# 1nc

### 1nc

#### War Powers are the “Power to wage war successfully”

SCOTUS 1948 (LICHTER ET AL., DOING BUSINESS AS SOUTHERN FIREPROOFING CO., v. UNITED STATES¶ No. 105¶ SUPREME COURT OF THE UNITED STATES¶ 334 U.S. 742; 68 S. Ct. 1294; 92 L. Ed. 1694; 1948 U.S. LEXIS 2705¶ November 20-21, 1947, Argued June 14, 1948, Decided¶ PRIOR HISTORY: CERTIORARI TO THE CIRCUIT COURT OF APPEALS FOR THE SIXTH CIRCUIT. [\*](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-23.770161.6902095558&target=results_DocumentContent&returnToKey=20_T17977466602&parent=docview&rand=1376730771592&reloadEntirePage=true" \l "fnote1)¶ [\*](http://www.lexisnexis.com/lnacui2api/frame.do?tokenKey=rsh-23.770161.6902095558&target=results_DocumentContent&returnToKey=20_T17977466602&parent=docview&rand=1376730771592&reloadEntirePage=true" \l "ref1) Together with No. 74, Pownall et al. v. United States, on certiorari to the Circuit Court of Appeals for the Ninth Circuit; and No. 95, Alexander Wool Combing Co. v. United States, on certiorari to the Circuit Court of Appeals for the First Circuit, argued November 21, 1947.¶ The cases are stated concisely in the opinion with citations to the decisions below, pp. 746-753. Affirmed, p. 793.

The war powers of congress and the president are only those which are to be derived from the Constitution of the United States but the primary implication of a war power is that it shall be an effective power to wage the war successfully. While the constitutional structure and controls of our government are our guides equally in war and in peace, they must be read with the realistic purposes of the entire instrument fully in mind.

#### Restrictions are prohibitions on action --- the aff is a reporting requirement

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

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

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

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

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

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

#### Vote neg---

#### Only prohibitions on authority guarantee neg ground---their interpretation lets affs no link the best neg offense like deference

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

### 1N

#### Rhetoric of terrorist threat is the primary cause of policy overreach and economic degradation ----- must reject politicization

GARTENSTEIN-ROSS 2013 – Director of the Center for the Study of Terrorist Radicalization at the Foundation for Defense of Democracies, Associate Professor at Georgetown University (Gartenstein-Ross, Daveed, “Bin Laden’s Legacy”)

