to defy him or to disregard the will of their constituents—broadly defined in the case of Syria; activist and money-driving in the case of Summers. This, of course, indirectly announces the beginning of the 2016 presidential campaign and an intra-party struggle over the post-Obama Democratic matrix.

This shift—a tectonic one—will give Republicans new opportunities on the fiscal issues and in coming debates over immigration and implementation of Obamacare. Republicans have never known a world where Democratic defections were so unyielding and damaging.

This does not mean Republicans will find a way to exploit these fissures. The GOP’s current agony over delaying or defunding Obamacare and the related shambling incoherence around the sequester/shutdown/debt ceiling suggest not.

#### Obama pushing to raise the debt ceiling

Reuters 9/18 (Mark Felsenthal and Roberta Rampton, Washington, 9/18/13, “Obama asks leaders to push Congress to raise debt limit”, http://www.reuters.com/article/2013/09/18/us-usa-economy-obama-idUSBRE98H0BT20130918, zzx)

(Reuters) - President Barack Obama appealed to business leaders on Wednesday to urge Congress to approve an increase in the U.S. debt limit without any conditions attached and avoid a default that is possible as early as mid-October. "It is going to be important for all of you over the next several weeks to understand what's at stake and to make sure that you are using your influence in whatever way we can to get back to what used to be called regular order around here," Obama told the Business Roundtable. The president's speech to about 100 top corporate executives was part of an effort to focus on domestic budget and economic issues after a month dominated by foreign policy, mainly the conflict in Syria.

### Debt Impact: Economy Internals

#### Even delaying to raise the debt ceiling would end the recovery

Masters 13 (Jonathan, Deputy Editor at the Council on Foreign Relations, Backgrounder, jan 2 2013"US Debt Ceiling. Costs and Consequences")

Most economists, including those in the White House and from former administrations, agree that the impact of an outright government default would be severe. Federal Reserve Chairman Ben Bernanke has said a U.S. default could be a ["recovery-ending event"](http://blogs.wsj.com/economics/2011/03/01/bernanke-warns-on-debt-limit-chaos/) that would likely spark another financial crisis. Short of default, officials warn that legislative delays in raising the debt ceiling could also inflict significant harm on the economy.¶ Many analysts say congressional gridlock over the debt limit will likely sow significant uncertainty in the bond markets and place upward pressure on interest rates. Rate increases would not only hike future borrowing costs of the federal government, but would also raise capital costs for struggling U.S. businesses and cash-strapped homebuyers. In addition, rising rates could divert future taxpayer money away from much-needed federal investments in such areas as infrastructure, education, and health care.¶ The protracted and politically acrimonious debt limit showdown in the summer 2011 prompted Standard and Poor's to take the unprecedented step of downgrading the U.S. credit rating from its triple-A status, and analysts fear such brinksmanship in early 2013 could bring about similar moves from other rating agencies.¶ A 2012 study by the non-partisan Government Accountability Office estimated that [delays in raising the debt ceiling](http://www.gao.gov/products/GAO-12-701) in 2011 cost taxpayers approximately $1.3 billion for FY 2011. BPC estimated the ten-year costs of the prolonged fight at roughly $19 billion.¶ The stock market also was thrown into frenzy in the lead-up to and aftermath of the 2011 debt limit debate, with the [Dow Jones Industrial Average](http://www.bizjournals.com/nashville/news/2011/08/08/slideshow-dows-10-worst-days-ever.html) plunging roughly 2,000 points from the final days of July through the first days of August. Indeed, the Dow recorded one of its worst single-day drops in history on August 8, the day after the S&P downgrade, tumbling 635 points.¶ Speaking to the [Economic Club of New York](http://www.reuters.com/article/2012/11/20/idUSW1E8KA00A20121120) in November 2012, Fed Chairman Ben Bernanke warned that congressional inaction with regard to the fiscal cliff, the raising of the debt ceiling, and the longer-term budget situation was creating uncertainty that "appears already to be affecting private spending and investment decisions and may be contributing to an increased sense of caution in financial markets, with adverse effects on the economy."