It did not have to turn out this way. On September 11, 2001, even after absorbing a dramatic terrorist strike, the United States remained the world’s unchallenged military and economic superpower. The 9/11 attacks were a clear moral outrage, and al Qaeda represented a threat to numerous governments. The outpouring of sympathy for the United States was immediate and widespread internationally, with various countries pledging their cooperation in the fight against jihadi militancy. The conventional wisdom among U.S. politicians and commentators was that al Qaeda had underestimated America’s resolve: the vigorous response to come would test, and almost certainly overwhelm, the militant group’s resiliency. The past decade of efforts has in fact degraded al Qaeda. Key leaders have been captured or killed, and it is experiencing financial trouble.19 Yet despite the harm that has been done to al Qaeda, the United States is in a far weaker position relative to the jihadi group now than it was ten years ago. There are many reasons this is so, many core errors that the United States has made. The United States has simply never taken the time to fully understand al Qaeda’s strategy: its ends, ways, and means. As a result, U.S. planners failed to comprehend two core goals that al Qaeda possessed: bleeding the U.S. economy and making its conflict with the United States as broad as possible. In part because of this failure to understand al Qaeda’s strategy, the United States ended up with a system for fighting the militant group that is almost precisely backward in three important ways. First, although a great deal of resources was devoted to the fight against jihadi militancy, these resources have been allocated in an incredibly inefficient manner. The most visible example has been airport security. In the immediate wake of 9/11, searches of airline passengers were intensified, but every effort was made to ensure that no group felt unfairly singled out. Rather than having a system that focused its resources on passengers most likely to pose a terrorist threat, we ended up with one where figures like Al Gore received unnecessary scrutiny. Gore was in fact twice singled out for extra screening during a 2002 trip to Wisconsin. A seventy-five-year-old congressman, John Dingell, was forced to strip down to his underwear in Washington, D.C.’s Reagan National Airport in January 2002 to prove that his artificial hip, and not a weapon, had set off a metal detector.20 There was, of course, a noble goal underlying the desire to avoid terrorist profiling: policy makers wanted to avoid making people (specifically, those of Arab or South Asian descent) feel unfairly singled out on the basis of their ethnicity. But there are a couple of problems with the way this concern was operationalized. There is no question that singling out someone like Al Gore—a former presidential candidate, vice president, and senator—for extra screening is a plain waste of policing resources. Even though Gore’s selection for additional screening represents only a couple of incidents, it is indicative of a broader inefficiency that, aggregated over the entire system, caused airport security to be far more resource-intensive than necessary. The other problem concerns public debates over profiling. When many pundits speak of profiling terrorists, they’re talking about racial or ethnic profiling alone. But many other factors can be incorporated into the terrorist profile that will increase the efficacy of the practice while minimizing the risk of unfairly and unnecessarily singling out any one ethnicity. The impoverished public debate on this issue has helped to constrain the range of options available to policy makers. Compounding the inefficiency of our policing efforts, immediately after 9/11, states, municipalities, and private contractors realized that a vast array of policies could be packaged as “counterterrorism” when they would have a marginal impact at best on the terrorist threat. And politicians thought they could show the public how serious they were about tackling the issue by devoting resources to these various proposals despite their marginal impact. The second major problem with the way we fight jihadi militancy has been the politicization of the fight against terrorism. Politicians’realization that they could demonstrate their bona fides on terrorism by supporting programs that had little to do with actually addressing the problem was one product of this politicization. The public clearly cared deeply about the issue—but using an issue to win a political campaign is not the same as actually addressing the problem. By making terrorism a hard-fought partisan issue, we have created a climate that produces posturing, bad policy, and squabbling that weakens the country. A third major error has been an eagerness to broaden, rather than narrow, the war on terrorism. President George W. Bush said in 2002 that “the best way to keep America safe from terrorism is to go after terrorists where they plan and hide.”21 He would later phrase this somewhat differently and more directly: “We’re taking the fight to the terrorists abroad so we don’t have to face them here at home.” Terrorist safe havens in remote parts of the world can indeed directly threaten the United States, and the war in Afghanistan was necessary rather than a war of choice. After all, al Qaeda’s safe haven in that country posed a systemic risk of another catastrophic act of terrorism against America.22 But the United States proved to be too eager to enter wars abroad, in particular the adventure in Iraq that was supposed to advance the war on terrorism but has been so costly in both blood and treasure. The decision to invade Iraq was made with little appreciation of the second-order and third-order consequences that it would produce—and little appreciation of its potential to breathe life into al Qaeda rather than bury it. Ten years after the 9/11 attacks, our enemies are correct to see the United States as weaker: economically troubled, militarily exhausted, and politically divided. Indeed, although it is difficult to precisely measure al Qaeda’s contribution to America’s grave economic woes, it is certain that these three core errors—coupled with al Qaeda’s own ingenuity and deadly competence—made America’s war against the jihadi group incredibly costly. The 9/11 attacks cost the United States at least $1 trillion through direct property damage and second-order economic consequences, including the impact on the stock market. Thereafter, budgetary outlays for the military operations in Afghanistan and Iraq that were undertaken as a response to al Qaeda’s attacks have been about $1.3 trillion. This included the cost of the operations themselves, expenditures to secure military bases, reconstruction costs, and foreign aid.23 But direct expenditures do not encompass the full cost of these operations. When second-order consequences and opportunity costs are considered, the Iraq War alone may have cost the United States more than $3 trillion.24 And then there are the costs of escalating homeland security and intelligence measures. Our response to bin Laden has been incredibly costly, and the present system is likely unsustainable. Bin Laden’s strategy for defeating the United States survives his death—and if we don’t understand what this strategy is, how it developed, and how America’s responses have been so ill-suited to defeating al Qaeda, the United States may find itself locked in combat with bin Laden’s legacy for longer than necessary. If bin Laden’s death is to truly represent a turning point in the fight against jihadi militancy, it won’t be due just to his importance to al Qaeda. Rather, it will be because his death allowed the United States to reevaluate its paradigms for protecting itself from and defeating this adversary. But to do so, it is first necessary to understand the key errors that the country has made along the way and why these mistakes occurred. How to Beat a Superpower If you know others and know yourself, you will not be imperiled in a hundred battles; if you do not know others and do not know yourself, you will be imperiled in every single battle. —Sun Tzu, The Art of War The United States has suffered for its failure to understand al Qaeda and its late leader Osama bin Laden. Before al Qaeda destroyed the Twin Towers in New York City and a large section of the Pentagon on that fateful Tuesday in September 2001, leaving almost three thousand dead on U.S. soil, few within the government paid any attention to it—this despite the fact that by the end of 2000, al Qaeda had already executed two dramatic terrorist strikes against American targets. The United States was slow to recognize the growing strategic challenge posed by nonstate actors like al Qaeda. Thus, when the U.S. was struck by the deadliest terrorist attack the world has seen, it had no plan at the ready for deposing the Taliban regime in Afghanistan that had been sheltering the jihadi group. Even after the 9/11 attacks made the threat that al Qaeda posed undeniable, the United States did little to understand the group’s strategy for defeating its superpower rival—which in turn [delayed] retarded American planning. Since then, the United States has often mistaken tactics for strategy. More problematic, the United States has committed to drastic measures—such as the invasion of Iraq, a country that had nothing to do with the 9/11 attacks—without giving sufficient thought to how doing so could strengthen its adversary. Thus, America’s failure to understand al Qaeda has made it difficult to avoid self-inflicted wounds. This chapter examines al Qaeda’s origins and shows that two major prongs of thejihadi group’s strategy—to undermine the economy of its enemy and to make the battlefield on which its war would be fought as broad as possible—were eminently knowable by the time 9/11 occurred. Bin Laden in the Afghan-Soviet War Osama bin Laden was born in the late 1950s to Mohammed bin Laden, who from humble beginnings in Yemen rose to become a mul- tibillionaire construction magnate and confidant of Saudi Arabia’s royal family. Osama had twenty-four brothers and twenty-nine sisters; his father, who practiced polygamy, had a total of twenty-two wives throughout his life. When Osama was only ten years old, Mohammed bin Laden perished in a plane crash. By all accounts, Osama was pious and religiously conservative when he was growing up in Jeddah, Saudi Arabia. One example of his religiosity in his younger years was his reprimand of a friend for wearing shorts—which bin Laden saw as immodest and religiously proscribed—to play soccer.1 Those who knew him during this period recall a shy young man, more a follower than a leader. Bin Laden rose to international prominence after the Soviet Union invaded Afghanistan in December 1979. The Soviet invasion was prompted by multiple factors, including an Islamist insurgency that threatened the country’s pro-Soviet regime, concern that the United States might deepen its role in Afghanistan after the Iranian revolution undermined U.S. regional interests, and infighting among Afghanistan’s communists that culminated in bloody internecine clashes and the assassination of the Afghan president Nur Mohammed Taraki.2 Although the Soviet general staff opposed the invasion, Leonid Brezhnev, the general secretary of the Communist Party, insisted that operations in Afghanistan would end successfully in three to four weeks.3 The war did not turn out as Brezhnev predicted. The Soviets withdrew only after nine years of costly occupation, during which they experienced stiff resistance from the Afghan mujahedin backed by the United States, Saudi Arabia, and Pakistan. The mujahedin were the beneficiaries of the largest U.S. covert aid program since the Vietnam War, with American support (totaling around $3 billion) matched dollar for dollar by Saudi Arabia. The Americans strengthened the mujahedin by providing supplies and weaponry, including Stinger missiles that helped to negate the Soviet airpower advantage. Bin Laden traveled to Pakistan in the early 1980s, soon after the Afghan-Soviet war began. Bruce Riedel, a Brookings Institution senior fellow and former CIA officer, notes that once bin Laden arrived, he became “a major financier of the mujahedin, providing cash to the relatives of wounded or martyred fighters, building hospitals, and helping the millions of Afghan refugees fleeing to the border region of Pakistan.”4 Bin Laden and a radical Palestinian cleric named Abdullah Azzam founded an organization known as the Services Bureau (maktab al khidmat), which was dedicated to integrating Arabs into the anti-Soviet struggle by placing them with relief organizations or alongside Afghan factions on the battlefield. “Azzam was the critical force both ideologically and organizationally for the recruitment of thousands of Muslims from around the world to engage in some way with the Afghan struggle against the Soviets,” writes Peter Bergen, a CNN national security analyst and astute chronicler of al Qaeda’s history. “And Azzam would become bin Laden’s mentor, the first and most important of a series of father figures that he would find to replace his own father.”5 Bin Laden’s wealth and financial generosity earned him many friends, and many wanted to curry the rich young Saudi’s favor. But it was his first trip to the front lines in Afghanistan in 1984 that left a lasting impression on bin Laden and gave him a thirst for more action. In 1986, he established a base for Arab fighters near Khost in eastern Afghanistan, where the Soviets had a garrison. This was a divisive move. Jamal Khalifa, a university classmate of bin Laden’s who also became involved in the anti-Soviet resistance, was concerned about bin Laden’s lack of military experience, and he believed that these plans would result in many young Arabs being needlessly killed on the front lines.6 After a harsh confrontation over bin Laden’s plans, the two friends became distant. Azzam also thought that the Arab fighters should be embedded with Afghan units to teach the latter “true Islam,” and thus he opposed a separate Arab force. Bin Laden and his comrades-in-arms, establishing the base near Khost despite the opposition of Azzam, Khalifa, and others, called it al Masada, Arabic for “the lion’s den.” They were attacked by the Soviets in the spring of 1987—which was rather predictable, given al Masada’s proximity to a Soviet garrison. But bin Laden and his comrades unexpectedly held their ground in the face of several attacks by Russian special forces (spetsnaz). This intense combat, lasting for about three weeks, launched bin Laden to prominence in the Arab media as a war hero.7 In reality, that battle was completely insignificant for the outcome of the Afghan-Soviet war. Although bin Laden subsequently emphasized his role in the conflict, every serious history concludes that the “Afghan Arabs,” the fighters from the Arab world who traveled to South Asia to join the war against the Soviets, were not a military factor in Russia’s defeat. Nonetheless, bin Laden’s time on the Afghan battlefield was a formative experience for him that shaped the approach he would take when running al Qaeda. Russia didn’t just withdraw from Afghanistan in ignominious defeat. The Soviet empire itself collapsed soon thereafter, in late 1991. Thus, bin Laden thought that he had not only bested one of the world’s superpowers on the battlefield but had also played an important role in its demise. Regardless of the dubious nature of this belief, it seems to have been bin Laden’s perception. From the view that he had played a critical role in causing the Soviet empire to fall, we can discern a further aspect of bin Laden’s thought: the centrality of economics to his fight against a superpower. It is indisputable, after all, that the Soviet withdrawal from Afghanistan did not directly collapse the Soviet Union. The most persuasive connection that can be drawn between that war and the Soviet empire’s dissolution is through the costs imposed by the conflict. Indeed, bin Laden spoke of how he used “guerrilla warfare and the war of attrition to fight tyrannical superpowers, as we, alongside the mujahedin, bled Russia for ten years, until it went bankrupt.”8 This may seem like an implausible propaganda piece that even bin Laden couldn’t have believed. But let’s examine one construction of this argument: that the costs imposed by the Afghan-Soviet war prevented the Soviet Union from adapting to other economic challenges. One such challenge was grain shortages. Since 1928-1929, with the expropriation of farmers’property and forced collectivization, bad agricultural policies had left the Soviets with no growth in grain production since the 1960s. Meanwhile, they experienced an urban population increase of eighty million. Once the world’s biggest grain exporter, Russia by the 1980s had become its biggest importer instead.9 Compounding the problem, Saudi Arabia decided on September 13, 1985, to ramp up its oil production in order to collapse world prices. Oil prices dropped precipitously from around $30 a barrel to just $12 a barrel by March 1986.10 While being battered by huge expenditures to pay for its grain imports, the Soviet Union’s oil export—based economy was also being pressured by a significantly smaller revenue stream. For this reason, Yegor Gaidar—who from 1991 to 1994 served as Russia’s acting prime minister, minister of economy, and first deputy prime minister—has written that the combination of grain shortages and falling oil prices ultimately undermined the Soviet Union.11 Although Gaidar does not blame the Afghan-Soviet war, his arguments are instructive on how someone might see that conflict playing a role in the Soviet Union’s collapse by diminishing the resources available to deal with the twin catastrophes of grain shortages and low oil prices. The Soviet Union ended up with enormous budget deficits, Gaidar writes, and therefore faced difficult choices. To cut costs, it could give up its hold over Eastern Europe, ration food to reduce its grain imports, or massively cut its military-industrial complex. Instead, the government ignored the problem and borrowed money from overseas (a solution that may sound hauntingly familiar to us today). By 1989 the Soviet Union’s credit rating had fallen, and its loans dried up. In need of $ 100 billion from the West and faced with possible famine in Moscow, Soviet premier Mikhail Gorbachev essentially offered political concessions in exchange for credit, and these concessions precipitated an August 1991 coup by hard-liners. But the economic situation doomed this coup from the outset. Even if the hard-liners crushed the demonstrators who turned out to oppose them, Gaidar asks, “Would the grain appear? Where would they find the food necessary to feed the larger cities? Would the West rapidly give the $100 billion? Their case, like the Soviet state itself, was entirely lost.” The Soviet state essentially ended with a November 1991 letter from its Foreign Trade Bank informing the country’s leadership that it had no money left.12 The point is not that Gaidar’s view of how this history unfolded should be accepted over competing accounts. Rather, Gaidar’s history is presented to illustrate how economics can be seen as relevant to the Soviet Union’s demise—and how one could reasonably believe that the Afghan-Soviet war played a role by imposing costs that, coupled with other problems, overwhelmed the Soviet state’s ability to adapt and survive. Indeed, some serious scholars credit the Afghan-Soviet war as being a significant factor, though not the sole one, in the Soviet Union’s collapse.13 The fact that a major strategic lesson taken by bin Laden from his experiences in the Afghan-Soviet war was the importance of economics to defeating a superpower is underscored by his numerous comparisons of the United States to the Soviet Union. When he did so, the comparison was explicitly economic in nature. For example, in October 2004 bin Laden said that just as the Afghan mujahedin and Arab fighters had destroyed Russia economically, al Qaeda was now doing the same to the United States, “continuing this policy in bleeding America to the point of bankruptcy.”14 Similarly, in a September 2007 video message, bin Laden claimed that “thinkers who study events and happenings” were now predicting the American empire’s collapse. Comparing President Bush to Brezhnev, the architect of the Soviet invasion of Afghanistan, bin Laden said, “The mistakes of Brezhnev are being repeated by Bush.”15 Had American strategists understood from the outset the connection between economics and bin Laden’s envisioned path to victory, perhaps the United States could have avoided some of its costly blunders. But it is not clear that U.S. strategists saw this link—even after bin Laden boasted of it on the world stage. Broadening the Fight Another aspect of bin Laden’s experience in the Afghan-Soviet war that influenced his strategic understanding of his fight against the United States was the breadth of the anti-Russian resistance. The Soviet invasion of Afghanistan outraged the Muslim world, including heads of state, clerics, the Arab media, and the man on the street. In January 1980, Egypt’s prime minister declared the Soviet invasion “a flagrant aggression against an Islamic state” and said that it showed the Soviet Union was “but an extension of the colonialist Tsarist regime.”16 By the end of the month, the foreign ministers of thirty-five Muslim countries, as well as the Palestine Liberation Organization, passed a resolution through the Organization of the Islamic Conference (OIC) declaring the invasion of Afghanistan to be a “flagrant violation of all international covenants and norms, as well as a serious threat to peace and security in the region and throughout the world.” The Soviet- installed regime in Afghanistan was expelled from the OIC, the delegates of which urged all Muslim countries “to withhold recognition of the illegal regime in Afghanistan and sever diplomatic relations with that country until the complete withdrawal of Soviet troops.” On January 30, 1980, the Christian Science Monitor described this condemnation of Soviet actions as “some of the strongest terms ever used by a third-world parley.”17 The stream of Arabs who flocked to South Asia to help the Afghan cause—about ten thousand—was a testament to the widespread outrage caused by the invasion. Mohammed Hafez, an associate professor in the Naval Postgraduate School’s National Security Affairs Department, notes that these Arab volunteers “included humanitarian aid workers, cooks, drivers, accountants, teachers, doctors, engineers and religious preachers. They built camps, dug and treated water wells, and attended to the sick and wounded.”18 There was, of course, also a contingent of Arab foreign fighters, of which bin Laden became a part. But the volunteers who went to South Asia were not the only Arabs to support the Afghan resistance. The Afghan jihad was also aided by a donor network known as the “golden chain,” whose financiers came primarily from Saudi Arabia and other Gulf Arab states.19 Essentially, bin Laden sat at the top of a major multinational organization during the Afghan-Soviet war. Its members included fighters, aid workers, and other volunteers. It enjoyed a significant media presence, external donors, and widespread support. Indeed, when al Qaeda was later engaged in a global fight against the United States, bin Laden and his companions understood both the media and the struggle for sympathy and allegiance throughout the Muslim world as crucial battlefields. In a 2005 letter to al Qaeda in Iraq (AQI) leader Abu Musab al Zarqawi, bin Laden’s deputy, Ayman al Zawahiri, noted that “more than half of this battle is taking place in the battlefield of the media.” Zawahiri said that when it comes to attaining the caliphate, a goal of al Qaeda’s that will be discussed shortly, “the strongest weapon which the mujahedin enjoy, after the help and granting of success by God, is popular support from the Muslim masses in Iraq, and the surrounding Muslim countries.”20 This is a telling statement: it shows how important it is to al Qaeda to win Muslim support and turn the Islamic world against the United States. Had U.S. strategists understood al Qaeda’s goal of broadening its fight against the United States, they might have raised more objections to the invasion of Iraq, which created a far broader battlefield for America. Al Qaeda’s Birth Al Qaeda was founded in August 1988, in the waning days of the Afghan-Soviet war.21 At that time, bin Laden and Abdullah Azzam agreed that the organization they had built during the conflict shouldn’t simply dissolve when the war ended.22 Rather, they wanted the structure they had created to serve as “the base” (al qaeda) for future mujahedin efforts. As Azzam and bin Laden repurposed this structure into an organization that would endure, al Qaeda’s founding minutes reveal a broad mission. They describe the organization as “basically an organized Islamic faction” with the goal of lifting “the word of God, to make His religion victorious.”23 Although Azzam had been the leader in the Services Bureau, by August 1988 it was clear that bin Laden was the head of al Qaeda.24 The group was led by an advisory (shura) council in which bin Laden held the dominant position. Under this council the group had an intricate structure, including military, financial, and political committees, an intelligence wing, and a media-propaganda wing. In other words, al Qaeda was a prototypically centralized militant organization up until the time it executed the 9/11 attacks. In addition to the group’s hierarchical structure, there were specific qualifications for each leadership position as well as for membership. The commander, for example, was required to have been a member of al Qaeda for at least seven years, have a sufficient understanding of Islamic law and jihad, and “have operational experience from jihad.” Below the commander were a deputy, who must share the same qualifications; a secretary, whom the commander appointed; and a command council.25 Early documents also detailed members’ duties, salaries, and even vacation time.26 Under this system, bachelors qualified for a round-trip plane ticket home after a year, but they also had the option of using the ticket for the hajj (the religious pilgrimage to Mecca that is considered one of the five pillars of Islam) instead. The application to train for jihad in one of al Qaeda’s camps inquired about the applicant’s education level, professional experience, medical history, and how much of the Qur’an he had memorized.27 Despite bin Laden’s disdain for the United States because of its support for Israel, initially al Qaeda wasn’t focused on America; rather, its mission centered on the threat that communism posed to the umma (the worldwide community of Muslims), especially the communist regime that then ruled South Yemen.28 But Iraq’s August 2, 1990, invasion of Kuwait transformed bin Laden’s outlook. Saddam Hussein’s invasion of the tiny monarchy to his south posed an unmistakable threat to Saudi Arabia. With a hundred thousand Iraqi troops amassed in Kuwait, which shared a border with Saudi Arabia, it seemed that the Saudis could be next. President George H. W. Bush offered to furnish a quarter of a million U.S. soldiers to defend the Saudi monarchy. Bin Laden, however, had a different idea. Bin Laden approached the Saudi defense minister, Prince Sultan bin Abdul Aziz al Saud, and suggested that an army of mujahedin, veterans of the Afghan-Soviet war, could defend the kingdom. His quixotic proposal was politely declined, and a U.S.-led multinational army succeeded in liberating Kuwait in 1991.29 Bin Laden saw the U.S. troop presence in Saudi Arabia as a violation of his faith, a view informed by a famous hadith (part of the collection of the customs and sayings of the Prophet Muhammad) in which the prophet, on his death bed, ordered that “two deens [faiths] shall not co-exist in the land of the Arabs.”30 Rather than seeing the Americans as a friendly force defending Saudi Arabia from Iraqi aggression, bin Laden saw them as invaders. In the spring of 1991, bin Laden left Saudi Arabia for Sudan, where he resolved to sponsor attacks on the United States. Neither a December 1992 bombing of two hotels in Yemen, which housed U.S. soldiers en route to the Horn of Africa for Operation Restore Hope (a U.N.-sanctioned humanitarian mission to Somalia), nor the indeterminate role that al Qaeda played in the October 1993 downing of a U.S. helicopter in Mogadishu launched bin Laden into the Western public’s consciousness.31 But his involvement in terrorism did come to the attention of the U.S. and Saudi intelligence services, and the resulting pressure on Sudan’s government caused it to see bin Laden as a liability. Sudan seized the construction equipment that formed the backbone of bin Laden’s business in that country, giving him only a fraction of its value in return.32 His business suddenly gone, and clearly on his enemies’ radar, bin Laden fled to Afghanistan on May 18, 1996—returning to the country where he had first carved out his reputation. The fundamentalist Taliban regime that controlled about 90 percent of that country agreed to protect him. It said, in one statement, “If an animal sought refuge with us we would have had no choice but to protect it. How, then, about a man who has given himself and his wealth in the cause of Allah and in the cause of jihad in Afghanistan?”33 A1 Qaeda’s War against America On August 23, 1996, bin Laden, within a few months of arriving in Afghanistan, issued a manifesto proclaiming himself at war with the world’s only remaining superpower. Bin Laden’s overarching grievance was the U.S. military presence in Saudi Arabia, which he described as “one of the worst catastrophes to befall the Muslims since the death of the Prophet.”34 Bin Laden also named America’s support for Israel and U.S.ded sanctions against Saddam Hussein’s Iraq as additional justifications for his fight. (There was no love lost between bin Laden and Iraq’s secular dictator, but he blamed U.S. sanctions for a humanitarian catastrophe in that country.) Few in the United States took notice of bin Laden’s declaration, either among the public at large or within the government. As Michael Scheuer, the former head of the CIA’s Bin Laden Unit, has written, these political grievances were intended to place al Qaeda’s fight within the realm of “a defensive jihad sanctioned by the revealed word of God.”35 That is, in contrast to an “offensive jihad,” expansionist warfare designed to enlarge the abode of Islam, this was a case, bin Laden argued, in which the faith itself was under attack by its foes. In such instances, each Muslim has an individual obligation to join the battle. It’s not enough if some group takes up arms; this must be done by all Muslims. If such a religious duty is an individual obligation (fard ayn), young people don’t even have to receive permission from their parents to join the fight. This declaration of war did not represent an aberrant turn within Islamic thought, as some commentators have claimed. Although there are credible, powerful, and widely held interpretations of the faith that find bin Laden’s arguments and actions unjustified and immoral, bin Laden does draw on legitimate sources, tap into venerable currents of Islamic thought, and make arguments that resonate with many of the faithful.36 As previously mentioned, the concept of jihad has variegated meanings, and there are nonmilitary aspects of this struggle. But as Bernard Lewis, professor emeritus of Near Eastern Studies at Princeton University, has written, “The overwhelming majority of early authorities, citing the relevant passages in the Qur’an, the commentaries, and the traditions of the Prophet, discuss jihad in military terms.”37 As a salafi—an adherent to an austere religious methodology that seeks to re-create Islam as it was supposedly practiced by the Prophet Muhammad and the first generations of Muslims—bin Laden argued that other Muslims should return to the earliest, purest interpretation of the faith. If Muslims do return to the earliest interpretation of Islam, salafi jihadism holds, they will understand the righteousness and the necessity of these calls for violence. Thus bin Laden tapped into currents of thought that preceded him. These currents of thought have also survived his death. The narrative of al Qaeda and other salafi jihadi groups holds that Islam itself is under attack, both physically and morally, by the United States and other forces of nonbelief (including the corrupt regimes that dominated the Middle East throughout the twentieth century) and that violence is necessary to defend the faith.38 This is not to say that al Qaeda is correct in its interpretation of the Islamic faith, or otherwise. But it is always a mistake to underestimate the strength of your enemy’s arguments, which is precisely what many Western analysts have done in the case of al Qaeda and other salafi jihadi groups. There has been a division within the jihadi movement concerning whether it should focus on the “near enemy”—the toppling of the corrupt Arab regimes, which jihadis sometimes refer to as apostate governments—or instead target the “far enemy,” the United States and other Western powers.39 Thomas Hegghammer, a senior research fellow at the Norwegian Defense Research Establishment in Oslo, notes that this controversy may be “the most significant political rift in the world of militant Islamism since the mid-1990s.”40 Although al Qaeda views both the United States and the apostate Arab regimes as its enemies, it has largely focused its warfare against the United States and other Western countries. A study released in the summer of 2009 by a jihadi “think tank” that supports al Qaeda’s decision to do so explains that in waging war against the Saudi regime, the group was faced with the decision of fighting Saudi Arabia directly or striking at the American presence in that country. If it fought Saudi Arabia, the attacks would have met with condemnation by the Saudi ulema (religious scholars). A1 Qaeda’s war against the Saudis would have been a losing effort, “given the size and weight of the religious institution, and the legitimacy and prestige it instilled in the people’s minds across more than 70 years.”41 On the other hand, the study viewed striking at the Americans as a wise choice, because the kingdom would be forced to defend their presence, “which will cost them their legitimacy in the eyes of Muslims.” Moreover, the ulema would be delegitimized if they too defended the U.S. presence. Thus, many of those who favor fighting the United States rather than the “near enemy” think that jihadi groups can weaken both foes simultaneously in that manner. Although the political grievances that bin Laden and other jihadi thinkers have articulated illuminate their short-term ambitions, the movement also possesses long-term goals. One is to spread sharia, or Islamic law. As bin Laden said in a 1998 letter published in the Rawalpindi-based newspaper Jang, he believes that al Qaeda’s struggle should continue until “the Islamic sharia is enforced on the land of God.”42 He has repeatedly emphasized the importance of establishing sharia since then, as have other jihadi leaders.43 Extrapolating from their conception of the religious concept of tawhid (the unity of God), these jihadi thinkers argue that if only Allah can be worshiped and obeyed, then only Allah’s laws can have legitimacy.44 The version of sharia that these thinkers embrace is undeniably harsh. Illustrating this, when Peter Bergen asked bin Laden’s London media representative Khalid al Fawwaz in the late 1990s what present government most resembled his vision of an ideal Islamic state, Fawwaz replied that Afghanistan’s brutal Taliban regime was “getting there.”45 For perspective, the Taliban’s treatment of women was so inhumane that Physicians for Human Rights released a report in 1998 noting that “no other regime in the world has methodically and violently forced half of its population into virtual house arrest, prohibiting them on pain of physical punishment from showing their faces, seeking medical care without a male escort, or attending school.”46 Homosexuals were executed, although there was some disagreement among jurists as to whether they should be pushed to their deaths from a high altitude or crushed beneath a toppling wall. Virtually every imaginable form of light entertainment was banned, including kite flying, movies, television, music, and dancing. Also banned were paintings and the celebration of holidays that were cultural rather than religious, such as the Afghan new year.47 Afghans were beaten and sometimes killed for flouting this complex and outright absurd set of rules. Another goal of the jihadi movement is reestablishment of the caliphate, a theocratic government that would rule a united Muslim world. Islam’s first caliph (Arabic for “successor,” denoting that the caliph follows Muhammad as the faith’s political leader) was Abu Bakr, who led the umma beginning in 632 a.d., after the Prophet Muhammad’s death. One jihadi thinker, in a representative statement, described Mustafa Kemal Atatiirk’s abolition of the caliphate in 1924 as the “mother of all crimes.”48 Similarly, bin Laden made explicit reference to the grave injustice of the caliphate’s fall in his 1996 declaration of war against the United States and referred to the need to reestablish it multiple times thereafter.49 Indeed, the introduction to al Qaeda’s training manual describes the manual as a “contribution toward paving the road that leads to majestic Allah and establishing a caliphate.”50 And Zawahiri has written that al Qaeda’s “intended goal in this age is the establishment of a caliphate in the manner of the Prophet.”51 Yet the caliphate’s establishment wouldn’t end the war against the infidels. One work that shows how the jihad would continue is Jordanian journalist Fouad Hussein’s influential 2005 bookAI Zarqawi: The Second Generation of al Qaeda, which Pulitzer Prize-winning author Lawrence Wright has called “perhaps the most definitive outline of al Qaeda’s master plan.”52 Hussein shows that in this master plan, al Qaeda’s strategists foresee a “stage of all-out confrontation” with the forces of atheism after the caliphate is declared. He writes, “Al Qaeda ideologues believe that the all-out confrontation with the forces of falsehood will take a few years at most. The enormous potential of the Islamic state—particularly because the Muslim population will amount to more than 1.5 billion—will terrify the enemy and prompt them to retreat rapidly.”53 Some Western analysts fail to appreciate what the caliphate’s reestablishment signifies. For example, Michael Scheuer, in his 2004 book Imperial Hubris, describes Saudi Arabia as “a regime that, since its founding, has deliberately fostered an Islamic ideology, whose goals—unlike bin Laden’s—can be met only by annihilating all non- Muslims.”54 This claim is nonsensical. It is premised on the idea that bin Laden’s practice of Islam (and that of al Qaeda) was more moderate than Saudi Arabia’s. There is not a shred of evidence to suggest that this is the case. Bin Laden turned against the Saudi monarchy not because it was too extreme nor because he had rejected the tenets of its Wahhabi creed, but rather because he believed that the Saudis were not living up to their strict ideals.55 Once Scheuer concedes that Saudi ideology is designed to foster an eternal conflict with non-Muslims—a view supported by a literal reading of Wahhabi scholarship—it makes no sense to say that al Qaeda’s conflict with the West is anything but existential. Scheuer may have been conflating al Qaeda’s often invoked political grievances with its overall objectives. Or he may have focused on the fact that bin Laden had declared a defensive jihad rather than an offensive one—and assumed that al Qaeda could not declare an offensive jihad, which in Scheuer’s estimation “must be called by a Caliph, the recognized leader of the world Islamic community,” a position that has not existed since 192 4.56 If so, Scheuer is overly casual in dismissing the possibility that, like the twentieth-century Pakistani Islamist ideologue Sayyid Abul A’la Maududi, al Qaeda might see the distinction between offensive and defensive jihad as artificial. Maududi wrote that jihad is “both offensive and defensive at one and the same time”: it is offensive because a Muslim undertaking jihad “attacks the rule of an opposing ideology,” but is simultaneously defensive because by mounting such an attack, a Muslim can “protect the principles of Islam in space-time forces.”57 Moreover, if al Qaeda were able to create the caliphate that it desires, that superstate would have the necessary authority to declare an offensive jihad. The role of the caliphate in al Qaeda’s strategic vision thus cannot be ignored. America Turns Away It was not just bin Laden’s 1996 declaration of war against the United States that went unnoticed in the West. Even a couple of skilled and deadly terrorist attacks—the August 1998 bombings of two U.S. embassies in Kenya and Tanzania and the October 2000 strike on the USS Cole destroyer in Yemen’s port of Aden—failed either to make bin Laden a household name for Westerners or to provoke a significant response by the U.S. government. Indeed, while the embassy bombings produced limited cruise missile strikes against al Qaeda camps in Afghanistan, the Cole attack engendered no U.S. retaliation at all. In June 2001, a propaganda video released by al Qaeda claimed credit for the Cole bombing and called for more attacks on U.S. interests. During that summer, there were signs that more were on the way. CIA director George Tenet would later tell the 9/11 Commission that the U.S. intelligence system “was blinking red” with credible reports of al Qaeda’s plans.58 Yet even though al Qaeda was clearly plotting, the United States was not taking advantage of these warnings to make plans of its own with respect to al Qaeda’s safe haven in Afghanistan. Legendary journalist Bob Woodward notes that while the U.S. military “seemed to have contingency plans for the most inconceivable scenarios,” there was “nothing on the shelf that could be pulled down to provide at least an outline” for addressing al Qaeda’s safe haven in Afghanistan were a large-scale attack to force America’s hand.59 In part, this is because top administration officials were firmly ensconced in traditional security paradigms that focused on threats posed by other nation-states to the exclusion of nonstate actors. CIA director Tenet mentioned al Qaeda in his daily briefings to President Bush more than forty times before the 9/11 attacks.60 Bush famously received an intelligence briefing on August 6, 2001, titled “Bin Laden Determined to Strike in U.S.” The briefing warned of “patterns of sus-picious activity in this country consistent with preparations for hijackings or other types of attacks” and claimed, using a figure that proved to be exaggerated, that seventy Federal Bureau of Investigation field investigations were considered related to bin Laden.61 Yet despite these and other warnings, Bush did not publicly mention al Qaeda between August 6 and September 11. National Security Adviser Condoleezza Rice was in fact scheduled to deliver a major address on September 11, 2001, that in the White House’s own words was designed to examine “the threats and problems of today and the day after, not the world of yesterday” But the focus of this address was on promoting missile defense, and it did not mention Osama bin Laden, al Qaeda, or any other jihadi groups.62 The intended speech demonstrates the power of a paradigmatic focus on nationstate threats to the exclusion of nonstate actors. An interesting academic article published in the Massachusetts Institute of Technology Press journal International Security in the summer of 2001 provided an indication of what U.S. planners should have been considering before the 9/11 attacks. Written by Ivan Arreguin- Toft, a postdoctoral fellow in the International Security Program at the Belfer Center for Science and International Affairs at Harvard University’s Kennedy School of Government, “How the Weak Win Wars” began with an extended look at the famed “rumble in the jungle” boxing match that Muhammad Ali and George Foreman fought in Kinshasa, Zaire (now the Democratic Republic of the Congo) in October 1974.63 Foreman had been heavily favored in the fight, for he was “the strongest, hardest hitting boxer of his generation” and had sparred with nimble opponents in preparation for the quick and graceful Ali. But as Arreguin-Toft recounts, the more powerful Foreman’s preparation did not ready him for Ali’s strategy, which turned Foreman’s strength against him: In round two, instead of moving into the ring to meet Foreman, Ali appeared to cower against the ropes. Foreman, now confident of victory, pounded him again and again, while Ali whispered hoarse taunts: “George, you’re not hit- tin,” “George, you disappoint me.” Foreman lost his temper, and his punches became a furious blur. To spectators, unaware that the elastic ring ropes were absorbing much of the force of Foreman’s blows, it looked as if Ali would surely fall. By the fifth round, however, Foreman was worn out. And in round eight, as stunned commentators and a delirious crowd looked on, Muhammad Ali knocked George Foreman to the canvas, and the fight was over.64With the right strategy, a weak actor may be able to neutralize a stronger power’s inherent advantage. Indeed, Muhammad Ali’s “rope a dope” would serve as a chilling metaphor for events to come. Could al Qaeda similarly succeed in making a series of U.S. measures directed at the militant group exhaust the world’s only superpower? September 11, 2001 The subtlest change in New York is something people don’t speak much about but that is in everyone’s mind. The city, for the first time in its long history, is destructible. A single flight of planes no bigger than a wedge of geese can quickly end this island fantasy, burn the towers, crumble the bridges, turn the underground passages into lethal chambers, cremate the millions. The intimation of mortality is part of New York now: in the sound of jets overhead, in the black headlines of the latest edition. —E. B. White, Here Is New York, 1949 Despite millions of words that have been written about that shocking day in September 2001, it is difficult to fully express the impact it had on the American psyche. The world watched in horror as two hijacked airplanes crashed into and toppled the World Trade Center’s Twin Towers in New York City and another demolished a large section of the Pentagon in Washington, D.C. After a struggle between passengers and hijackers, a fourth plane crashed in a field in Shanksville, Pennsylvania, killing everyone on board. Various rumors and confused reports that surfaced during the day held the damage to be even worse. Officials in Washington, D.C., heard that eleven aircraft may have been hijacked. There were reports of a car bomb at the State Department. Richard Clarke, then a high- ranking counterterrorism official in the Bush administration, recalled mentally tabulating the possible damage: “With the towers collapsed, the death toll could be anywhere from 10,000 to maybe as high as 50,000. No one knew. And it wasn’t over.”1 What so profoundly changed the United States was not just the enormous structural damage and massive death toll incurred by the most vicious surprise attack in U.S. history. There was also the shattering of national myths and assumptions. The 9/11 attacks showed that the United States could no longer rely on the Pacific and Atlantic Oceans for its security. The attacks disproved the rather comforting assumption that terrorist groups were deterred from carrying out mass casualty attacks out of fear that they would lose public sympathy. And September 11, 2001, boldly announced the rise of nonstate actors capable of striking at the heart of the military and economic power of the world’s strongest country. As Clarke put it, “They had proven the superpower was vulnerable, that they were smarter, they had killed thousands.”2 On a warm, tranquil morning, Americans sat glued to their televisions in horror as three separate sites on the East Coast were transformed into unthinkable open-air graves. The new world seemed overwhelmingly unsafe. For many Americans, the attacks were a horrifying introduction to the depths of hatred directed at the United States. Terrorists’ lethal capabilities were now clear. And the 9/11 attacks awoke many citizens to the inherent difficulties of defending an open society from attack. Suddenly there seemed to be no shortage of easy targets: shopping malls, amusement parks, pizzerias, trains, buses, and bridges. Underscoring our vulnerabilities—and ostensibly confirming Americans’ worst fears—a number of prominent figures received letters containing anthrax the following month. Five people died, and seventeen others were infected; the figures to whom these letters were addressed included NBC News anchor Tom Brokaw and Senators Tom Daschle and Patrick Leahy. Although it seems that these letters were not mailed by Islamic extremists, they were a sign of the dangerous new environment that Americans were only beginning to understand.3 9/11 and the U.S. Economy I have already noted that the United States has suffered because of its failure to understand al Qaeda. America’s lack of knowledge about the jihadi group should have been apparent the moment the 9/11 attacks occurred. After all, the attacks demonstrated a massive underestimation of al Qaeda’s ability to strike the continental United States. But even after witnessing the group’s deadly competence, U.S. planners likewise underestimated its resilience and made little effort to comprehend its strategy. This strategy could be known and understood through a nuanced look at bin Laden’s personal history and thought. Even at the time of 9/11, it was clear that bin Laden believed it was essential to undermine the economy of his superpower foe and to make the battlefield on which the Americans had to fight as broad as possible. American strategic documents analyzing al Qaeda reveal a lack of awareness of these twin goals. Bin Laden’s attacks on the United States before 9/11 did not have much of an economic impact. Al Qaeda’s most successful previous attack on American interests was its near-simultaneous bombings of the U.S. embassies in Kenya and Tanzania in August 1998. Although 247 people died in those attacks (12 of them U.S. citizens) and the attacks forced the United States to expend a decent amount of money upgrading the security of its overseas facilities, these are the kind of losses and expenditures that an economic and military superpower can absorb. In the wake of those attacks, the government took immediate action to upgrade perimeter security at overseas embassies and missions.4 It reprioritized construction and upgrades in order to bring overseas facilities up to “Inman standards,” so named after a report that outlined the standards sufficient to deal with contingencies like terrorist attacks. The embassy bombings also led the State Department to initiate a $21 billion program to replace 201 different facilities that it regarded as either dilapidated or insecure.5 America’s ability to absorb these security outlays could be seen in the fact that the country continued to run a budget surplus during this period. But the economic damage caused by 9/11 dwarfed that of previous terrorist attacks, a fact that was not lost on bin Laden. Some observers doubt that bin Laden and al Qaeda were as focused on attacking their enemy’s economy in 2001 as they would later be. The reason for this skepticism can be found, for example, in an early fatwa (religious ruling) issued by Sheikh Omar Abdel Rahman, a spiritual guide to two Egyptian jihadi groups, who has been imprisoned in the United States since his October 1995 conviction for taking part in a terrorist conspiracy to attack the United Nations and other New York City landmarks.6 The fatwa reads, “Cut off all relations with [the Americans, Christians, and Jews], tear them to pieces, destroy their economies, burn their corporations, destroy their peace, sink their ships, shoot down their planes and kill them on air, sea, and land. And kill them wherever you may find them, ambush them, take them hostage, and destroy their observatories.”7 Peter Bergen assesses this document as significant, writing that the “fatwa to attack the United States economy and American aviation was an important factor in the 9/11 attacks.”8 The flavor of Abdel Rahman’s fatwa, which was typical of early jihadi arguments for striking Western economies, helps to show why some observers have been skeptical that the U.S. economy was a major focus for al Qaeda in 2001. Although economic targets are prominent within the fatwa, the incitement to violence is broad, suggesting to skeptics that while al Qaeda did have America’s economy in mind, it was not central to the group’s strategy. Two critical data points shed light on how bin Laden and al Qaeda thought of the connection between 9/11 and the U.S. economy at the time the attacks were executed. The first is a letter bin Laden wrote to Taliban leader Mullah Omar on October 3, 2001, just before the United States began to bomb Afghanistan. (The letter was subsequently recovered from one of al Qaeda’s computers.) In the let-ter, bin Laden claimed that if the United States invaded Afghanistan, the military conflict “will impose great long-term economic burdens, leading to further economic collapse, which will force America, God willing, to resort to the former Soviet Union’s only option: withdrawal from Afghanistan, disintegration, and contraction.”9 He continued that the campaign against the United States should focus on “serving a blow to the American economy,” which would in turn shake investors’ confidence, causing them “to refrain from investing in America or participating in American companies, thus accelerating the fall of the American economy.” The fact that bin Laden explicitly compared the situation the United States would face in Afghanistan to that encountered by the Soviets speaks volumes. So too does the fact that he connected America’s coming campaign in Afghanistan to the Soviet campaign exclusively through the impact of invasion and occupation on both countries’economies. Thus, even as a retaliatory U.S. attack on al Qaeda’s safe haven was imminent, bin Laden recognized the American economy as the superpower’s key vulnerability. The second data point is an October 21, 2001, television interview that bin Laden gave to Al Jazeera’s Taysir Allouni, who is now imprisoned in Spain after a controversial criminal conviction for cooperating with al Qaeda.10 The wide-ranging interview, conducted shortly after the U.S. military campaign began, is significant contemporaneous evidence of what bin Laden intended to accomplish through the 9/11 attacks. The interview began with bin Laden acknowledging al Qaeda’s culpability but insisting that the attacks were a form of self-defense, designed to defend the Palestinian people and religious sites in Saudi Arabia. He continued, “And if inciting for this is terrorism, and if killing the ones who kill our sons is terrorism, then let history witness that we are terrorists.”11 Allouni pointed out that in the United States, al Qaeda faced an opponent that “dominates the world militarily, politically, and technologically.” Since the jihadi group couldn’t match America’s capabilities, he asked bin Laden, what hope did it have of defeating the United States? It should come as no surprise that bin Laden pointed to the Soviet Union and the Afghan-Soviet war in his answer. Bin Laden explained that at the beginning of the 1980s, “the Soviet empire was a force that was very, very strong, which scared the whole world, and NATO used to shake in fear in front of the Soviet empire.” Yet the Soviet Union dissolved after the war in Afghanistan, its massive empire fracturing into Russia and a number of smaller states. Bin Laden thought that America could likewise be defeated. When bin Laden was asked to speak of the impact of the 9/11 attacks, his first observation concerned the economic damage they caused. “According to their own admissions,” he said in the interview with Allouni, referring to the Americans, “the share of the losses on the Wall Street market reached 16%. They said that this number is a record, which has never happened since the opening of the market more than 230 years ago.” Bin Laden then provided an extended exposition of the economic numbers, as well as associated costs, that shows he had given much thought to the economic implications of 9/11. “The gross amount that is traded in that market reaches $4 trillion,” he said. “So if we multiply 16% [by] $4 trillion to find out the loss that affected the stocks, it reaches $640 billion of losses from stocks, with Allah’s grace. So this amount, for example, is the budget of Sudan for 640 years.” He knew, though, that the direct damage to America’s stock market was not the only economic impact. He factored in lost productivity, but in doing so reached a bizarre conclusion about post-9/11 life in America. Figuring the national daily income to be $20 billion, bin Laden claimed that the country did not work for an entire week after the attacks because of the psychological impact. “So if you multiply $20 billion by one week, it comes out to $140 billion, and it is even bigger than this,” he said. One might be inclined to gloss over this inaccuracy, but it is worth dwelling on for one reason: it illustrates that even though the United States often misinterprets and underestimates jihadi militants, they do the same to the United States. The notion that the entire nation missed a full week of work is preposterous. In September 2001 I was living in New York City, which experienced more death and trauma as a result of the 9/11 attacks than any other city in the country. Although Lower Manhattan was shut down temporarily after the Twin Towers’ collapse, the rest of the city was back at work immediately I remember how New York City seemed dazed as it returned to its daily life. Most noticeable was the change in traffic patterns: New York’s aggressive drivers typically honk their horns in anticipation before traffic lights turn green, but now an unexpected politeness gripped the citizenry Horns were rarely heard for several days, and drivers looking to make a turn through a crosswalk would uncharacteristically wave pedestrians through first. Equally unexpected was how the movie theater up the street from where I lived, the United Artists Union Square Stadium 14, decided to show free films for a day. Restaurants brought free food to the ground zero workers, and New Yorkers lined the West Side Highway offering support to the rescue crews. The attacks changed the United States and changed New York; but even in the city that absorbed the most damage, people were not just staying home in shock. After claiming falsely that Americans had missed a full week of work because of the attacks, bin Laden estimated to Allouni that building and construction losses may have amounted to $30 billion. He then gloated about all of the lost American jobs—stating that 170,000 employees were fired from the airline industry and that the InterContinental Hotel chain had been forced to cut 20,000 jobs. So taking into account the second- and third-order economic consequences, bin Laden calculated that the cost to the United States was “no less than $1 trillion by the lowest estimate.” Yet even though some of bin Laden’s claims were false, his overall damage estimates were accurate and may in fact have been conservative. As former CIA officer Bruce Riedel has noted, the property damage and lost productivity caused by the 9/11 attacks probably cost more than $100 billion. When factoring in lower profits and economic volatility, Riedel writes that the price tag is even larger, “as high as $2 trillion according to some estimates.”12 In a video that bin Laden released in October 2004, he amplified this analysis by pointing out how much damage 9/11 inflicted upon the United States, in comparison to the much smaller costs that al Qaeda incurred in executing them. “Al Qaeda spent $500,000 on the event,” he said, “while America, in the incident and its aftermath, lost— according to the lowest estimate—more than $500 billion, meaning that every dollar of al Qaeda defeated a million dollars.”13 To be sure, bin Laden spoke with Allouni in the October 2001 interview about more than just economics. A consummate propagandist, he also discussed how Western civilization itself had lost its appeal with the collapse of the Twin Towers. But the first demonstration of the 9/11 attacks’ success that bin Laden pointed to was their economic impact, and he had obviously given a great deal of thought to the precise costs for the United States. The economic aspects of bin Laden’s fight with America dominated his interview with Allouni. Thus, the earliest data points reflecting bin Laden’s thinking at the time of the 9/11 attacks—his interview with Allouni and the letter he had written to Mullah Omar—show that he had America’s economy in mind from the very outset. Know Your Enemy? The United States has not heeded the ancient Chinese military strategist Sun Tzu’s famous maxim that to succeed in a military conflict, it is necessary to know your enemy.14 America gave little thought to al Qaeda’s strategy at the time of the 9/11 attacks, and thejihadi group’s overarching strategy remains poorly understood today. To comprehend America’s shallow understanding of al Qaeda, one need look no further than the official documents outlining U.S. thinking about this conflict. The “National Military Strategic Plan for the War on Terrorism” (NMSP-WOT), published by the chairman of the Joint Chiefs of Staff, Richard B. Myers, on February 1, 2006, accurately bills itself as “the comprehensive military plan to prosecute the Global War on Terrorism (GWOT) for the Armed Forces of the United States.”15 Although the NMSP-WOT outlines America’s ends, ways, and means, it does not perform the same analysis for al Qaeda—which is striking, because understanding an enemy’s ends, ways, and means is fundamental to formulating military strategy. Indeed, the NMSP-WOT displays a laserlike focus on a single tactic—terrorism—without asking deeper questions about this tactic. What objectives does the enemy hope to accomplish through the use of terrorism? The NMSP-WOT tries to sidestep this question by stating that “there is no monolithic enemy network with a single set of goals and objectives.”16 But certainly there are commonalities among the various groups affiliated with al Qaeda. The NMSP-WOT does not explore these common goals and strategies, other than making the rather banal observation that such groups possess “extremist ideologies antagonistic to freedom, tolerance, and moderation” and use terrorism “to impede and undermine political progress, economic prosperity, the security and stability of the international state system, and the future of civil society.”17 The report also examines the enemy’s center of gravity—a concept that the Department of Defense describes as “the source of power that provides moral or physical strength, freedom of action, or will to act”— but it does not explain how al Qaeda and affiliated movements understand America’s center of gravity.18 Is their use of terrorism aimed at a particular point of weakness? Reading the NMSP-WOT, one gets the impression that these groups are striking at random targets, with no overarching plan. The White House’s “National Strategy for Combating Terrorism,” published in September 2006, does more to explain the common goals of America’s jihadi foes. It notes that although the transnational jihadi movement isn’t monolithic and is not controlled by one leader, “what unites the movement is a common vision, a common set of ideas about the nature and destiny of the world, and a common goal of ushering in totalitarian rule.” The document continues by noting that these groups “seek to expel Western power and influence from the Muslim world and establish regimes that rule according to a violent and intolerant distortion of Islam.”19 But even though the National Strategy for Combating Terrorism discusses the end state that these groups desire, it doesn’t even try to assess how they intend to get there. Do they have an envisioned path to victory that seeks to exploit certain U.S. vulnerabilities? Or have they embraced the tactic of terrorism and the goal of creating totalitarian religious regimes without any conception of how the tactic might connect to the goal? Even the 9/11 Commission Report fails to provide any kind of strategic assessment of bin Laden and al Qaeda. It notes that “for those yearning for a lost sense of order in an older, more tranquil world, [bin Laden] offers his ‘caliphate’ as an imagined alternative to today’s uncertainty.”20 But the report provides no assessment of how al Qaeda intends to bring about the caliphate. There is yet again an unresolved disconnect between al Qaeda’s tactics and goals. It is, of course, possible that al Qaeda doesn’t think strategically: that its desired end state is a pie-in-the-sky dream, and this adversary has no concept of how its dream can be turned into a reality. But it is dangerous to begin strategic assessments with the assumption of an adversary’s incompetence, and the idea that al Qaeda does not possess strategic thought is just that, an assumption. Moreover, it is an unfounded assumption. Al Qaeda is in fact rather strategically adept. Charlie Allen, a forty-year veteran of the intelligence community who also served as a high-ranking official in the fledgling Department of Homeland Security (DHS), has been described by U.S. News & World Report as “more of a legend than a man around the CIA.”21 When I asked him about the lack of an assessment of al Qaeda’s strategy, he said, “I think it was a frenetic period where everyone was pushed to the limit as we expanded on the intelligence and military side. Lirst DHS was setting up, and we didn’t have any analysts. Then came the planning for the Iraq War, and we had to wield a great deal of resources to deal with that.” Sitting in his office near Washington, D.C.’s Dupont Circle, Allen concluded, “But there’s no excuse for not taking a cold eye to al Qaeda’s strategies and capabilities.”22 Brian Michael Jenkins, senior adviser to the president at the RAND Corporation, is a well-regarded terrorism expert, a Vietnam veteran, and a former Green Beret. He also agreed that the lack of assessment of al Qaeda’s strategy is a significant problem. “We have to do a better job of understanding our foe,” he told me. “At the governmental level, we need to have a better understanding of our foe’s approach to warfare and strategy. One of the reasons we haven’t done so is that we’re trapped by the word terrorism itself.” Jenkins compared the current shallow strategic assessments of al Qaeda to those performed during World War II and the Cold War, when America’s understanding of Soviet strategy and means was sophisticated, and American planners carefully examined the writings and thinking of the German generals. In contrast, Jenkins said, in the view of U.S. planners, terrorists “were not worthy foes; they didn’t measure up.”23 To return to Ivan Arreguin-Toft’s metaphor of Muhammad Ali’s rope-a-dope strategy (see chapter 2), this lack of strategic awareness made it difficult for American planners to discern whether al Qaeda had adopted a plan designed to neutralize America’s inherent advantages. This lack of strategic awareness made it difficult to avoid being sucked into a fight where the harder the United States hit, the more worn out and vulnerable it became. High Hopes After the 9/11 attacks, it seemed that American politics had fundamentally changed. The United States had been through a divisive election in 2000, with the outcome of Florida’s critical recount ultimately being determined by the Supreme Court. Partisan wounds remained from the court’s controversial decision in Bush v. Gore, which held that a constitutionally valid recount could not be completed in Florida by the relevant deadline.24 That decision in effect handed the election to George W. Bush, and as a result many Americans saw Bush as an illegitimate president. Beyond this, as one newspaper noted in August 2001, President Bush faced “a nation skeptical of his policies.”25 Yet despite this political antagonism, the shock of 9/11 brought people together. The public rallied behind President Bush, and his approval rating soared to over 90 percent in the days after the attack.26 This represented the highest public approval that had been recorded for a serving president; Americans clearly wanted to “rally ’round the flag” in a time of crisis. As one analyst put it, conventional wisdom holds that “a foreign crisis plays into the hands of a sitting president” because “people look to their leaders for reassurance.”27 Democrats expressed their support for the Republican president. As Senator Joe Biden said, 9/11 represented “the most god-awful wake-up call we’ve ever had.”28 The change in political dynamics—with the public standing behind President Bush and the Democratic Party offering its support—prompted Cornell University government professor Theodore J. Lowi to tell the New York Times that the United States would likely be “operating as if we have a national unity party.”29 The media agreed that a vigorous response to the attacks was justified and necessary. The government, in turn, promised that its response would be overwhelming. Secretary of State Colin Powell encapsulated widely held views of how the administration would respond when he said of al Qaeda, “We will go after that group, that network, and those who have harbored, supported and aided that network.” Representing the scope of the administration’s ambitions, Powell then said that “when were through with that network, we will continue with a global assault against terrorism in general.”30 It appeared to all observers that al Qaeda had awoken a sleeping dragon: the powerful United States of America had finally been hit by a provocation that it could not ignore. All elements of national power were trained on al Qaeda. The United States was determined to deprive it of its safe haven and its flow of money, and to capture or kill its leaders and operatives. It was natural for Americans to rally around their country and their government after the attack. But this moment of national consensus makes all the more tragic what would follow. Colin Powell’s hubris- tic and laughably overoptimistic statement—in which he anticipated finishing off al Qaeda quickly and then moving on to other, unrelated terrorist groups—was indicative of official thinking. The statement was representative in failing to account for the enemy’s strategic logic, massively underestimating al Qaeda’s resilience, and possessing a star- tlingly ambitious scope. The decisions the government made at the very outset of the fight against al Qaeda and associated movements would have long-lasting ramifications. If the government established the right systems for addressing the challenge, capabilities could build over time. Expertise could be developed internally, and counterterrorism efforts could become more competent and more efficient. If the wrong system were put in place—a bloated, disconnected bureaucracy that has trouble keeping up with a small, nimble foe—the costs would only mount.  