#### Destroys the global economy

DAVIDSON 9 – 15 – 13 co-founder and co-host of Planet Money, a co-production of the NYT and NPR [Adam Davidson, Our Debt to Society, <http://www.nytimes.com/2013/09/15/magazine/our-debt-to-society.html?pagewanted=all&_r=1&>]

The Daily Treasury Statement, a public accounting of what the U.S. government spends and receives each day, shows how money really works in Washington. On Aug. 27, the government took in $29 million in repaid agricultural loans; $75 million in customs and duties; $38 million in the repayment of TARP loans; some $310 million in taxes; and so forth. That same day, the government also had bills to pay: $247 million in veterans-affairs programs; $2.5 billion to Medicare and Medicaid; $1.5 billion each to the departments of Education and Defense. By the close of that Tuesday, when all the spending and the taxing had been completed, the government paid out nearly $6 billion more than it took in. This is the definition of a deficit, and it illustrates why the government needs to borrow money almost every day to pay its bills. Of course, all that daily borrowing adds up, and we are rapidly approaching what is called the X-Date — the day, somewhere in the next six weeks, when the government, by law, cannot borrow another penny. Congress has imposed a strict limit on how much debt the federal government can accumulate, but for nearly 90 years, it has raised the ceiling well before it was reached. But since a large number of Tea Party-aligned Republicans entered the House of Representatives, in 2011, raising that debt ceiling has become a matter of fierce debate. This summer, House Republicans have promised, in Speaker John Boehner’s words, “a whale of a fight” before they raise the debt ceiling — if they even raise it at all. 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.

### Cleanup

#### China overwhelms—emits more than the US and swamps prevention efforts—that’s Heinberg

#### No modeling--even if it happens it won’t be big enough or fast enough because an international agreement is key

**Pielke**, Professor Enviro Studies U of Colorado, 8-6-**’12** (Roger, “Climate of Failure” Foreign Policy, <http://www.foreignpolicy.com/articles/2012/08/06/climate_of_failure>)