If we invaded the wrong country, anti-American passions could be inflamed and the United States could become insolubly bogged down. Every decision by a person or a country is made in light of all previous decisions, and it can be exceedingly difficult to turn back after making the wrong move in the fight against terrorism. There is even a political science concept explaining how early decisions in a sequence matter more than later ones: path dependence. As University of California at Berkeley political science professor Paul Pierson puts it, path dependency is the idea that in any political system, “once a particular path gets established . . . self-reinforcing processes make reversals very difficult.”31 This is true, because interested parties make investments around the initial decisions, and institutions are organized around them. These investments and institutional arrangements function as “positive feedbacks” that make it difficult to turn back from one’s first choices.32 America’s initial response to the 9/11 attacks, unfortunately, contained the paradigmatic failures that would drive up costs, present the enemy with openings it never expected, and ultimately play into al Qaeda’s hands. Our Politicized Fight against Terrorism Here is the thing that the Democrats do not get. .. . They do not seem to get the fact that there are people, terrorists in this world, really dangerous people that want to come here and kill us. That in fact they did come here and kill us twice and they got away with it because we were on defense. —Rudy Giuliani, 2007 It was perhaps inevitable that the fight against al Qaeda and other jihadi groups would become politicized, but it has nonetheless been extremely harmful to the United States. The fact that being seen as tough and effective in the fight against terrorism could help one’s political fortunes was evident almost immediately, for the standing of two politicians—George W. Bush and Rudy Giuliani—and that of the entire Republican Party dramatically changed because of the events of September 11, 2001.President Bush’s initial reaction to the attacks was in fact rather confused and unimpressive. Just before he sat down with a class of second graders at Emma E. Booker Elementary School in Sarasota, Florida, he learned that a jumbo jet had hit the World Trade Center’s North Tower. Bush thought at the time—as did many Americans—that the incident had been a tragic accident. But at 9:03 a.m., when United Airlines flight 175 struck the South Tower, there could be no further doubt. As Bush interacted with the second graders, his chief of staff, Andy Card, whispered to him, “A second plane has hit the second tower. America is under attack.”1 Bush tried to remain stoic, but the look on his face conveyed the gravity of the news. One of the students in that class still recalled the president’s expression ten years later, after bin Laden was killed. “In a heartbeat, he leaned back and he looked flabbergasted, shocked, horrified,” Lazaro Dubrocq, now seventeen, told Time. “I was baffled. I mean, did we read something wrong? Was he mad or disappointed in us?”2 One of Dubrocq’s classmates, Mariah Williams, told Time that she would “always remember watching his face turn red.” She added, “I’m just glad he didn’t get up and leave, because then I would have been more scared and confused.” Bush’s facial reaction and delayed response after hearing this news (in other words, his decision to stay with the children rather than immediately spring into action) were famously lampooned by leftist documentarian Michael Moore in his film Fahrenheit 9/11, but this is not the reason I say that Bush’s initial reaction was unimpressive. There would be critics of virtually anything President Bush did just after learning that the country had been attacked, but his decision not to leave the classroom in emergency mode was imminently defensible. “The President told us his instinct was to project calm,” the 9/11 Commission Report noted, “not to have the country see an excited reaction at a moment of crisis.” Noticing that members of the press were learning about the attack through their cell phones and pagers, Bush reasonably decided that the best course was to “project strength and calm until he could better understand what was happening.”3 After concluding his time with the students, Bush went to a classroom where a secure phone had been set up. He spoke briefly to Vice President Dick Cheney, then gave his first address to the nation after the attacks. “Ladies and gentlemen,” President Bush said, “this is a difficult moment for America. Today, we’ve had a national tragedy. Two airplanes have crashed into the World Trade Center in an apparent terrorist attack on our country.” Bush was then rushed to Air Force One. Concerned that the president could be a target, his security detail wanted to keep him on the move until they had a better understanding of the threat. As Bush flew around the country, he clearly became frustrated by the situation. The TV signal on board Air Force One kept breaking up, and his calls to Vice President Cheney would lose reception.4 In the thick fog of war, Bush heard reports that Camp David and the State Department had been attacked, that there was a fire in the White House, and that his own ranch in Texas may have been targeted. Most critical were the fears that Air Force One could be a target. The president’s plane checked its internal security and also received two F-l 6s to escort it. Air Force One was cautious in the transmissions it sent, out of fear that they could be heard by the attackers. Although the concern that Air Force One could be targeted was understandable, these fears helped make President Bush’s reaction to the attacks less than impressive. Fie was generally invisible throughout the day, a situation that made strong leadership basically impossible. Bush touched down just before noon at Louisiana’s Barksdale Air Force Base to issue another brief statement to the nation. He then took off again, landing at Nebraska’s Offutt Air Force Base around 3 p.m. Bush stayed there for some time before finally being flown back to Washington. As 60 Minutes noted, the fact that Bush was largely out of touch for most of that fateful day raised doubts in the public’s mind. “Some wondered,” it said, “with the president out of sight, was he still running the government?”5 Fortunately, President Bush hit his stride rapidly. That night, back in Washington, he declared in an address to the country, “Today, our fellow citizens, our way of life, our very freedom came under attack in a series of deliberate and deadly terrorist acts.” Bush invoked the victims of 9/11, who were just going about their lives and their work when they were struck. The speech outlined several themes that would become his administration’s staples: al Qaeda’s targeting of the United States “because were the brightest beacon for freedom and opportunity in the world,” America’s resilience in the face of terrorism, the need to bring the full weight of the country’s resources to bear against those responsible, and his refusal to distinguish between the terrorists attacking America and the regimes harboring them. After quoting from Psalm 23—“Even though I walk through the valley of the shadow of death, I fear no evil, for You are with me”—President Bush declared that “none of us will ever forget this day, yet we go forward to defend freedom and all that is good and just in our world.”6 The speech was well received. As one British commentator said, it “was not the Gettysburg address, but it summed up admirably the trauma of his countrymen.”7 President Bush’s growing confidence was obvious later in the week, when he visited rescue workers digging through the rubble at ground zero. Grabbing a bullhorn to speak to them, he said, “I can hear you. And the rest of the world can hear you. And the people who knocked these buildings down will hear all of us soon!” He was greeted by chants of “USA! USA! USA!” Karen Hughes, who at the time served as an adviser on Bush’s public statements, told the New York Times, “At that moment, I thought America is seeing the President Bush that I know, his ability to relate to people.”8 Bush would give several more increasingly forceful speeches that month. The public’s connection with him was obvious; Bush’s approval ratings rose from 55 percent to over 90 percent within two weeks of the attack. His ratings would not stay at that level, and Bush would leave office a controversial and highly unpopular figure. But the remarkable rise in his ratings just after 9/11 showed the public’s fear, concern, and desire for action. It also showed why politicians would be so tempted to politicize terrorism. America’s Mayor New York City mayor Rudy Giuliani also found his fortunes dramatically changed by the 9/11 attacks. A former prosecutor known for his toughness, Giuliani had won two mayoral terms because of his ability to return good governance to the city, in particular for tackling its seemingly intractable crime problem. A profile of Giuliani published in Time in December 2001 noted that “he had restored New York’s spirit, cutting crime by two-thirds, moving 691,000 people off the welfare rolls, boosting property values and incomes in neighborhoods rich and poor, redeveloping great swaths of the city.”9 Despite these accomplishments, Giuliani’s popularity had eroded, and he was viewed as a divisive figure at the time of the 9/11 attacks. The controversy surrounding Giuliani was a result of his double- edged personality. On the one hand, his ego, tenaciousness, and combativeness actually served him well, leading him to believe he could govern the city that mayor after mayor had failed to fix. He exceeded all expectations when he proved to be right. On the other hand, even though crime had plunged, New Yorkers thought that this problem had been supplanted by police heavy-handedness, a perception that was bolstered by such incidents as the racially charged shooting of twenty-three-year- old Guinean immigrant Amadou Diallo by four New York City Police Department (NYPD) officers. There were multiple ways that Giuliani’s finicky, angry personality created further problems. Time explains: New York City was getting better, but the mayor seemed to be getting worse. When New York magazine launched an ad campaign calling itself “Possibly the only good thing in New York Rudy hasn’t taken credit for,” Giuliani had the ads yanked from the sides of city buses. The magazine sued and won. . . . Giuliani launched a “civility campaign” against jaywalkers, street vendors and noisy car alarms and a crusade against publicly funded art that offended his moral sensibilities. But the pose seemed hypocritical at best when Giuliani, whose wife had not been seen at City Hall in years, began making the rounds with Judi Nathan, a stylish New Yorker with wide, liquid eyes. The clash between the mayor’s life-style and his policies became a pop-culture target, deftly skewered by Saturday Night Live comedian Tina Fey. “New York Mayor Rudy Giuliani is once again expressing his outrage at an art exhibit, this time at a painting in which Jesus is depicted as a naked woman,” Fey deadpanned. “Said the mayor: ‘This trash is not the sort of thing that I want to look at when I go to the museum with my mistress.’”10 As Giuliani’s biographer, Fred Siegel, noted, it is impossible to separate Giuliani’s ego and intransigence from his success in running “ungovernable” New York City: these characteristics allowed him to stand up to entrenched interests and boldly act in ways that flouted the conventional wisdom. As Siegel writes, “You couldn’t pick and choose from among his virtues and vices. You had to take him whole.”11 But the mayor’s inspiring response to the 9/11 attacks caused these critical perceptions to recede. Giuliani projected not only leadership and toughness but also compassion. “Mayor Giuliani survived his own scrape with death,” the New York Daily News noted, referring to a close call with the collapse of the World Trade Center’s Building 7. “Consoled grieving families. Marshaled selfless rescue workers of the nation’s largest city. Worked tirelessly, almost around the clock.”12 The mayor took time to condemn the racial and religious hatred that might be directed at New York City’s Muslim community, a move that New Yorkers, and Americans as a whole, saw as genuine and laudable. Encapsulating the changing perceptions of the mayor, one scenic artist who was not a Giuliani supporter told the New York Times, “I have newfound love for him, for what he said about how we are a multicultural city, we can’t begin to single out cultures, harbor ill feelings. Fie sounded like a real leader. I didn’t feel that way about President Bush.”13 Giuliani became known as “America’s mayor,” an iconic figure who was instantly recognizable countrywide. Fie was named Time’s Person of the Year, and he became regarded as a viable presidential candidate. Fie did run for president in 2008, and early polls put Giuliani at the forefront of the Republican contenders. A January 2007 Washington Post-ABC News survey showed Giuliani leading Senator John McCain 34 percent to 27 percent among Republican-leaning voters.14 The following month, a Gallup poll showed Giuliani continuing to lead eventual nominee McCain, and the poll’s issue-by-issue breakdown made clear that the coolness and resolve that Giuliani had displayed on September 11 was his key political strength. Although McCain had some significant foreign-policy advantages over Giuliani in Republican eyes, Gallup noted that Giuliani enjoyed a clear edge over McCain on terrorism. “Giuliani’s widely praised response to the Sept. 11 terror attacks while serving as mayor of New York City is likely the reason for this,” Gallup stated, “and is enough to overcome the perhaps more general sense that McCain is better on international matters.”15 By May 2007, polls showed Giuliani handily beating the Democratic frontrunner, Senator Hillary Clinton, in a general election, and tying Senator Barack Obama. Britain’s Economist described these numbers as “extraordinary,” since the United States then had a “snarlingly anti-Republican mood.”16 A July 2007 Gallup poll inquiring about what voters perceived as the best and worst aspects of a Giuliani presidency found that Americans, by an overwhelming margin, identified “good on terrorism/security/handling of Sept. 11” as the most positive thing about having Giuliani in the White House.17 Giuliani ultimately did not receive the Republican nomination. There were multiple reasons for his loss, including his blemished personal life and a bizarre campaign strategy that involved skipping the Iowa caucuses, running halfhearted campaigns in both New Hampshire and South Carolina, and placing all his bets on winning the Florida primary.18 (Giuliani finished third in that critical contest.) Even though he was dealt a strong hand on terrorism issues, he may have overplayed it. Joe Biden famously commented in an October 2007 debate that Giuliani only mentions three things in a sentence: “a noun, and a verb, and 9/11.” But if Giuliani did overemphasize his response to those attacks, it was because he realized that it was such a political asset. Although Giuliani didn’t win the presidency, his experience confirms the political benefits of being seen as strong on terrorism. The Republicans Capitalize The fact that there were clear political benefits to being seen as strong on terrorism wouldn’t inevitably create a problem. After all, it could be healthy to motivate politicians to perform admirably under intense pressure, as Rudy Giuliani did. Rather, the problem was that terrorism became politicized as an issue within a year of the attacks in an incredibly divisive manner. A climate was created that has harmed rather than helped America’s effectiveness. The Republicans were able to capitalize in the 2002 midterm election on the fact that their party was identified as tougher on terrorism. Before the attacks, it seemed that the Republicans could face significant midterm losses. Layoffs and rising unemployment, projected to hit 5 percent by the beginning of 2002, created the risk that voters would punish the party.19 (The fact that 5 percent unemployment was considered a major political liability seems quaint today.) Moreover, Vermont senator James Jeffords’s sudden defection from the party after the 2000 election deprived Republicans of their control of the Senate. Prominent Republicans feared that this change could have a ripple effect, dampening donations and discouraging grassroots activism. Furthermore, they were concerned that being relegated to minority status in the Senate could discourage some Republicans from seeking reelection and make the recruitment of strong candidates more difficult.20 The 9/11 attacks, however, transformed the political landscape. Although the economy had been the voters’ predominant concern until terrorists struck the United States, Gallup polling from January to June 2002 consistently found that terrorism and national security had eclipsed the economy as the issue voters cared about most. (In July 2002, the economy again surpassed terrorism and national security, 40 percent to 30 percent.) And if terrorism was on voters’ minds, this was good for the Republicans. An August 2002 Gallup analysis noted that although Democrats had a six-point edge among all voters (48 percent to 42 percent), Republicans enjoyed a commanding nine- point lead among registered voters who considered terrorism to be the most important electoral issue.21 The Republicans exploited this national security advantage. Karl Rove, a senior adviser to President Bush whom the president would later refer to as “the Architect” of his 2004 electoral victory, said in January 2002 that the fight against terrorism would help the Republicans because voters “trust the Republican Party to do a better job of protecting and strengthening America’s military might and thereby protecting America.” During the campaign, Rove misplaced a computer disk that contained his PowerPoint presentations about the upcoming midterm election. One piece of advice to candidates in the presentations was that they should “focus on the war” in their campaigns.22 Rove’s advice proved controversial once the public learned of it, but the issue resonated with voters, as did President Bush’s focus on selling the coming Iraq War during the campaign. Time reported that in private, “Republicans concede that Bush’s focus on Iraq has vastly improved their chances in November and bless Rove for his efforts.”23 The Democrats complained loudly. In September 2002, the Washington Post quoted President Bush as saying at a GOP fundraiser in New Jersey, “Democrats are not interested in the security of the American people.” When Senate Majority Leader Tom Daschle demanded an apology, the White House argued that the quote was not as incendiary as it initially appeared when understood in its context. The White House claimed that Bush had in fact criticized the Senate for slowing down the creation of a Cabinet-level Department of Homeland Security. Rather than saying that the Democrats were uninterested in national security, he had said that “the Senate is more interested in special interests in Washington and not interested in the security of the American people.”24 Daschle would hear none of this. Saying that the White House’s explanations about context were “not worth the paper they are printed on,” he continued to demand an apology. “We ought not to politicize this war,” Daschle said. “We ought not to politicize the rhetoric about war and life and death.” (Senate Minority Leader Trent Lott responded to Daschle with a bizarre non sequitur: “Who is the enemy here, the president of the United States or Saddam Hussein?”) The bottom line is that Daschle was right: politicizing national security when there was general agreement between the Republicans and the Democrats on how to combat terrorism was bad for the country. After all, the actual point of contention that had caused Bush to claim that the Senate was “not interested in the security of the American people” was whether civil service protections should be preserved for employees of the new Department of Homeland Security. I do not want to diminish the significance of this issue: the dispute was legitimate, representing a genuine philosophical disagreement between the two parties. But the Republicans and the Democrats agreed on the need to create the department and were capable of forging ahead without the kind of incendiary accusations that Bush made. Rather than taking advantage of the opportunity to try to create a consensus paradigm on national security issues (albeit one that would feature inevitable differences between the parties), the Republicans helped to create an environment where national security was a constant point of contention. In this environment, safeguarding the country often took a backseat to opportunities for partisan gain. But even though Daschle was right philosophically, the Republicans read national politics correctly. They regained control of the Senate in the 2002 election, picked up five seats in the House, outperformed expectations in the gubernatorial races, and even gained in state legislatures. In general, the president’s party averages a loss of 350 state legislature seats in a midterm election, but in this one the Republicans actually gained 200 seats.25 The GOP’s overwhelming victory was not just unexpected but also historic: not since Franklin D. Roosevelt in 1934 had a president’s party made gains in both the House and the Senate during the midterm election of his first term in office.26 Terrorism was the key to this victory. Afterward, Democratic Party chairman Terry McAuliffe commented that the Republicans derived significant political advantages from the war on terrorism as well as the looming war with Iraq. “You put all that together with the President out there actively campaigning,” he said, and it added up to a Democratic defeat.27 McAuliffe’s perception of why the Democrats lost squared precisely with the Republican game plan. A Newsweek investigative report published in mid-November 2002 concluded that Bush and his advisers had formulated a three-part plan for electoral victory by August: “to raise the stakes and lengthen the debate on our dealings with Iraq, to press the Democrats to accept the White House version of a Department of Homeland Security (and hammer them if they opposed it) and to deploy both issues to burnish the president’s popularity with the GOP faithful, to whom Bush would appeal in coast-to-coast campaigning in the final weeks of the 2002 campaign.”28 Summarizing what many commentators had come to realize after the midterm election, conservative columnist Charles Krauthammer wrote, “Why did the Democrats lose? Forget the tactics. Forget the fundraising. Forget even the President’s popularity. This election was about Sept. II.”29 The 2004 Election Terrorism and national security would continue to be a critical, divisive issue for the next few election cycles. It was clear from the outset that terrorism would factor heavily in the 2004 campaign. The Republicans’ choice of New York City as the location for that year’s Republican National Convention and their decision to hold it in September were obvious references. As Brookings Institution govern-ment scholar Stephen Fless told CNN, “Terrorism is why they’re in New York and why they’re doing it at the beginning of September. It’s not very subtle.”30 Terrorism was invoked almost constantly throughout the convention. In a speech that mentioned terror or terrorism forty-four times, and 9/11 eleven times, Rudy Giuliani said, “President Bush sees world terrorism for the evil that it is. John Kerry has no such clear, precise and consistent vision.”31 Arnold Schwarzenegger claimed in his convention speech, “If you believe we must be fierce and relentless and terminate terrorism, then you are a Republican!”32 (Though not as ubiquitous as Giuliani’s invocations of 9/11, Schwarzenegger’s references to the Terminator movie series have been every bit as consistent when he has spoken publicly and privately.)33 Although the Iraq War clearly helped the Republicans in the 2002 election, by 2004 the public perception was mixed. The death toll, both American and Iraqi, was mounting. So too were the economic costs of the war. And an intensive search had failed to unearth evidence that Saddam Hussein had rebuilt his nuclear weapons program—which was the central claim the Bush administration had used to justify its invasion. Kerry, Bush’s rival in the general election, campaigned on the idea that the invasion had been “the wrong war, in the wrong place, at the wrong time.”34 President Bush’s campaign would not—in all likelihood, could not—back down from its claim that the Iraq War had been good for America. Instead, it linked that war to the broader fight against terrorism and positioned Bush as the only candidate Americans could trust with keeping the country safe. One line of attack for the Bush campaign was the so-called Kerry Doctrine. Speaking of Bush’s decision to undertake preemptive warfare against Iraq, Senator Kerry had said he would preemptively attack another country only when doing so “passes the global test where your countrymen, your people understand fully why you’re doing what you’re doing, and you can prove to the world that you did it for legitimate reasons.”35 Labeling this idea of a “global test” the Kerry Doctrine, President Bush insisted that it was radical and dangerous. “Think about this,” Bush said during an Ohio campaign stop less than a month before the election. “Senator Kerry’s approach to foreign policy would give foreign governments veto power over our national security decisions.” In contrast, Bush said that in his administration, “our national security decisions will be made in the Oval Office, not in foreign capitals.”36 Naturally, Senator Kerry took issue with the way the Bush campaign had portrayed the Kerry Doctrine. In addition to criticizing Senator Kerry’s “global test,” President Bush argued that the invasion of Iraq made America safer—period. In the first of three presidential debates, he argued that one critical lesson of 9/11 was to “take threats seriously, before they fully materialize.” Because of the U.S. invasion of Iraq, he said, “Saddam Hussein now sits in a prison cell. America and the world are safer for it.” Later in the debate, Bush said that Kerry’s criticism of the Iraq War reflected a “pre-September 11th mentality, the hope that somehow resolutions and failed inspections would make this world a more peaceful place.”37 Similarly, in the vice presidential debate, Dick Cheney said that if he had to decide whether to recommend war with Iraq all over again, he would take the same course. “The world is far safer today because Saddam Hussein is in jail,” Cheney said. “His government is no longer in power. And we did exactly the right thing.” He said that in contrast, he didn’t think Kerry “would pursue the kind of aggressive policies that need to be pursued if we’re going to defeat these terrorists.” Invoking one of the antiterrorism paradigms that the government adopted in the immediate wake of the 9/11 attacks, Cheney concluded that “we need to battle them overseas so we don’t have to battle them here at home.”38 For his own part, Kerry did himself few favors on these issues. For example, the Democrats were eager to capitalize on the popularity of Michael Moore’s Fahrenheit 9/11, a documentary critiquing the Iraq War. Moore spoke at several events at the Democratic National Convention in Boston, and the cameras caught him sitting next to former president Jimmy Carter during part of the convention. The problem is that Moore was more than just an antiwar filmmaker. In one statement on his personal website, posted about three months before the convention, he wrote: “The Iraqis who have risen up against the occupation are not ‘insurgents’or ‘terrorists’or ‘The Enemy.’ They are the REVOLUTION, the Minutemen, and their numbers will grow—and they will win. Get it, Mr. Bush?”39 Rather than simply disagreeing with the war, this post celebrated the insurgents who were killing American forces—and it generated justifiable controversy. Predictably, the image of Moore sitting next to Carter featured prominently on conservative cable news shows, making the concerns that the Bush campaign raised about Kerry’s seriousness on national security issues seem credible to many voters. As election day neared, the Bush campaign continued to emphasize its national security bona fides. Typical of the campaign’s rhetoric, President Bush clearly framed the issue during one stop in Pennsylvania: “A crucial difference between my opponent and me is the most important question for voters this election: Who can lead this war against terror to victory? Which candidate can best protect America’s families and our national security?”40 Then on October 29, mere days before the election, Osama bin Laden appeared in a video address that was broadcast on the A1 Jazeera Arabic-language satellite station. Obviously timed to coincide with the U.S. election, bin Laden addressed the American people directly. In the speech, he boasted that al Qaeda was winning its war against the United States. The primary reason he gave was the economics of the fight and his group’s strategy of “bleeding America to the point of bankruptcy.” Explaining that al Qaeda alone could not be credited with the coming victory, bin Laden said that the Bush administration’s decision to open multiple war fronts was also bringing about America’s downfall. “And so it has appeared to some analysts and diplomats,” bin Laden said, “that the White House and us are playing as one team towards the economic goals of the United States, even if the intentions differ.”41 The voting public was largely uninterested in the substance of bin Laden’s speech. Rather, the most significant aspect to Americans was that the video showed that bin Laden was still alive. Before that, bin Laden featured infrequently in al Qaeda’s propaganda, and it had been years since he’d appeared in a video, leading many commentators to believe that he had been killed. (Baseless rumors that bin Laden was in ill health, forced onto a dialysis machine by kidney problems, further bolstered these conclusions.)42 Bin Laden’s video dominated the news cycle in the days leading up to the election, again putting national security at the forefront of voters’minds. President Bush won the election in 2004, and the GOP again made gains in both the House and the Senate. Party insiders correctly pointed to national security as a critical issue. The Democrats Capitalize, Too By 2006, national security issues had been transformed from a significant Republican advantage into a thorn in the party’s side. The overarching reason was the Iraq War. Bloodshed markedly increased in that country during the course of the year, and many observers thought it was mired in civil war. Certainly anything resembling a victory appeared implausible. An event that had a major impact on the war was the February 22, 2006, destruction of the Golden Dome Mosque in Samarra, a major holy site for Iraq’s Shia community and for Shiites throughout the world, in a bombing ordered by the leader of al Qaeda in Iraq (AQI), Abu Musab al Zarqawi. The Golden Dome Mosque’s importance to the Shia community was underscored by Iraqi vice president Adel Abdul Mahdi, who likened the attack to 9/11.43 Some observers believe that this attack dramatically reshaped the war, whereas others think that it was an indicator of an already existing instability rather than a trigger. Taking the latter position, Pulitzer Prize-winning journalist Thomas Ricks noted that “according to the United States military’s database of ‘significant acts,’violence had increased at a steady pace since March 2005 and would continue to increase at about the same pace after the mosque bombing until peaking in June 2007.”44 Regardless, it’s clear that the mosque attack did produce a ripple effect. Shiite reprisals against Sunnis were swift, devastating, and largely indiscriminate. The Sunnis struck back, often with AQI taking the lead. Some Sunnis found allegiance with al Qaeda to be advantageous in protecting them from sectarian bloodshed. For other Sunni insurgents, bloody attacks orchestrated by Shiite militias made some of al Qaeda’s sectarian arguments seem sensible for the first time. (Zarqawi referred to the Shia as “the insurmountable obstacle, the lurking snake, the crafty and malicious scorpion, the spying enemy, and the penetrating venom.”)45 The fact that AQI came to the fore of the Sunni insurgency during this period has been verified by insurgents who later changed sides.46 By the time Americans turned out to vote in the 2006 midterm election, the cycle of violence in Iraq was clearly spiraling out of control, and the damage seemed irreparable. AQI had been able to take and hold territory. It became the dominant player in Iraq’s expansive Anbar province and was able to erect a governing structure in the city of Mosul.47 As the situation deteriorated, the Democrats realized that this time, unlike in the last two elections, the Republicans were vulnerable on the issue of terrorism and national security. Democratic senator Evan Bayh of Indiana said in February 2006 that “for both substantive and political reasons,” the Democrats should take the Republicans on over terrorism and national security.48 Indeed, Senate Democrats took advantage of the anniversaries of 9/11 and the Hurricane Katrina disaster to argue that Bush and the Republicans hadn’t done enough to safeguard Americans from terrorism and from other threats they faced.49 The Republicans were viewed as vulnerable on national security in general, but Democratic strategists saw Iraq as their Achilles’heel. Key Democratic politicians promised to push for immediate withdrawal. Indicative of the mood within the party was Connecticut’s senatorial race, where long-serving Democratic senator and former vice presidential candidate Joe Lieberman—who supported the U.S. efforts in Iraq— lost a primary challenge to Ned Lamont, who campaigned on his opposition to the Iraq War. Lamont wanted to withdraw American troops within a year. Lieberman, a popular and powerful figure in Connecticut politics, decided to run in the general election as an independent, and he was expected to caucus with the Democrats if he prevailed. Yet despite Lieberman’s long service to the party and his vice presidential nomination just six years earlier, key colleagues threw their support behind Lamont. John Kerry sent a fundraising appeal to millions of supporters on behalf of Lamont, as well as on behalf of Senate candi-dates in New Jersey and Hawaii, making clear that Iraq and defense issues were the reason. “Each of these candidates is making the mess in Iraq a central issue in their campaigns for the Senate,” he wrote.50 Other Democratic politicians, including Representative Jack Murtha of Pennsylvania and Senator Russell Feingold of Wisconsin, likewise called for a quick withdrawal. Campaigning on national security issues again paid off in 2006, this time for the Democrats, who took back the House and the Senate. According to late November polling data from the Pew Research Center, 53 percent of Americans considered the Iraq War one of the top two issues in the election.51 ABC News analyst Gary Langer noted, “Opposition to the war remains the prime issue driving congressional voter preference. And the war’s critics include not just eight in 10 Democrats but 64 percent of independents, 40 percent of conser-vatives, 35 percent of evangelical white Protestants and a quarter of Republicans.”52 Although Iraq had been central to the GOP’s defeat, President Bush did not hasten to withdraw after the election. Instead, he announced a “surge,” an increase in the presence of American soldiers in an attempt to clear out al Qaeda’s strongholds and diminish sectarian violence. There was nothing wrong with the Democrats campaigning on national security issues: the Iraq War was incredibly costly and there was a strong argument for political accountability But many Democrats went beyond this, arguing that Bush’s surge ignored the “mandate” provided by the American people to get the U.S. military out of Iraq as soon as possible. They first registered this disapproval by passing House Resolution 157, which condemned Bush’s decision to send more soldiers to Iraq. Speaking in favor of the resolution, Representative Dale Kildee of Michigan said, “President Bush either did not get or did not understand the message the American people sent last November. Before the end of this year, United States troops should be redeployed and their efforts focused on support and training the Iraqi Security Forces.”53 Representative Kirsten Gillibrand of New York mentioned her own constituency’s vote, saying, “Last November the voters in upstate New York spoke loudly and clearly in demanding a change in direction in Iraq, and I will cast my vote in favor of this resolution to fulfill my duty to represent their will.” Representative Joe Courtney of Connecticut also referred to the 2006 vote: “Today we are here, exactly 100 days after a historic watershed election in this country, in which the American people spoke loudly and clearly that they wanted a new Congress to rise to its constitutional duty and hold this administration accountable for its war policy in Iraq. The day I was sworn in as a new Member of Congress, I accepted this responsibility, and I rise today in opposition to the President’s escalation of the war.” Although it passed, House Resolution 157 was nonbinding. However, the dispute over the surge between the White House and Congress produced funding battles, raising the question of whether the legislature would use its power of the purse to deprive the White House of the funds it required to execute the surge. One of the surge’s most consistent critics was Illinois senator Barack Obama. On January 10, 2007, as the surge was announced, Obama said, “I am not persuaded that 20,000 additional troops in Iraq is going to solve the sectarian violence there. In fact, I think it will do the reverse.” Obama swore that he would “actively oppose the president’s proposal.”54 In May 2007, Obama introduced a plan to begin redeploying troops out of Iraq, with all combat troops to be removed by March 31, 2008. Ultimately, the surge was given the funding that it needed, and—as will be discussed in detail later—it worked. Although serious questions remain as the United States draws down its troops, President Bush made the right decision by undertaking a surge rather than a withdrawal. This is particularly true when one recalls the dark days of 2007, when Iraq was wracked by sectarian violence and ethnic cleansing and AQI was able to carve out geographic safe havens. Obama himself conceded in a September 2008 interview with Fox News Channel host Bill O’Reilly, “I think that the surge has succeeded in ways that nobody anticipated. . . . It’s succeeded beyond our wildest dreams.”55 But in the highly politicized context in which debates over national security issues take place, the results of the 2006 midterm election were used to argue that President Bush should have chosen a course of action that would have been worse for the country. And it was not just Democrats who employed the election results in this manner. “By step- ^ ping up the American military presence in Iraq, President Bush is not ^ only inviting an epic clash with the Democrats who run Capitol Hill,” Sheryl Gay Stolberg wrote in a news analysis column for the New York Times. “He is ignoring the results of the November elections, rejecting the central thrust of the bipartisan Iraq Study Group and flouting the advice of some of his own generals, as well as Prime Minister Nuri Kamal al Maliki of Iraq.”56 The 2008 and 2010 Elections National security and terrorism was not the key election issue in either 2008 or 2010 that it had been previously; the September 2008 financial crisis caused economic issues to overshadow everything. This does not mean, however, that the issue was entirely absent. By 2008, Bush’s approval rating was microscopic, and he was considered politically toxic. The Republican nominee, Senator John McCain, found himself in the unique position of running a general-election presidential campaign that took aim at his own party’s incumbent. The Democratic nominee, Senator Barack Obama, ran against the Bush administration virtually across the board, including on national security. When the Obama administration took office after a resounding electoral victory, the new president trumpeted the new direction he would take on terrorism and foreign affairs. His efforts appeared so derogatory toward the Bush administration’s approach that they prompted Juan Zarate, President Bush’s counterterrorism advisor, to tell NPR, “I don’t think the administration has helped themselves, or frankly helped the country, by trying so hard to paint their policies as being so radically different from the past. They’re not, and for the sake of the country they shouldn’t be.”57 Zarate was right. Although Obama swore on the campaign trail that his national security efforts would differ markedly from those of his predecessor, and although he made considerable efforts during his first year in office to show the public that substantive differences existed, Obama’s CounterTerrorism policies have largely been a continuation of those forged during the last two years of the Bush administration. Some conservative pundits still attempt to show Obama’s overarching weakness on national security, and a select few portray him as dangerous, but there is a growing awareness among analysts of the continuity between Bush and Obama on counterterrorism policy.58 Indeed, national security was marginal as an issue in the 2010 midterm election. One Republican pollster noted during that campaign that the economy “dwarfs everything. It’s sort of like looking at a house and there’s all these things that need repair, but if the roof’s on fire, all these things are secondary. Jobs and the economy are the equivalent of the fire on the roof.”59 An ABC News analysis of the election results found that the economy, health care, and illegal immigration were the top three issues for voters. The Afghanistan War came in a distant fourth, with only 7 percent of voters citing it as their top concern.60 From 2002 through 2008, the politicians and parties that benefited from their politicization of terrorism and national security got a number of significant substantive points wrong. In 2002, the Republicans were wrong to politicize the issue in the first place. Moreover, the midterm results were viewed by many as a mandate for the disastrous invasion of Iraq. In 2004, President Bush’s winning campaign insisted that the country was safer due to this invasion and that the administration would change neither its decision to go to war nor its execution of the conflict if given the opportunity. Not only did the invasion not make the United States safer, but the situation in Iraq would not improve until the administration dramatically changed its approach. The Democrats finally gained some advantage from Bush’s foreign policy failures in the 2006 election, but they promptly interpreted the vote as a mandate to get out of Iraq while it was mired in civil war and al Qaeda enjoyed a significant foothold. They used the 2006 results as a bludgeon with which to attack the surge that would help to reverse that dangerous situation. And in 2008, Obama exaggerated the aspects of Bush’s counterterrorism policies that should be changed, even making campaign promises that he couldn’t keep in an attempt to capitalize on the issue. The good news is that because of the continuity between the Bush and Obama administrations on terrorism and national security, as well as waning voter interest, it may be possible to eliminate some of the harmful partisanship that has produced a suboptimal policy. Later I will address how this can be done. For now, what matters is that after the 9/11 attacks, politicians immediately realized how terrorism could benefit them and their parties as a campaign issue. This politicization in turn contributed to the misallocation of resources designed to serve counterterrorism purposes and to the inefficiency of efforts that were actually important to public safety. This book now turns to these twin problems.