The heady days of early 2009, when advocates for global action on climate change anticipated world leaders gathering later that year around a conference table in Copenhagen to reach a global agreement, are but a distant memory. Today, with many of these same leaders focusing their attention on jumpstarting economic growth, environmental issues have taken a back seat. For environmentalists, it may seem that climate policy has dropped from the political agenda altogether. They're right. The world's biggest emitters have reached a consensus of sorts, but not the one hoped for in Copenhagen. In the United States, President Barack Obama has borrowed his energy policy -- "all of the above" -- from the Republicans. Europe has dithered on any further commitments to emissions reductions as governments have been completely consumed by the euro crisis. China and India have used the follow-on conferences to Copenhagen, held in Durban and Cancun, to decisively push international climate negotiations into the long weeds. Leaders' attention to climate policy is not coming back -- at least not in any form comparable to the plans being discussed just a few years ago. Copenhagen will likely be remembered as the moment when advocates for action lost their innocence. For more than a decade, expectations had been raised for a grand global bargain to put a price on carbon that would compel a major reduction in greenhouse-gas emissions -- notably carbon dioxide -- over the coming decades. To understand why this bargain failed requires a basic understanding of where carbon dioxide comes from and how it is reduced. A very simple but powerful framework for such an understanding was proposed in the 1980s by Japanese scientist Yoichi Kaya. Kaya explained that future carbon dioxide emissions would be the product of four factors: population, economic activity, how we obtain our energy, and how we use that energy. We can simplify these four factors even further. Population and income together are simply GDP, or aggregate economic activity, and the production and consumption of energy reflect the technologies of energy supply and demand. The resulting Kaya Identity -- as his equation has come to be called -- simply says: Emissions = GDP x Technology With this simple equation before us, we can see the fundamental challenge to reducing emissions: A rising GDP, all else equal, leads to more emissions. But if there is one ideological commitment that unites nations and people around the world in the early 21st century, it is that GDP growth is non-negotiable. Right now, leaders on six different continents are focused on efforts to grow GDP, and with it jobs and wealth. They're not as worried about emissions. If you spend any time in the midst of the climate debate, it won't be long before you will be assailed by those who would like to argue that economic growth is unnecessary or even wrong, and stopping it is a key to reducing emissions. I hear these arguments mostly from wealthy liberal academics in posh university towns across the richer parts of the world. Noted environmental activist Bill McKibben, for example, frequently makes the case that "growth may be the one big habit we finally must break," and he is far from a lone voice. But of course, no candidate has ever secured political office on an anti-growth platform. One has to live in a thickly insulated bubble to think that stopping or reversing growth could ever be a feasible way to reduce emissions. So what's the solution, then? The Kaya Identity tells us that instead of GDP, the focus must be on technology, and here the math is surprisingly simple. Stabilizing the level of carbon dioxide in the atmosphere would require more than 90 percent of the energy we consume to come from carbon-free sources like nuclear, wind, or solar. Policymakers often discuss reducing annual emissions by 80 percent from 1990 levels. But emissions today are already more than 45 percent higher than in 1990, so that higher level implies a need to cut by more than 90 percent from today's levels. Put another way, in round numbers, we could keep at most 10 percent of our current energy supply, and 90 percent or more would have to be replaced with a carbon-free alternative. Today, about 10 percent of the energy that we consume globally comes from carbon-free sources -- leaving a long way to go. Frustratingly, this 90 percent threshold for carbon-free energy supply is largely independent of how much energy the world consumes. Every major projection of future energy consumption foresees growth in energy demand around the world, which makes sense when you consider that today 2 billion people or more lack basic access to energy. Energy demand is skyrocketing in China and India, and eventually will in Africa. But even letting your imagination go wild and envisioning a future world that consumes half of the energy we do today would still require that more than 80 percent of our energy supply be carbon-free. This isn't a statement about the feasibility or desirability of improved energy efficiency; it's just math. Consider this: If the goal is to stabilize the amount of carbon dioxide in the atmosphere at a low level by 2050 (in precise terms, at 450 parts per million or less), then the world would need to deploy a nuclear power plant worth of carbon free energy every day between now and 2050. For wind or solar, the figures are even more daunting. For several decades, the dominant view among climate specialists was that imposing a high price on carbon emissions -- whether through a tax or a traded permit system -- would create the economic incentive necessary to stimulate the green energy innovation needed. Unfortunately, the track record of such schemes is not encouraging. Any policy that depends for its success on creating economic stress on consumers (or voters) to motivate massive change is a policy doomed to fail. Voters typically respond to higher energy prices by voting out of office any politician or party who is perceived to be working against their economic interests. Supporters of carbon pricing have no good answer for the politics. Australia has tried to get around this problem by subsidizing its relatively low carbon tax with broader income-tax reform -- that is, the government is returning to consumers more money than is collected by the tax. But the policy still remains wildly unpopular, with 38 percent of the public feeling worse off under the tax and only 5 percent feeling better off one month after its introduction, despite consistent strong support for non-specific action on climate. Or consider Germany, where the government, having expressed a desire to shut down nuclear and fossil-fuel power altogether, is quickly waking up to reality. German politicians have begun to realize that their present choices are more carbon-intensive fossil fuel, more nuclear, or letting the lights go out. The impotence of the European Emissions Trading Scheme, due to an excess of tradable permits resulting from the economic downturn, actually creates incentives for more coal -- in 2012, black coal consumption is expected to increase by 13.5 percent. The Economist recently concluded that for Germany, "Greenhouse-gas emissions are likely to be higher than they would have been [without the nuclear shutdown] for quite a while to come." Efforts to secure a high carbon price to create incentives for change still have staunch advocates in the environmental community, despite the little evidence that it can work. Advocates for carbon pricing typically argue that the costs are low or even nonexistent. The typical basis for such claims is an economic model that projects net costs over the better part of a century, with claims of low costs based on that aggregated, hypothetical sum. Such models, often laden with dodgy assumptions -- such as predictions of the magnitude and pace of future technological innovation in energy -- offer little solace to the politician who runs for election every two years and whose political fortunes hinge on the actual short-term costs. The evidence that a high carbon tax is politically infeasible seems irrefutable, based on experience and common sense. Yet, even so, to try to push the debate forward, advocates constantly seek to demonstrate that climate change is taking place with high tangible costs, as if to try to rebalance the cost-benefit math. Such efforts to stoke alarm have no apparent limit, no matter how tenuous the science. For instance, even though scientists, including the Intergovernmental Panel on Climate Change (IPCC), have observed that the magnitude of drought in the central United States has actually decreased over the past century, there has been a rush to attribute the 2012 drought solely to human causes. Thomas Homer-Dixon, a Canadian economist, cheered on the drought and its devastation, writing "It sounds harsh, but in light of these realities, this year's U.S. drought is good news ... fears about imperiled food security may be our best hope for breaking through widespread climate-change denial and generating the political pressure to do something."

No scenario for attacks on nuclear power plants – their evidence is about attacks on nuclear weapons

#### No meltdown impact—their authors are hacks.

Rod **Adams 12**, Former submarine Engineer Officer, Founder, Adams Atomic Engines, Inc., “Has Apocalyptic Portrayal of Climate Change Risk Backfired?”, May 2, <http://atomicinsights.com/2012/05/has-apocalyptic-portrayal-of-climate-change-risk-backfired.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+AtomicInsights+%28Atomic+Insights%29>