#### Economic collapse causes nuclear war

Merlini 11

[Cesare Merlini, 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? DOI: 10.1080/00396338.2011.571015 Article Requests: Order Reprints : Request Permissions Published in: journal Survival, Volume 53, Issue 2 April 2011 , pages 117 - 130 Publication Frequency: 6 issues per year Download PDF Download PDF (357 KB) View Related Articles To cite this Article: Merlini, Cesare '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 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.

#### Reject the 1AC’s communicative approach to approaching the terrorist threat ---- No link turn or permutation ---- disparate practices like the plan collapses the alternative

LYNCH 2010 - Associate Professor of Political Science and the Director of the Institute for Middle East Studies at the George Washington University, Elliott School of International Affairs; the editor of the Middle East Channel on ForeignPolicy.com; and a Non-Resident Senior Fellow at the Center for a New American Security (Lynch, Marc, “Rhetoric and Reality: Countering Terrorism in the Age of Obama”, http://www.cnas.org/files/documents/publications/CNAS\_Rhetoric%20and%20Reality\_Lynch.pdf)

The Obama[’s] administration’s strategy has been multifaceted and well-conceptualized, building clearly upon the successful adaptations made by the Bush administration in its final years, and has seen success in a number of ways. The administration has struggled, however, to communicate this new approach in a clear way or to change significantly the legal foundations of the "Global War on Terror." The new rhetorical focus and practices do not yet seem either durable enough to withstand a major setback, such as another unpopular war in the Middle East or a successful terrorist attack on the American homeland. Problems remain with coordinating counterterrorism efforts across the government and with unresolved tensions about the appropriate relationship between global engagement and CVE. Furthermore, it is not clear that the United States is adapting well to the new domestic aspect of the challenge. To fully deliver on the promise of the Obama administration’s approach and create an effective strategy, the administration should: Articulate and Institutionalize the Strategy The National Security Strategy clearly lays out a guiding framework for combating al Qaeda and its affiliates within a broader foreign policy vision. A new counterterrorism strategy should then reshape the legal authorities and programming which have, for the last eight years, been framed around the “Global War on Terror.” Coining a new term for the administration’s strategy is not simply an exercise in public relations or branding. An old frame will not be displaced without something credible to replace it, and the administration needs to provide that alternative. To do this, the administration needs to articulate a compelling alternative that makes sense of its disparate actions to relevant domestic and foreign audiences, and that can guide the reorganization of government programs and authorities. Adapt, but Don’t Overreact, to New Domestic Threats The rising concerns surrounding domestic radicalization and the transnational mobilization of threats to the homeland should galvanize action across the government without causing overreaction. The National Security Strategy rightly warns of the need to "resist fear and overreaction" in the face of terrorist attacks and provocations.109 The administration should resist, and push back hard against, public demands to respond to domestic threats by taking actions that would alienate American Muslims and threaten civil liberties; an example would be Senator Joseph Lieberman’s suggested legislation to strip suspected terrorists of their American citizenship.110 Internationally- and domestically-oriented agencies need to work together and overcome cultural and legal barriers. The domestic challenge should employ the same multi-layered, disaggregated strategy as in the international realm: broad-based engagement with Muslim communities, targeted efforts against violent extremists, continuing vigilance by law enforcement and renewed respect for the rule of law. Better Integrate Global Engagement and Countering Violent Extremism The reasons to separate global engagement from CVE are compelling, but they must be coordinated as part of an overall strategy for both to be fully effective. The United States should continue its efforts to reach out to mainstream Muslim communities by building networks around issues of common interest, and to make progress on core political issues that galvanize the mainstream of the Arab and Muslim worlds and affect their willingness to cooperate with America – including the Israeli-Palestinian issue. At the same time, CVE efforts should seek to prevent the extremist narrative from hijacking those mainstream grievances and multiplying the appeal of extremists who seem to offer better explanations for those problems than do their more mainstream rivals. These efforts should not ease up on disrupting and challenging extremist messaging and propaganda. Engagement and CVE efforts help to eliminate the “demand side” for extremist appeals and help create environments in which extremist groups and ideas are rejected. Even if this engagement is not framed around CounterTerrorism, global engagement and CVE should be coordinated as part of a coherent strategy for marginalizing al Qaeda and building support for U.S. objectives and interests around the world. Think Holistically Difficult counterterrorism decisions should take into consideration the effects on other parts of the integrated strategy – global engagement, CVE and the rule of law – when calculating costs and benefits. For example, if drone strikes inflame local sentiments against the United States, fuel extremist narratives or compromise efforts to restore the rule of law, then those potential costs should be taken fully and explicitly into account during the decision making process. Similarly, the costs, in terms of both Muslim engagement and CVE, of not living up to rule-of-law commitments – such as closing Guantanamo or bringing suspected terrorists to trial in civilian courts – should be included in those difficult decisions. Policies designed to confront al Qaeda’s affiliates in places such as Yemen, Somalia, and the Maghreb must not fall into the trap of focusing exclusively on al Qaeda. Taking a holistic approach will ensure that various layers of the strategy reinforce one another. The NSC-led interagency process should include representatives of each priority in discussions of such policies in order to ensure coherent cooperation toward a common strategic objective. Prepare for the Worst A successful attack linked to an Islamist network in the United States seems likely at some point given the plethora of soft targets and the evident interest by al Qaeda and its affiliated movements. Even the most effective counterterrorism strategy cannot prevent every attack, and perfect security will never be achieved. The administration should prepare its response to such a successful attack well in advance, with clear communications designed to demonstrate American resilience and commitment to its current strategy. All of these recommendations point toward one final master imperative: preventing the return to a spiral of conflict between the United States and an undifferentiated “Islam.” Abroad and at home, the U.S. goal must be to dispel al Qaeda’s narrative that the United States is at war with Islam and to prevent extremist voices from again hijacking America’s relationship with the Muslim world. The spate of recent terrorist incidents should not lead the United States to jettison what has been working and bring back “Global War on Terror” rhetoric and practice that only serves to strengthen al Qaeda’s hand. The Obama administration is on the right track, but much remains to be done to translate strategic commitments into operational practice and bureaucratic reality. It must soon adapt to the changing nature of the threat or risk seeing its comprehensive strategy collapse.

### 1nc

#### The executive branch of the United States should:

- remove barriers that discourage information sharing between public-private entities

- create a cyber-liability system

- establish a non-profit organization that would evaluate and accredit technology companies’ supply chain security

- allow more internal self-defense measures by private entities

- encourage more professional base-level training and early STEM education

- promote international cyber security outreach efforts

as advocated per our Bucci et al evidence

#### That solves and avoids our net benefits

Bucci et al 13 ( Steven P. Bucci, Ph.D. Director, Douglas and Sarah Allison Center for Foreign Policy Studies , Paul Rosenzweig Visiting Fellow at the Heritage Foundation, David Inserra Research Assistant, National Security and Cyber Security, The Heritage Foundation, "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace", http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace, 4-1-13)

A Cybersecurity Policy that Works

Congress should pursue a cybersecurity policy that avoids a cumbersome and expensive regulatory approach and includes the seven key elements detailed there that will produce truly dynamic cybersecurity defenses. Such an approach should:

Enable cyber information sharing by removing ambiguities, providing strong protections to sharers, and establishing a public-private partnership to facilitate sharing. Entities that share cybersecurity information need certain protections. These protections include exempting all shared information from FOIA requests and regulatory use, and providing information sharers with strong liability protection. Effective information sharing requires the government to share fully and in a timely manner with the private sector through a public-private partnership established for this purpose.

Promote the development of a viable cybersecurity liability and insurance system. Liability for irresponsible cybersecurity actions should be established through common law development. This process may need some initial incentives from the government, but, ultimately, such a system returns cybersecurity liability to those who are largely responsible for cybersecurity losses. The natural establishment of a cyber insurance community will then assist in the administration of risk assessments and foster improved security methodologies.

Encourage the creation of cyber-supply-chain security ratings. Such ratings should be granted by a nonprofit organization that will assess the surety of an organization’s supply chain, similar to how Underwriters Limited assesses the safety of various commercial products. By promoting such ratings, consumers will be able to make risk-based decisions and support better security by tying it to their profit motive.

Clarify boundaries and standards for cyber self-defense. The terms of an entity’s right to self-defense must be set within reasonable limits. Such terms would allow entities with the correct capabilities to take active measures to protect themselves without usurping the responsibility or authority of the federal government.

Advocate more private-sector awareness, education, and training for the general population. Such an effort will ensure that the American public becomes an asset, not a liability, in the struggle. Making the public more aware, without hype or feel-good security measures, is a start. Ongoing cyber education for the general workforce must also be promoted through standardized yet dynamic education programs, most likely originating in the private sector. This must be a major priority, not a minor ancillary effort.

Alter technical education and clearance practices to encourage the development of a cyber workforce. A well-trained cyber workforce is critical to the task facing America. The U.S. should promote STEM education and adjust visa, security clearance, and certification practices to attract, train, and retain the very best personnel for America’s key public-sector and private-sector entities. This requires issuing more security clearances as appropriate and emphasizing cyber certification and credentialing programs. Achieving the workforce needed requires the U.S. to more effectively leverage its cybersecurity personnel, whether that is integrating military personnel into cyber efforts, or tapping highly skilled hackers who would normally not be eligible to work for businesses or government agencies.

Lead international cyber engagement. The U.S. should lead international efforts to “name and shame” nations that use the cyber realm for malicious purposes, either against other nations or their own people. Additionally, the U.S. must respond to aggressive cyber campaigns by other nations by causing those nations to feel diplomatic and economic pain to deter cyber aggression. The U.S. response should include ceasing naive cooperation, curtailing visas for guilty parties, and subjecting those with stolen information and intellectual property to criminal charges and other legal action. Furthermore, many bad cyber actors also maintain some form of control over the Internet in their country. The U.S. should explore ways to weaken these nations’ grip on the Internet in order to weaken their control of the populace. All of these efforts should be tied to the completion of a coherent national conversation concerning the entire array of cyberspace issues.

Cybersecurity is one of the most critical issues the U.S. faces today. The threats are real and the need is pressing. Despite the best intentions of those involved with previous cyber legislative efforts, a regulatory basis simply will not work. It will not improve security and may actually lower it by providing a false level of comfort and tying the private sector down with outdated regulations. Cyberspace’s dynamic nature must be acknowledged and addressed by policies that are equally dynamic.

#### plan would uniquely decimate Obama and the military’s ability to calm alliances and deter enemies through cyber arms --- Makes terrorism and global nuclear war more likely --- INDEPENDENTLY prevents ability to negotiate north Korean miscalc

WAXMAN 2013 - law professor at Columbia Law School, co-chairs the Roger Hertog Program on Law and National Security (Matthew Waxman, “The Constitutional Power to Threaten War,” August 27, 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2316777)

As a prescriptive matter, Part II also shows that examination of threatened force and the credibility requirements for its effectiveness calls into question many orthodoxies of the policy advantages and risks attendant to various allocations of legal war powers, including the existing one and proposed reforms.23 Most functional arguments about war powers focus on fighting wars or hostile engagements, but that is not all – or even predominantly – what the United States does with its military power. Much of the time it seeks to avert such clashes while achieving its foreign policy objectives: to bargain, coerce, deter.24 The President’s flexibility to use force in turn affects decision-making about threatening it, with major implications for securing peace or dragging the United States into conflicts. Moreover, constitutional war power allocations affect potential conflicts not only because they may constrain U.S. actions but because they may send signals and shape other states’ (including adversaries’) expectations of U.S. actions.25 That is, most analysis of war-powers law is inward-looking, focused on audiences internal to the U.S. government and polity, but thinking about threatened force prompts us to look outward, at how war-powers law affects external perceptions among adversaries and allies. Here, extant political science and strategic studies offer few clear conclusions, but they point the way toward more sophisticated and realistic policy assessment of legal doctrine and proposed reform. More generally, as explained in Part III, analysis of threatened force and war powers exposes an under-appreciated relationship between constitutional doctrine and grand strategy. Instead of proposing a functionally optimal allocation of legal powers, as legal scholars are often tempted to do, this Article in the end denies the tenability of any such claim. Having identified new spaces of war and peace powers that legal scholars need to take account of in understanding how those powers are really exercised, this Article also highlights the extent to which any normative account of the proper distribution of authority over this area depends on many matters that cannot be predicted in advance or expected to remain constant.26 Instead of proposing a policy-optimal solution, this Article concludes that the allocation of constitutional war powers is – and should be –geopolitically and strategically contingent; the actual and effective balance between presidential and congressional powers over war and peace in practice necessarily depends on fundamental assumptions and shifting policy choices about how best to secure U.S. interests against potential threats.27 I. Constitutional War Powers and Threats of Force Decisions to go to war or to send military forces into hostilities are immensely consequential, so it is no surprise that debates about constitutional war powers occupy so much space. But one of the most common and important ways that the United States uses its military power is by threatening war or force – and the constitutional dimensions of that activity receive almost no scrutiny or even theoretical investigation. A. War Powers Doctrine and Debates The Constitution grants Congress the powers to create military forces and to “declare war,”28 which the Supreme Court early on made clear includes the power to authorize limited uses of force short of full-blown war.29 The Constitution then vests the President with executive power and designates him commander in chief of the armed forces,30 and it has been well-accepted since the Founding that these powers include unilateral authority to repel invasions if the United States is attacked.31 Although there is nearly universal acceptance of these basic starting points, there is little legal agreement about how the Constitution allocates responsibility for the vast bulk of cases in which the United States has actually resorted to force. The United States has declared war or been invaded only a handful of times in its history, but it has used force – sometimes large-scale force – hundreds of other times.32 Views split over questions like when, if ever, the President may use force to deal with aggression against third parties and how much unilateral discretion the President has to use limited force short of full-blown war. For many lawyers and legal scholars, at least one important methodological tool for resolving such questions is to look at historical practice, and especially the extent to which the political branches acquiesced in common practices.33 Interpretation of that historical practice for constitutional purposes again divides legal scholars, but most would agree at least descriptively on some basic parts of that history. In particular, most scholars assess that from the Founding era through World War II, Presidents and Congresses alike recognized through their behavior and statements that except in certain narrow types of contingencies, congressional authorization was required for large-scale military operations against other states and international actors, even as many Presidents pushed and sometimes crossed those boundaries.34 Whatever constitutional constraints on presidential use of force existed prior to World War II, however, most scholars also note that the President asserted much more extensive unilateral powers to use force during and after the Cold War, and many trace the turning point to the 1950 Korean War.35 Congress did not declare war in that instance, nor did it expressly authorize U.S. participation.36 From that point forward, presidents have asserted broad unilateral authority to use force to address threats to U.S. interests, including threats to U.S. allies, and that neither Congress nor courts pushed back much against this expanding power.37 Concerns about expansive presidential war-making authority spiked during the Vietnam War. In the wind-down of that conflict, Congress passed – over President Nixon’s veto – the War Powers Resolution,38 which stated its purpose as to ensure the constitutional Founders’ original vision that the “collective judgment of both the Congress and the President will apply to the introduction of United States Armed Forces into hostilities, or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, and to the continued use of such forces in hostilities or in such situations.”39 Since then, presidentialists have argued that the President still retains expansive authority to use force abroad to protect American interests,40 and congressionalists argue that this authority is tightly circumscribed.41 These constitutional debates have continued through the first decade of the 21st century. Constitutional scholars split, for example, over President Obama’s power to participate in coalition operations against Libya without congressional authorization in 2011, especially after the War Powers Resolution’s 60-day clock expired.42 Some argue that President Obama’s use of military force without specific congressional authorization in that case reflects the broad constitutional discretion presidents now have to protect American interests, at least short of full-blown “war”, while others argue that it is the latest in a long record of presidential violations of the Constitution and the War Powers Resolution.43 B. Threats of Force and Constitutional Powers These days it is usually taken for granted that – whether or not he can make war unilaterally – the President is constitutionally empowered to threaten the use of force, implicitly or explicitly, through diplomatic means or shows of force. It is never seriously contested whether the President may declare that United States is contemplating military options in response to a crisis, or whether the President may move substantial U.S. military forces to a crisis region or engage in military exercises there. To take the Libya example just mentioned, is there any constitutional limitation on the President’s authority to move U.S. military forces to the Mediterranean region and prepare them very visibly to strike?44 Or his authority to issue an ultimatum to Libyan leaders that they cease their brutal conduct or else face military action? Would it matter whether such threats were explicit versus implicit, whether they were open and public versus secret, or whether they were just a bluff? If not a constitutional obstacle, could it be argued that the War Powers Resolution’s reporting requirements and limits on operations were triggered by a President’s mere ultimatum or threatening military demonstration, insofar as those moves might constitute a “situation where imminent involvement in hostilities is clearly indicated by the circumstances”? These questions simply are not asked (at least not anymore).45 If anything, most lawyers would probably conclude that the President’s constitutional powers to threaten war are not just expansive but largely beyond Congress’s authority to regulate directly. From a constitutional standpoint, to the extent it is considered at all, the President’s power to threaten force is probably regarded to be at least as broad as his power to use it. One way to look at it is that the power to threaten force is a lesser included element of presidential war powers; the power to threaten to use force is simply a secondary question, the answer to which is bounded by the primary issue of the scope of presidential power to actually use it. If one interprets the President’s defensive war powers very broadly, to include dealing with aggression not only directed against U.S. territories but also against third parties,46 then it might seem easy to conclude that the President can also therefore take steps that stop short of actual armed intervention to deter or prevent such aggression. If, however, one interprets the President’s powers narrowly, for example, to include only limited unilateral authority to repel attacks against U.S. territory,47 then one might expect objections to arguably excessive presidential power to include his unilateral threats of armed intervention. Another way of looking at it is that in many cases, threats of war or force might fall within even quite narrow interpretations of the President’s inherent foreign relations powers to conduct diplomacy or his express commander in chief power to control U.S. military forces – or some combination of the two – depending on how a particular threat is communicated. A President’s verbal warning, ultimatum, or declared intention to use military force, for instance, could be seen as merely exercising his role as the “sole organ” of U.S. foreign diplomacy, conveying externally information about U.S. capabilities and intentions.48 A president’s movement of U.S. troops or warships to a crisis region or elevation of their alert level could be seen as merely exercising his dayto- day tactical control over forces under his command.49 Generally it is not seriously contested whether the exercise of these powers alone could so affect the likelihood of hostilities or war as to intrude on Congress’s powers over war and peace.50 We know from historical examples that such unilateral military moves, even those that are ostensibly pure defensive ones, can provoke wars – take, for example, President Polk’s movement of U.S. forces to the contested border with Mexico in 1846, and the resulting skirmishes that led Congress to declare war.51 Coming at the issue from Congress’s Article I powers rather than the President’s Article II powers, the very phrasing of the power “To declare War” puts most naturally all the emphasis on the present tense of U.S. military action, rather than its potentiality. Even as congressionalists advance interpretations of the clause to include not merely declarative authority but primary decision-making authority as to whether or not to wage war or use force abroad, their modern-day interpretations do not include a power to threaten war (except perhaps through the specific act of declaring it). None seriously argues – at least not any more – that the Declare War Clause precludes presidential threats of war. This was not always the case. During the early period of the Republic, there was a powerful view that beyond outright initiation of armed hostilities or declaration of war, more broadly the President also could not unilaterally take actions (putting aside actual military attacks) that would likely or directly risk war,52 provoke a war with another state,53 or change the condition of affairs or relations with another state along the continuum from peace to war.54 To do so, it was often argued, would usurp Congress’s prerogative to control the nation’s state of peace or war.55 During the Quasi-War with France at the end of the 18th century, for example, some members of Congress questioned whether the President, absent congressional authorization, could take actions that visibly signaled an intention to retaliate against French maritime harassment,56 and even some members of President Adams’ cabinet shared doubts.57 Some questions over the President’s power to threaten force arose (eventually) in relation to the Monroe Doctrine, announced in an 1823 presidential address to Congress and which in effect declared to European powers that the United States would oppose any efforts to colonize or reassert control in the Western Hemisphere.58 “Virtually no one questioned [Monroe’s proclamation] at the time. Yet it posed a constitutional difficulty of the first importance.”59 Of course, Monroe did not actually initiate any military hostilities, but his implied threat – without congressional action – risked provoking rather than deterring European aggression and by putting U.S. prestige and credibility on the line it limited Congress’s practical freedom of action if European powers chose to intervene.60 The United States would have had at the time to rely on British naval power to make good on that tacit threat, though a more assertive role for the President in wielding the potential for war or intervention during this period went hand in hand with a more sustained projection of U.S. power beyond its borders, especially in dealing with dangers emanating from Spanish-held Florida territory.61 Monroe’s successor, John Quincy Adams, faced complaints from opposition members of Congress that Monroe’s proclamation had exceeded his constitutional authority and had usurped Congress’s by committing the United States – even in a non-binding way – to resisting European meddling in the hemisphere.62 The question whether the President could unilaterally send militarily-threatening signals was in some respects a mirror image of the issues raised soon after the Constitution was ratified during the 1793 Neutrality Controversy: could President Washington unilaterally declare the United States to be neutral as to the war among European powers. Washington’s politically controversial proclamation declaring the nation “friendly and impartial” in the conflict between France and Great Britain (along with other European states) famously prompted a back-and-forth contest of public letters by Alexander Hamilton and James Madison, writing pseudonymously as “Pacificus” and “Helvidius”, about whether the President had such unilateral power or whether it belonged to Congress.63 Legal historian David Currie points out the irony that the neutrality proclamation was met with stronger and more immediate constitutional scrutiny and criticism than was Monroe’s threat. After all, Washington’s action accorded with the principle that only Congress, representing popular will, should be able to take the country from the baseline state of peace to war, whereas Monroe’s action seemed (at least superficially) to commit it to a war that Congress had not approved.64 Curiously (though for reasons offered below, perhaps not surprisingly) this issue – whether there are constitutional limits on the President’s power to threaten war – has almost vanished completely from legal discussion, and that evaporation occurred even before the dramatic post-war expansion in asserted presidential power to make war. Just prior to World War II, political scientist and presidential powers theorist Edward Corwin remarked that “[o]f course, it may be argued, and has in fact been argued many times, that the President is under constitutional obligation not to incur the risk of war in the prosecution of a diplomatic policy without first consulting Congress and getting its consent.”65 “Nevertheless,” he continued,66 “the supposed principle is clearly a maxim of policy rather than a generalization from consistent practice.” In his 1945 study World Policing and the Constitution, James Grafton Rogers noted: [E]xamples of demonstrations on land and sea made for a variety of purposes and under Presidents of varied temper and in different political climates will suffice to make the point. The Commander-in-Chief under the Constitution can display our military resources and threaten their use whenever he thinks best. The weakness in the diplomatic weapon is the possibility of dissidence at home which may cast doubt on our serious intent. The danger of the weapon is war.67 At least since then, however, the importance to U.S. foreign policy of threatened force has increased dramatically, while legal questions about it have receded further from discussion. In recent decades a few prominent legal scholars have addressed the President’s power to threaten force, though in only brief terms.

[CONTINUED]

**Exec Power DA – 1NC [3/5]**

[CONTINUED]