Not only was the discussion enlightening about the reasons why different people end up with different opinions about climate change responses when presented with essentially the same body of information, but it also got me thinking about a possible way to fight back against the Gundersens, Caldicotts, Riccios, Grossmans and Wassermans of the world. That group of five tend to use apocalyptic rhetoric to describe what will happen to the world if we do not immediately start turning our collective backs on all of the benefits that abundant atomic energy can provide. They spin tall tales of deformed children, massive numbers of cancers as a result of minor radioactive material releases, swaths of land made “uninhabitable” for thousands of years, countries “cut in half”, and clouds of “hot particles” raining death and destruction ten thousand miles from the release point. Every one of those clowns have been repeating similar stories for at least two solid decades, and continue to repeat their stories even after supposedly catastrophic failures at Fukushima have not resulted in a single radiation related injury or death. According to eminent scientists – like Dr. Robert Gale – Fukushima is unlikely to EVER result in any measurable increase in radiation related illness. One important element that we have to consider to assess cancer risks associated with an accident like Fukushima is our baseline risk for developing cancer. All of us, unfortunately, have a substantial risk of developing cancer in our lifetime. For example, a 50-year-old male has a 42% risk of developing cancer during his remaining life; it’s almost the same for a 10-year-old. This risk only decreases when we get much older and only because we are dying of other causes. It’s true that excess radiation exposure can increase our cancer risk above baseline levels; it’s clear from studies of the survivors of the 1945 atomic bombings of Hiroshima and Nagasaki, of people exposed to radiation in medical and occupational settings, and of people exposed to radon decay products in mines and home basements. When it comes to exposures like that of Fukushima, the question is: What is the relative magnitude of the increased risk from Fukushima compared to our baseline cancer risk? Despite our fears, it is quite small. If the nuclear industry – as small and unfocused as it is – really wanted to take action to isolate the apocalyptic antinuclear activists, it could take a page from the effective campaign of the fossil fuel lobby. It could start an integrated campaign to help the rest of us to remember that, despite the dire predictions, the sky never fell, the predicted unnatural deaths never occurred, the deformations were figments of imagination, and the land is not really irreversibly uninhabitable for generations. The industry would effectively share the story of Ukraine’s recent decision to begin repopulating the vast majority of the “dead zone” that was forcibly evacuated after the Chernobyl accident. It would put some context into the discussion about radiation health effects; even if leaders shy away from directly challenging the Linear No Threshold (LNT) dose assumption, they can still show that even that pessimistic model says that a tiny dose leads to a tiny risk. Aside: My personal opinion is that the LNT is scientifically unsupportable and should be replaced with a much better model. We deserve far less onerous regulations; there is evidence that existing regulations actually cause harm. I hear a rumor that there is a group of mostly retired, but solidly credentialed professionals who are organizing a special session at the annual ANS meeting to talk about effective ways to influence policy changes. End Aside. Most of us recognize that there is no such thing as a zero risk; repeated assertions of “there is no safe level” should be addressed by accepting “close enough” to zero so that even the most fearful person can stop worrying. The sky has not fallen, even though we have experienced complete core meltdowns and secondary explosions that did some visible damage. Nuclear plants are not perfect, there will be accidents and there will be radioactive material releases. History is telling me that the risks are acceptable, especially in the context of the real world where there is always some potential for harm. The benefits of accepting a little nuclear risk are immense and must not be marginalized by the people who market fear and trembling.

#### Reactors won’t meltdown

**NEI 12**, Nuclear Energy Institute, “U.S. Reactors Add Safety Equipment”, Spring, http://www.nei.org/resourcesandstats/publicationsandmedia/insight/insightspring2012/us-reactors-add-safety-equipment/

The U.S. nuclear energy industry has implemented a far-reaching program to ensure that America’s 104 reactors will remain safe even if a site loses electrical power for an extended period. Even though a nuclear energy facility generates electricity, it depends on power from the grid to operate. As one lesson learned from last year’s accident at Japan’s Fukushima Daiichi nuclear energy facility, all U.S. nuclear energy companies have ordered pumps, generators, fire trucks and other portable equipment to provide electricity and cooling capability in an extreme event. The industry also will develop regional centers stocked with safety equipment and supplies that can be rushed to a reactor site, if needed. “We can provide an indefinite supply of electrical power, enabling plant operators to prevent fuel damage,” said Anthony Pietrangelo, senior vice president and chief nuclear officer at the Nuclear Energy Institute. The loss of electricity to power reactor cooling systems after the 2011 earthquake and tsunami resulted in damage to four reactors at the Fukushima Daiichi plant on Japan’s coastline. When a massive earthquake struck the facility, the reactors shut down safely, but the ensuing tsunami disabled backup generators and left the plant without power to cool the reactors. The fuel overheated and melted, which led to the release of radiation. The U.S. nuclear energy industry’s lessons learned from that event focus on ensuring backup supplies of power and cooling after an extreme event of any kind. “We said, never mind how we got there, never mind debating how likely it could be or how extreme it could be,” said Charles Pardee, chief operating officer for Exelon Generation and chairman of the industry’s Fukushima Response Steering Committee. Instead, the industry’s diverse and flexible coping approach, or “FLEX,” focuses on preventing the loss of power and cooling. All U.S. energy companies that operate reactors have ordered backup portable equipment to position at strategic locations on site and at regional centers. FLEX is designed to meet new requirements from the U.S. Nuclear Regulatory Commission on emergency equipment.