Taylor Reveley noted in his volume on war powers the importance of allocating constitutional responsibility not only for the actual use of force but also “[v]erbal or written threats or assurances about the circumstances in which the United States will take military action …, whether delivered by declarations of American policy, through formal agreements with foreign entities, by the demeanor or words of American officials, or by some other sign of national intent.”68 Beyond recognizing the critical importance of threats and other non-military actions in affecting war and peace, however, Reveley made little effort to address the issue in any detail. Among the few legal scholars attempting to define the limiting doctrinal contours of presidentially threatened force, Louis Henkin wrote in his monumental Foreign Affairs and the Constitution that: Unfortunately, the line between war and lesser uses of force is often elusive, sometimes illusory, and the use of force for foreign policy purposes can almost imperceptibly become a national commitment to war. Even when he does not use military force, the President can incite other nations or otherwise plunge or stumble this country into war, or force the hand of Congress to declare or to acquiesce and cooperate in war. As a matter of constitutional doctrine, however, one can declare with confidence that a President begins to exceed his authority if he willfully or recklessly moves the nation towards war…69 The implication seems to be that the President may not unilaterally threaten force in ways that are dramatically escalatory and could likely lead to war, or perhaps that the President may not unilaterally threaten the use of force that he does not have the authority to initiate unilaterally.70 Jefferson Powell, who generally takes a more expansive view than Henkin of the President’s war powers, argues by contrast that “[t]he ability to warn of, or threaten, the use of military force is an ordinary and essential element in the toolbox of that branch of government empowered to formulate and implement foreign policy.”71 For Powell, the President is constantly taking actions as part of everyday international relations that carry a risk of military escalation, and these are well-accepted as part of the President’s broader authority to manage, if not set, foreign policy. Such brief mentions are in recent times among the rare exceptions to otherwise barren constitutional discussion of presidential powers to threaten force. That the President’s authority to threaten force is so well-accepted these days as to seem self-evident is not just an academic phenomenon. It is also reflected in the legal debates among and inside all three branches of government. In 1989, Michael Reisman observed: Military maneuvers designed to convey commitment to allies or contingent threats to adversaries … are matters of presidential competence. Congress does not appear to view as within its bailiwick many low-profile contemporaneous expressions of gunboat diplomacy, i.e., the physical interposition of some U.S. war-making capacity as communication to an adversary of United States’ intentions and capacities to oppose it.72 This was and remains a correct description but understates the pattern of practice, insofar as even major and high-profile expressions of coercive diplomacy are regarded among all three branches of government as within presidential competence. In Dellums v. Bush – perhaps the most assertive judicial scrutiny of presidential power to use large-scale force abroad since the end of the Cold War – the district court dismissed on ripeness grounds congressmembers’ suit challenging President George H. W. Bush’s intended military operations against Iraq in 1991 and seeking to prevent him from initiating an offensive attack against Iraq without first securing explicit congressional authorization for such action.73 That at the time of the suit the President had openly threatened war – through ultimatums and deployment of several hundred thousand U.S. troops – but had not yet “committed to a definitive course of action” to carry out the threat meant there was no justiciable legal issue, held the court.74 The President’s threat of war did not seem to give the district court legal pause at all; quite the contrary, the mere threat of war was treated by the court as a non-issue entirely.75 There are several reasons why constitutional questions about threatened force have dropped out of legal discussions. First, the more politically salient debate about the President’s unilateral power to use force has probably swallowed up this seemingly secondary issue. As explained below, it is a mistake to view threats as secondary in importance to uses of force, but they do not command the same political attention and their impacts are harder to measure.76 Second, the expansion of American power after World War II, combined with the growth of peacetime military forces and a set of defense alliance commitments (developments that are elaborated below) make at least some threat of force much more common – in the case of defensive alliances and some deterrent policies, virtually constant – and difficult to distinguish from other forms of everyday diplomacy and security policy.77 Besides, for political and diplomatic reasons, presidents rarely threaten war or intervention without at least a little deliberate ambiguity. As historian Marc Trachtenberg puts it: “It often makes sense … to muddy the waters a bit and avoid direct threats.”78 Any legal lines one might try to draw (recall early attempts to restrict the President’s unilateral authority to alter the state of affairs along the peacetime-wartime continuum) have become blurrier and blurrier. In sum, if the constitutional power to threaten war ever posed a serious legal controversy, it does so no more. As the following section explains, however, threats of war and armed force have during most of our history become a greater and greater part of American grand strategy, defined here as long-term policies for using the country’s military and non-military power to achieve national goals. The prominent role of threatened force in U.S. strategy has become the focus of political scientists and other students of security strategy, crises, and responses – but constitutional study has not adjusted accordingly.79 C. Threats of Force and U.S. Grand Strategy While the Korean and Vietnam Wars were generating intense study among lawyers and legal scholars about constitutional authority to wage military actions abroad, during that same period many political scientists and strategists – economists, historians, statesmen, and others who studied international conflict – turned their focus to the role of threatened force as an instrument of foreign policy. The United States was building and sustaining a massive war-fighting apparatus, but its security policy was not oriented primarily around waging or winning wars but around deterring them and using the threat of war – including demonstrative military actions – to advance U.S. security interests. It was the potential of U.S. military might, not its direct application or engagement with the enemy, that would do much of the heavy lifting. U.S. military power would be used to deter the Soviet Union and other hostile states from taking aggressive action. It would be unsheathed to prompt them to back down over disputes. It would reassure allies that they could depend on U.S. help in defending themselves. All this required that U.S. willingness to go to war be credible in the eyes of adversaries and allies alike. Much of the early Cold War study of threatened force concerned nuclear strategy, and especially deterrence or escalation of nuclear war. Works by Albert Wohlstetter, Herman Kahn, and others not only studied but shaped the strategy of nuclear threats, as well as how to use limited applications of force or threats of force to pursue strategic interests in remote parts of the globe without sparking massive conflagrations.80 As the strategic analyst Bernard Brodie wrote in 1946, “Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them.”81 Toward that end, U.S. government security and defense planners during this time focused heavily on preserving and improving the credibility of U.S. military threats – while the Soviet Union was doing likewise.82 The Truman administration developed a militarized version of containment strategy against the Soviet empire, emphasizing that stronger military capabilities were necessary to prevent the Soviets from seizing the initiative and to resist its aggressive probes: “it is clear,” according to NSC-68, the government document which encapsulated that strategy, “that a substantial and rapid building up of strength in the free world is necessary to support a firm policy intended to check and to roll back the Kremlin's drive for world domination.”83 The Eisenhower administration’s “New Look” policy and doctrine of “massive retaliation” emphasized making Western collective security both more effective and less costly by placing greater reliance on deterrent threats – including threatened escalation to general or nuclear war. As his Secretary of State John Foster Dulles explained, “[t]here is no local defense which alone will contain the mighty landpower of the Communist world. Local defenses must be reinforced by the further deterrent of massive retaliatory power.”84 As described in Evan Thomas’s recent book, Ike’s Bluff, Eisenhower managed to convince Soviet leaders that he was ready to use nuclear weapons to check their advance in Europe and elsewhere. In part due to concerns that threats of massive retaliation might be insufficiently credible in Soviet eyes (especially with respect to U.S. interests perceived as peripheral), the Kennedy administration in 1961 shifted toward a strategy of “flexible response,” which relied on the development of a wider spectrum of military options that could quickly and efficiently deliver varying degrees of force in response to foreign aggression.85 Throughout these periods, the President often resorted to discrete, limited uses of force to demonstrate U.S. willingness to escalate. For example, in 1961 the Kennedy administration (mostly successfully in the short-run) deployed intervention-ready military force immediately off the coast of the Dominican Republic to compel its government's ouster,86 and that same year it used military exercises and shows of force in ending the Berlin crisis;87 in 1964, the Johnson administration unsuccessfully used air strikes on North Vietnamese targets following the Tonkin Gulf incidents, failing to deter what it viewed as further North Vietnamese aggression.88 The point here is not the shifting details of U.S. strategy after World War II – during this era of dramatic expansion in asserted presidential war powers – but the central role of credible threats of war in it, as well as the interrelationship of plans for using force and credible threats to do so. Also during this period, the United States abandoned its long-standing aversion to “entangling alliances,”89 and committed to a network of mutual defense treaties with dependent allies. Besides the global collective security arrangement enshrined in the UN Charter, the United States committed soon after World War II to mutual defense pacts with, for example, groups of states in Western Europe (the North Atlantic Treaty Organization)90 and Asia (the Southeast Asia Treaty Organization,91 as well as a bilateral defense agreement with the Republic of Korea,92 Japan,93 and the Republic of China,94 among others). These alliance commitments were part of a U.S. effort to “extend” deterrence of Communist bloc aggression far beyond its own borders.95 “Extended deterrence” was also critical to reassuring these U.S. allies that their security needs would be met, in some instances to head off their own dangerous rearmament.96 Among the leading academic works on strategy of the 1960s and 70s were those of Thomas Schelling, who developed the theoretical structure of coercion theory, arguing that rational states routinely use the threat of military force – the manipulation of an adversary’s perceptions of future risks and costs with military threats – as a significant component of their diplomacy.97 Schelling distinguished between deterrence (the use of threats to dissuade an adversary from taking undesired action) and compellence (the use of threats to persuade an adversary to behave a certain way), and he distinguished both forms of coercion from brute force: “[B]rute force succeeds when it is used, whereas the power to hurt is most successful when held in reserve. It is the threat of damage to come that can make someone yield of comply. It is latent violence that can influence someone’s choice.”98 Alexander George, David Hall, and William Simons then led the way in taking a more empirical approach, reviewing case studies to draw insights about the success and failure of U.S. coercive threats, analyzing contextual variables and their effects on parties’ reactions to threats during crises. Among their goals was to generate lessons informed by history for successful strategies that combine diplomatic efforts with threats or demonstrations of force, recognizing that the United States was relying heavily on threatened force in addressing security crises. Coercive diplomacy – if successful – offered ways to do so with minimal actual application of military force.99 One of the most influential studies that followed was Force Without War: U.S. Armed Forces as a Political Instrument, a Brookings Institution study led by Barry Blechman and Stephen Kaplan and published in 1977.100 They studied “political uses of force”, defined as actions by U.S. military forces “as part of a deliberate attempt by the national authorities to influence, or to be prepared to influence, specific behavior of individuals in another nation without engaging in a continued contest of violence.”101 Blechman and Kaplan’s work, including their large data set and collected case studies, was important for showing the many ways that threatened force could support U.S. security policy. Besides deterrence and compellence, threats of force were used to assure allies (thereby, for example, avoiding their own drive toward militarization of policies or crises) and to induce third parties to behave certain ways (such as contributing to diplomatic resolution of crises). The record of success in relying on threatened force has been quite mixed, they showed. Blechman and Kaplan’s work, and that of others who built upon it through the end of the Cold War and the period that has followed,102 helped understand the factors that correlated with successful threats or demonstrations of force without resort or escalation to war, especially the importance of credible signals.103 After the Cold War, the United States continued to rely on coercive force – threatened force to deter or compel behavior by other actors – as a central pillar of its grand strategy. During the 1990s, the United States wielded coercive power with varied results against rogue actors in many cases that, without the overlay of superpower enmities, were considered secondary or peripheral, not vital, interests: Iraq, Somalia, Haiti, Bosnia, and elsewhere. For analysts of U.S. national security policy, a major puzzle was reconciling the fact that the United States possessed overwhelming military superiority in raw terms over any rivals with its difficult time during this era in compelling changes in their behavior.104 As Daniel Byman and I wrote about that decade in our study of threats of force and American foreign policy: U.S. conventional and nuclear forces dwarf those of any adversaries, and the U.S. economy remains the largest and most robust in the world. Because of these overwhelming advantages, the United States can threaten any conceivable adversary with little danger of a major defeat or even significant retaliation. Yet coercion remains difficult. Despite the United States’ lopsided edge in raw strength, regional foes persist in defying the threats and ultimatums brought by the United States and its allies. In confrontations with Somali militants, Serb nationalists, and an Iraqi dictator, the U.S. and allied record or coercion has been mixed over recent years…. Despite its mixed record of success, however, coercion will remain a critical element of U.S. foreign policy.105 One important factor that seemed to undermine the effectiveness of U.S. coercive threats during this period was that many adversaries perceived the United States as still afflicted with “Vietnam Syndrome,” unwilling to make good on its military threats and see military operations through.106 Since the turn of the 21st Century, major U.S. security challenges have included non-state terrorist threats, the proliferation of nuclear and other weapons of mass destruction (WMD), and rapidly changing power balances in East Asia, and the United States has accordingly been reorienting but retaining its strategic reliance on threatened force. The Bush Administration’s “preemption doctrine” was premised on the idea that some dangerous actors – including terrorist organizations and some states seeking WMD arsenals – are undeterrable, so the United States might have to strike them first rather than waiting to be struck.107 On one hand, this was a move away from reliance on threatened force: “[t]he inability to deter a potential attacker, the immediacy of today’s threats, and the magnitude of potential harm that could be caused by our adversaries’ choice of weapons, do not permit” a reactive posture.108 Yet the very enunciation of such a policy – that “[t]o forestall or prevent such hostile acts by our adversaries, the United States will, if necessary, act preemptively”109 – was intended to persuade those adversaries to alter their policies that the United States regarded as destabilizing and threatening. Although the Obama administration pulled back from this rhetoric and placed greater emphasis on international institutions, it has continued to rely on threatened force as a key pillar of its strategy with regard to deterring threats (such as aggressive Iranian moves), intervening in humanitarian crises (as in Libya), and reassuring allies.110 With regard to East Asia, for example, the credible threat of U.S. military force is a significant element of U.S. strategy for deterring Chinese and North Korean aggression as well as reassuring other Asian powers of U.S. protection, to avert a destabilizing arms race.111 D. The Disconnect Between Constitutional Discourse and Strategy There is a major disconnect between the decades of work by strategists and many political scientists on American security policy and practice since the Second World War and legal analysis and scholarship of constitutional war powers during that period. Lawyers and strategists have been relying on not only distinct languages but distinct logics of military force – in short, when it comes to using U.S. military power, lawyers think in terms of “going to war” while strategists focus on potential war and processes leading to it. These framings manifest in differing theoretical starting points for considering how exercises of U.S. military might affect war and peace, and they skew the empirical insights and normative prescriptions about Presidential power often drawn from their analyses. 1. Lawyers’ Misframing Lawyers’ focus on actual uses of force – especially engagements with enemy military forces – as constitutionally salient, rather than including threats of force in their understanding of modern presidential powers tilts analysis toward a one-dimensional strategic logic, rather than a more complex and multi-dimensional and dynamic logic in which the credible will to use force is as important as the capacity to do so. As discussed above, early American constitutional thinkers and practitioners generally wanted to slow down with institutional checks decisions to go to war, because they thought that would make war less likely. “To invoke a more contemporary image,” wrote John Hart Ely of their vision, “it takes more than one key to launch a missile: It should take quite a number to start a war.”112 They also viewed the exercise of military power as generally a ratchet of hostilities, whereby as the intensity of authorized or deployed force increased, so generally did the state of hostilities between the United States and other parties move along a continuum from peace to war.113 Echoes of this logic still reverberate in modern congressionalist legal scholarship: the more flexibly the President can use military force, the more likely it is that the United States will find itself in wars; better, therefore, to clog decisions to make war with legislative checks.114 Modern presidentialist legal scholars usually respond that rapid action is a virtue, not a vice, in exercising military force.115 Especially as a superpower with global interests and facing global threats, presidential discretion to take rapid military action – endowed with what Alexander Hamilton called “[d]ecision, activity, secrecy, and dispatch”116 – best protects American interests. In either case the emphasis tends overwhelmingly to be placed on actual military engagements with adversaries. Strategists and many political scientists, by contrast, view some of the most significant use of military power as starting well before armed forces clash – and including important cases in which they never actually do. Coercive diplomacy and strategies of threatened force, they recognize, often involve a set of moves and countermoves by opposing sides and third parties before or even without the violent engagement of opposing forces. It is often the parties’ perceptions of anticipated actions and costs, not the actual carrying through of violence, that have the greatest impact on the course of events and resolution or escalation of crises. Instead of a ratchet of escalating hostilities, the flexing of military muscle can increase as well as decrease actual hostilities, inflame as well as stabilize relations with rivals or enemies. Moreover, those effects are determined not just by U.S. moves but by the responses of other parties to them – or even to anticipated U.S. moves and countermoves.117 Indeed, as Schelling observed, strategies of brinkmanship sometimes operate by “the deliberate creation of a recognizable risk of war, a risk that one does not completely control.”118 This insight – that effective strategies of threatened force involve not only great uncertainty about the adversary’s responses but also sometimes involve intentionally creating risk of inadvertent escalation119 – poses a difficult challenge for any effort to cabin legally the President’s power to threaten force in terms of likelihood of war or some due standard of care.120 2. Lawyers’ Selection Problems Methodologically, a lawyerly focus on actual uses of force – a list of which would then commonly be used to consider which ones were or were not authorized by Congress – vastly undercounts the instances in which presidents wield U.S. military might. It is already recognized by some legal scholars that studying actual uses of force risks ignoring instances in which President contemplated force but refrained from using it, whether because of political, congressional, or other constraints.121 The point here is a different one: that some of the most significant (and, in many instances, successful) presidential decisions to threaten force do not show up in legal studies of presidential war powers that consider actual deployment or engagement of U.S. military forces as the relevant data set. Moreover, some actual uses of force, whether authorized by Congress or not, were preceded by threats of force; in some cases these threats may have failed on their own to resolve the crisis, and in other cases they may have precipitated escalation. To the extent that lawyers are interested in understanding from historical practice what war powers the political branches thought they had and how well that understanding worked, they are excluding important cases. Consider, as an illustration of this difference in methodological starting point, that for the period of 1946-1975 (during which the exercise of unilateral Presidential war powers had its most rapid expansion), the Congressional Research Service compilation of instances in which the United States has utilized military forces abroad in situations of military conflict or potential conflict to protect U.S. citizens or promote U.S. interests – which is often relied upon by legal scholars studying war powers – lists only about two dozen incidents.122 For the same time period, the Blechman and Kaplan study of political uses of force (usually threats) – which is often relied upon by political scientists studying U.S. security strategy – includes dozens more data-point incidents, because they divide up many military crises into several discrete policy decisions, because many crises were resolved with threat-backed diplomacy, and because many uses of force were preceded by overt or implicit threats of force.123 Among the most significant incidents studied by Blechman and Kaplan but not included in the Congressional Research Service compilation at all are the 1958-59 and 1961 crises over Berlin and the 1973 Middle East War, during which U.S. Presidents signaled threats of superpower war, and in the latter case signaled particularly a willingness to resort to nuclear weapons.124 Because the presidents did not in the end carry out these threats, these cases lack the sort of authoritative legal justifications or reactions that accompany actual uses of force. It is therefore difficult to assess how the executive branch and congress understood the scope of the President’s war powers in these cases, but historical inquiry would probably show the executive branch’s interpretation to be very broad, even to include full-scale war and even where the main U.S. interest at stake was the very credibility of U.S. defense commitments undergirding its grand strategy, not simply the interests specific to divided Germany and the Middle East region.

[CONTINUED]

**Exec Power DA – 1NC [4/5]**

[CONTINUED]

Of course, one might argue that because the threatened military actions were never carried out in these cases, it is impossible to know if the President would have sought congressional authorization or how Congress would have reacted to the use of force; nonetheless, it is easy to see that in crises like these a threat by the President to use force, having put U.S. credibility on the line in addition to whatever other foreign policy stakes were at issues, would have put Congress in a bind. 3. Lawyers’ Mis-Assessment Empirically, analysis of and insights gleaned from any particular incident – which might then be used to evaluate the functional merits of presidential powers – looks very different if one focuses predominantly on the actual use of force instead of considering also the role of threatened force. Take for example, the Cuban Missile Crisis – perhaps the Cold War’s most dangerous event. To the rare extent that they consider domestic legal issues of this crisis at all, lawyers interested in the constitutionality of President Kennedy’s actions generally ask only whether he was empowered to initiate the naval quarantine of Cuba, because that is the concrete military action Kennedy took that was readily observable and that resulted in actual engagement with Soviet forces or vessels – as it happens, very minimal engagement.125 To strategists who study the crisis, however, the naval quarantine is not in itself the key presidential action; after all, as Kennedy and his advisers realized, a quarantine alone could not remove the missiles that were already in Cuba. The most consequential presidential actions were threats of military or even nuclear escalation, signaled through various means including putting U.S. strategic bombers on highest alert.126 The quarantine itself was significant not for its direct military effects but because of its communicative impact in showing U.S. resolve. If one is focused, as lawyers often are, on presidential military action that actually engaged the enemy in combat or nearly did, it is easy to dismiss this case as not very constitutionally significant. If one focuses on it, as strategists and political scientists often do, on nuclear brinkmanship, it is arguably the most significant historical exercise of unilateral presidential powers to affect war and peace.127 Considering again the 1991 Gulf War, most legal scholars would dismiss this instance as constitutionally a pretty uninteresting military conflict: the President claimed unilateral authority to use force, but he eventually sought and obtained congressional authorization for what was ultimately – at least in the short-run – a quite successful war. For the most part this case is therefore neither celebrated nor decried much by either side of legal war powers debates,128 though some congressionalist scholars highlight the correlation of congressional authorization for this war and a successful outcome.129 Political scientists look at the case differently, though. They often study this event not as a successful war but as failed coercive diplomacy, in that the United States first threatened war through a set of dramatically escalating steps that ultimately failed to persuade Saddam Hussein to withdraw from Kuwait.130 Some political scientists even see U.S. legal debate about military actions as an important part of this story, assessing that adversaries pay attention to congressional arguments and moves in evaluating U.S. resolve (an issue taken up in greater detail below) and that congressional opposition to Bush’s initial unilateralism in this case undermined the credibility of U.S. threats.131 Whether one sees the Gulf War as a case of (successful) war, as lawyers usually do, or (unsuccessful) threatened war, as political scientists usually do, colors how one evaluates the outcome and the credit one might attach to some factors such as vocal congressional opposition to initially-unilateral presidential moves. Notice also that legal analysis of Presidential authority to use force is sometimes thought to turn partly on the U.S. security interests at stake, as though those interests are purely contextual and exogenous to U.S. decision-making and grand strategy. In justifying President Obama’s 2011 use of force against the Libyan government, for example, the Justice Department’s Office of Legal Counsel concluded that the President had such legal authority “because he could reasonably determine that such use of force was in the national interest,” and it then went on to detail the U.S. security and foreign policy interests.132 The interests at stake in crises like these, however, are altered dramatically if the President threatens force: doing so puts the credibility of U.S. threats at stake, which is important not only with respect to resolving the crisis at hand but with respect to other potential adversaries watching U.S. actions.133 The President’s power to threaten force means that he may unilaterally alter the costs and benefits of actually using force through his prior actions.134 The U.S. security interests in carrying through on threats are partly endogenous to the strategy embarked upon to address crises (consider, for example, that once President George H.W. Bush placed hundred of thousands of U.S. troops in the Persian Gulf region and issued an ultimatum to Saddam Hussein in 1990, the credibility of U.S. threats and assurances to regional allies were put on the line).135 Moreover, interests at stake in any one crisis cannot simply be disaggregated from broader U.S. grand strategy: if the United States generally relies heavily on threats of force to shape the behavior of other actors, then its demonstrated willingness or unwillingness to carry out a threat and the outcomes of that action affect its credibility in the eyes of other adversaries and allies, too.136 It is remarkable, though in the end not surprising, that the executive branch does not generally cite these credibility interests in justifying its unilateral uses of force. It does cite when relevant the U.S. interest in sustaining the credibility of its formal alliance commitments or U.N. Security Council resolutions, as reasons supporting the President’s constitutional authority to use force.137 The executive branch generally refrains from citing the similar interests in sustaining the credibility of the President’s own threats of force, however, probably in part because doing so would so nakedly expose the degree to which the President’s prior unilateral strategic decisions would tie Congress’s hands on the matter. \* \* \* In sum, lawyers’ focus on actual uses of force – usually in terms of armed clashes with an enemy or the placement of troops into hostile environments – does not account for much vaster ways that President’s wield U.S. military power and it skews the claims legal scholars make about the allocation of war powers between the political branches. A more complete account of constitutional war powers should recognize the significant role of threatened force in American foreign policy. II. Democratic Checks on Threatened Force The previous Parts of this Article showed that, especially since the end of World War II, the United States has relied heavily on strategies of threatened force in wielding its military might – for which credible signals are a necessary element – and that the President is not very constrained legally in any formal sense in threatening war. Drawing on recent political science scholarship, this Part takes some of the major questions often asked by students of constitutional war powers with respect to the actual use of force and reframes them in terms of threatened force. First, as a descriptive matter, in the absence of formal legal checks on the President’s power to threaten war, is the President nevertheless informally but significantly constrained by democratic institutions and processes, and what role does Congress play in that constraint? Second, as a normative matter, what are the strategic merits and drawbacks of this arrangement of democratic institutions and constraints with regard to strategies of threatened force? Third, as a prescriptive matter, although it is not really plausible that Congress or courts would ever erect direct legal barriers to the President’s power to threaten war, how might legal reform proposals to more strongly and formally constrain the President’s power to use force indirectly impact his power to threaten it effectively? For reasons discussed below, I do not consider whether Congress could legislatively restrict directly the President’s power to threaten force or war; in short, I set that issue aside because assuming that were constitutionally permissible, even ardent congressionalists have exhibited no interest in doing so, and instead have focused on legally controlling the actual use of force. Political science insights that bear on these questions emerge from several directions. One is from studies of Congress’ influence on use of force decisions, which usually assume that Congress’s formal legislative powers play only a limited role in this area, and the effects of this influence on presidential decision-making about threatened force. Another is international relations literature on international bargaining138 as well as literature on the theory of democratic peace, the notion that democracies rarely, if ever, go to war with one another.139 In attempting to explain the near-absence of military conflicts between democracies, political scientists have examined how particular features of democratic governments – electoral accountability, the institutionalized mobilization of political opponents, and the diffusion of decision-making authority regarding the use of force among executive and legislative branches – affect decision-making about war.140 These and other studies, in turn, have led some political scientists (especially those with a rational choice theory orientation) to focus on how those features affect the credibility of signals about force that governments send to adversaries in crises.141 My purpose in addressing these questions is to begin painting a more complete and detailed picture of the way war powers operate, or could operate, than one sees when looking only at actual wars and use of force. This is not intended to be a comprehensive account but an effort to synthesize some strands of scholarship from other fields regarding threatened force to inform legal discourse about how war powers function in practice and the strategic implications of reform. The answers to these questions also bear on raging debates among legal scholars on the nature of American executive power and its constraint by law. Initially they seem to support the views of those legal scholars who have long believed that in practice law no longer seriously binds the President with respect to war-making.142 That view has been taken even further recently by Eric Posner and Adrian Vermeule, who argue that “[l]aw does little constraint the modern executive” at all, but also observe that “politics and public opinion” operate effectively to cabin executive powers.143 The arguments offered here, however, do more to support the position of those legal scholars who describe a more complex relationship between law and politics, including that law is constitutive of the processes of political struggle.144 That law helps constitute the processes of political struggles is true of any area of public policy, though, and what is special here is the added importance of foreign audiences – including adversaries and allies, alike – observing and reacting to those politics, too. Democratic Constraints on the Power to the Threaten Force Whereas most lawyers usually begin their analysis of the President’s and Congress’s war powers by focusing on their formal legal authorities, political scientists usually take for granted these days that the President is – in practice – the dominant branch with respect to military crises and that Congress wields its formal legislative powers in this area rarely or in only very limited ways. A major school of thought, however, is that congressional members nevertheless wield significant influence over decisions about force, and that this influence extends to threatened force, so that Presidents generally refrain from threats that would provoke strong congressional opposition. Even without any serious prospect for legislatively blocking the President’s threatened actions, Congress under certain conditions can loom large enough to force Presidents to adjust their policies; even when it cannot, congressional members can oblige the President expend lots of political capital. As Jon Pevehouse and William Howell explain: When members of Congress vocally oppose a use of force, they undermine the president’s ability to convince foreign states that he will see a fight through to the end. Sensing hesitation on the part of the United States, allies may be reluctant to contribute to a military campaign, and adversaries are likely to fight harder and longer when conflict erupts— thereby raising the costs of the military campaign, decreasing the president’s ability to negotiate a satisfactory resolution, and increasing the probability that American lives are lost along the way. Facing a limited band of allies willing to participate in a military venture and an enemy emboldened by domestic critics, presidents may choose to curtail, and even abandon, those military operations that do not involve vital strategic interests. 145 This statement also highlights the important point, alluded to earlier, that force and threatened force are not neatly separable categories. Often limited uses of force are intended as signals of resolve to escalate, and most conflicts involve bargaining in which the threat of future violence – rather than what Schelling calls “brute force”146 – is used to try to extract concessions. The formal participation of political opponents in legislative bodies provides them with a forum for registering dissent to presidential policies of force through such mechanisms floor statements, committee oversight hearings, resolution votes, and funding decisions.147 These official actions prevent the President “from monopolizing the nation’s political discourse” on decisions regarding military actions can thereby make it difficult for the President to depart too far from congressional preferences.148 Members of the political opposition in Congress also have access to resources for gathering policy relevant information from the government that informs their policy preferences. Their active participation in specialized legislative committees similarly gives opponent party members access to fact-finding resources and forums for registering informed dissent from decisions within the committee’s purview.149 As a result, legislative institutions within democracies can enable political opponents to have a more immediate and informed impact on executive’s decisions regarding force than can opponents among the general public. Moreover, studies suggest that Congress can actively shape media coverage and public support for a president’s foreign policy engagements.150 In short, these findings among political scientists suggest that, even without having to pass legislation or formally approve of actions, Congress often operates as an important check on threatened force by providing the president’s political opponents with a forum for registering dissent from the executive’s decisions regarding force in ways that attach domestic political costs to contemplated military actions or even the threats to use force. Under this logic, Presidents, anticipating dissent, will be more selective in issuing¶ threats in the first place, making only those commitments that would not incite¶ widespread political opposition should the threat be carried through.151 Political¶ opponents within a legislature also have few electoral incentives to collude in an¶ executive’s bluff, and they are capable of expressing opposition to a threatened use of¶ force in ways that could expose the bluff to a threatened adversary.152 This again narrows¶ the President’s range of viable policy options for brandishing military force. Counter-intuitively, given the President’s seemingly unlimited and unchallenged¶ constitutional power to threaten war, it may in some cases be easier for members of¶ Congress to influence presidential decisions to threaten military action than presidential¶ war decisions once U.S. forces are already engaged in hostilities. It is widely believed¶ that once U.S. armed forces are fighting, congress members’ hands are often tied: policy¶ opposition at that stage risks being portrayed as undermining our troops in the field.153¶ Perhaps, it could be argued, the President takes this phenomenon into account and¶ therefore discounts political opposition to threatened force; he can assume that such¶ opposition will dissipate if he carries it through. Even if that is true, before that point¶ occurs, however, members of Congress may have communicated messages domestically¶ and communicated signals abroad that the President will find difficult to counter.154 The bottom line is that a body of recent political science, while confirming the¶ President’s dominant position in setting policy in this area, also reveals that policymaking¶ with respect to threats of force is significantly shaped by domestic politics and¶ that Congress is institutionally positioned to play a powerful role in influencing those¶ politics, even without exercising its formal legislative powers. Given the centrality of¶ threatened force to U.S. foreign policy strategy and security crises, this suggests that the¶ practical war powers situation is not so imbalanced toward the President as many assume. B. Democratic Institutions and the Credibility of Threats A central question among constitutional war powers scholars is whether robust¶ checks – especially congressional ones – on presidential use of force lead to “sound”¶ policy decision-making. Congressionalists typically argue that legislative control over¶ war decisions promotes more thorough deliberation, including more accurate weighing of¶ consequences and gauging of political support of military action.155 Presidentialists¶ usually counter that the executive branch has better information and therefore better¶ ability to discern the dangers of action or inaction, and that quick and decisive military¶ moves are often required to deal with security crises.156 If we are interested in these sorts of functional arguments, then reframing the¶ inquiry to include threatened force prompts critical questions whether such checks also¶ contribute to or detract from effective deterrence and coercive diplomacy and therefore¶ positively or negatively affect the likelihood of achieving aims without resort to war.¶ Here, recent political science provides some reason for optimism, though the scholarship¶ in this area is neither yet well developed nor conclusive. To be sure, “soundness” of policy with respect to force is heavily laden with¶ normative assumptions about war and the appropriate role for the United States in the¶ broader international security system, so it is difficult to assess the merits and¶ disadvantages of constitutional allocations in the abstract. That said, whatever their¶ specific assumptions about appropriate uses of force in mind, constitutional war powers¶ scholars usually evaluate the policy advantages and dangers of decision-making¶ allocations narrowly in terms of the costs and outcomes of actual military engagements¶ with adversaries. The importance of credibility to strategies of threatened force adds important new¶ dimensions to this debate. On the one hand, one might intuitively expect that robust democratic checks would generally be ill-suited for coercive threats and negotiations –¶ that institutional centralization and secrecy of decision-making might better equip nondemocracies¶ to wield threats of force. As Quincy Wright speculated in 1944, autocracies¶ “can use war efficiently and threats of war even more efficiently” than democracies,157¶ especially the American democracy in which vocal public and congressional opposition¶ may undermine threats.158 Moreover, proponents of democratic checks on war powers¶ usually assume that careful deliberation is a virtue in preventing unnecessary wars, but¶ strategists of deterrence and coercion observe that perceived irrationality is sometimes¶ important in conveying threats: “don’t test me, because I might just be crazy enough to¶ do it!”159 On the other hand, some political scientists have recently called into question this¶ view and concluded that the institutionalization of political contestation and some¶ diffusion of decision-making power in democracies of the kind described in the previous¶ section make threats to use force rare but especially credible and effective in resolving¶ international crises without actual resort to armed conflict. In other words, recent¶ arguments in effect turn some old claims about the strategic disabilities of democracies¶ on their heads: whereas it used to be generally thought that democracies were ineffective¶ in wielding threats because they are poor at keeping secrets and their decision-making is¶ constrained by internal political pressures, a current wave of political science accepts this¶ basic description but argues that these democratic features are really strategic virtues.160 Rationalist models of crisis bargaining between states assume that because war is¶ risky and costly, states will be better off if they can resolve their disputes through¶ bargaining rather than by enduring the costs and uncertainties of armed conflict.161¶ Effective bargaining during such disputes – that which resolves the crisis without a resort¶ to force – depends largely on states’ perceptions of their adversary’s capacity to wage an¶ effective military campaign and its willingness to resort to force to obtain a favorable¶ outcome. A state targeted with a threat of force, for example, will be less willing to resist¶ the adversary’s demands if it believes that the adversary intends to wage and is capable of¶ waging an effective military campaign to achieve its ends. In other words, if a state¶ perceives that the threat from the adversary is credible, that state has less incentive to¶ resist such demands if doing so will escalate into armed conflict. The accuracy of such perceptions, however, is often compromised by¶ informational asymmetries that arise from private information about an adversary’s¶ relative military capabilities and resolve that prevents other states from correctly¶ assessing another states’ intentions, as well as by the incentives states have to¶ misrepresent their willingness to fight – that is, to bluff.162 Informational asymmetries¶ increase the potential for misperception and thereby make war more likely; war,¶ consequentially, can be thought of in these cases as a “bargaining failure.”163 Some political scientists have argued in recent decades – contrary to previously common wisdom – that features and constraints of democracies make them better suited than non-democracies to credibly signal their resolve when they threaten force. To bolster their bargaining position, states will seek to generate credible signals of their resolve by taking actions that can enhance the credibility of such threats, such as mobilizing military forces or making “hand-tying” commitments from which leaders cannot back down without suffering considerable political costs domestically.164 These domestic audience costs, according to some political scientists, are especially high for leaders in democratic states, where they may bear these costs at the polls.165 Given the potentially high domestic political and electoral repercussions democratic leaders face from backing down from a public threat, they have considerable incentives to refrain from bluffing. An adversary that understands these political vulnerabilities is thereby more likely to perceive the threats a democratic leader does issue as highly credible, in turn making it more likely that the adversary will yield.166 Other scholars have recently pointed to the special role of legislative bodies in signaling with regard to threatened force. This is especially interesting from the perspective of constitutional powers debates, because it posits a distinct role for Congress – and, again, one that does not necessarily rely on Congress’s ability to pass binding legislation that formally confines the President. Kenneth Schultz, for instance, argues that the open nature of competition within democratic societies ensures that the interplay of opposing parties in legislative bodies over the use of force is observable not just to their domestic publics but to foreign actors; this inherent transparency within democracies – magnified by legislative processes – provides more information to adversaries regarding the unity of domestic opponents around a government’s military and foreign policy decisions.167 Political opposition parties can undermine the credibility of some threats by the President to use force if they publicly voice their opposition in committee hearings, public statements, or through other institutional mechanisms. Furthermore, legislative processes – such as debates and hearings – make it difficult to conceal or misrepresent preferences about war and peace. Faced with such institutional constraints, Presidents will incline to be more selective about making such threats and avoid being undermined in that way.168 This restraining effect on the ability of governments to issue threats simultaneously makes those threats that the government issues more credible, if an observer assumes that the President would not be issuing it if he anticipated strong political opposition. Especially when members of the opposition party publicly support an executive’s threat to use force during a crisis, their visible support lends additional credibility to the government’s threat by demonstrating that political conditions domestically favor the use of force should it be necessary.169 In some cases, Congress may communicate greater willingness than the president to use force, for instance through non-binding resolutions.170 Such powerful signals of resolve should in theory make adversaries more likely to back down. The credibility-enhancing effects of legislative constraints on threats are subject to dispute. Some studies question the assumptions underpinning theories of audience costs – specifically the idea that democratic leaders suffer domestic political costs to failing to make good on their threats, and therefore that their threats are especially credible171 – and others question whether the empirical data supports claims that democracies have credibility advantages in making threats.172 Other scholars dispute the likelihood that leaders will really be punished politically for backing down, especially if the threat was not explicit and unambiguous or if they have good policy reasons for doing so.173 Additionally, even if transparency in democratic institutions allows domestic dissent from threats of force to be visible to foreign audiences, it is not clear that adversaries would interpret these mechanisms as political scientists expect in their models of strategic interaction, in light of various common problems of misperception in international relations.174 These disputes are not just between competing theoretical models but also over the links between any of the models and real-world political behavior by states. At this point there remains a dearth of good historical evidence as to how foreign leaders interpret political maneuvers within Congress regarding threatened force. Nevertheless, at the very least, strands of recent political science scholarship cast significant doubt on the intuition that democratic checks are inherently disadvantageous to strategies of threatened force. Quite the contrary, they suggest that legislative checks – or, indeed, even the signaling functions that Congress is institutionally situated to play with respect to foreign audiences interpreting U.S. government moves – can be harnessed in some circumstances to support such strategies. C. Legal Reform and Strategies of Threatened Force Among legal scholars of war powers, the ultimate prescriptive question is whether the President should be constrained more formally and strongly than he currently is by legislative checks, especially a more robust and effective mandatory requirement of congressional authorization to use force. Calls for reform usually take the form of narrowing and better enforcement (by all three branches of government) of purported constitutional requirements for congressional authorization of presidential uses of force or revising and enforcing the War Powers Resolutions or other framework legislation requiring express congressional authorization for such actions.175

[CONTINUED]

**Exec Power DA – 1NC [5/5]**

[CONTINUED]

As applied to strategies of threatened force, generally under these proposals the President would lack authority to make good on them unilaterally (except in whatever narrow circumstances for which he retains his own unilateral authority, such as deterring imminent attacks on the United States). Whereas legal scholars are consumed with the internal effects of war powers law, such as whether and when it constrains U.S. government decision-making, the analysis contained in the previous section shifts attention externally to whether and when U.S. law might influence decision-making by adversaries, allies, and other international actors. In prescriptive terms, if the President’s power to use force is linked to his ability to threaten it effectively, then any consideration of war powers reform on policy outcomes and longterm interests should include the important secondary effects on deterrent and coercive strategies – and how U.S. legal doctrine is perceived and understood abroad.176 Would stronger requirements for congressional authorization to use force reduce a president’s opportunities for bluffing, and if so would this improve U.S. coercive diplomacy by making ensuing threats more credible? Or would it undermine diplomacy by taking some threats off the table as viable policy options? Would stronger formal legislative powers with respect to force have significant marginal effects on the signaling effects of dissent within Congress, beyond those effects already resulting from open political discourse? These are difficult questions, but the analysis and evidence above helps generate some initial hypotheses and avenues for further research and analysis. One might ask at this point why, though, having exposed as a hole in war powers legal discourse the tendency to overlook threatened force, this Article does not take up whether Congress should assert some direct legislative control of threats – perhaps statutorily limiting the President’s authority to make them or establishing procedural conditions like presidential reporting requirements to Congress. This Article puts such a notion aside for several reasons. First, for reasons alluded to briefly above, such limits would be very constitutionally suspect and difficult to enforce.177 Second, even the most ardent war-power congressionalists do not contemplate such direct limits on the President’s power to threaten; they are not a realistic option for reform. Instead, this Article focuses on the more plausible – and much more discussed – possibility of strengthening Congress’s power over the ultimate decision whether to use force, but augments the usual debate over that question with appreciation for the importance of credible threats. A claim previously advanced from a presidentialist perspective is that stronger legislative checks on war powers is harmful to coercive and deterrent strategies, because it establishes easily-visible impediments to the President’s authority to follow through on threats. This was a common policy argument during the War Powers Resolution debates in the early 1970s. Eugene Rostow, an advocate inside and outside the government for executive primacy, remarked during consideration of legislative drafts that any serious restrictions on presidential use of force would mean in practice that “no President could make a credible threat to use force as an instrument of deterrent diplomacy, even to head off explosive confrontations.”178 He continued: In the tense and cautious diplomacy of our present relations with the Soviet Union, as they have developed over the last twenty-five years, the authority of the President to set clear and silent limits in advance is perhaps the *most* important of all the powers in our constitutional armory to prevent confrontations that could carry nuclear implications. … [I]t is the diplomatic power the President needs most under the circumstance of modern life—the power to make a credible threat to use force in order to prevent a confrontation which might escalate.179 In his veto statement on the War Powers Resolution, President Nixon echoed these concerns, arguing that the law would undermine the credibility of U.S. deterrent and coercive threats in the eyes of both adversaries and allies – they would know that presidential authority to use force would expire after 60 days, so absent strong congressional support they could assume U.S. withdrawal at that point.180 In short, those who oppose tying the president’s hands with mandatory congressional authorization requirements to use force sometimes argue that doing so incidentally and dangerously ties his hands in threatening it. A critical assumption here is that presidential flexibility, preserved in legal doctrine, enhances the credibility of presidential threats to escalate.

#### Korean war goes nuclear

STRATFOR ‘10 (International Think Tank, “North Korea, South Korea: The Military Balance on the Peninsula,” http://www.stratfor.com/analysis/20100526\_north\_korea\_south\_korea\_military\_balance\_peninsula, May 26, 2010)

So the real issue is the potential for escalation — or an accident that could precipitate escalation — that would be beyond the control of Pyongyang or Seoul. With both sides on high alert, both adhering to their own national (and contradictory) definitions of where disputed boundaries lie and with rules of engagement loosened, the potential for sudden and rapid escalation is quite real. Indeed, North Korea’s navy, though sizable on paper, is largely a hollow shell of old, laid-up vessels. What remains are small fast attack craft and submarines — mostly Sang-O “Shark” class boats and midget submersibles. These vessels are best employed in the cluttered littoral environment to bring asymmetric tactics to bear — not unlike those Iran has prepared for use in the Strait of Hormuz. These kinds of vessels and tactics — including, especially, the deployment of naval mines — are poorly controlled when dispersed in a crisis and are often impossible to recall. For nearly 40 years, tensions on the Korean Peninsula were managed within the context of the wider Cold War. During that time it was feared that a second Korean War could all too easily escalate into and a thermonuclear World War III, so both Pyongyang and Seoul were being heavily managed from their respective corners. In fact, USFK was long designed to ensure that South Korea could not independently provoke that war and drag the Americans into it, which for much of the Cold War period was of far greater concern to Washington than North Korea attacking southward. Today, those constraints no longer exist. There are certainly still constraints — neither the United States nor China wants war on the peninsula. But current tensions are quickly escalating to a level unprecedented in the post-Cold War period, and the constraints that do exist have never been tested in the way they might be if the situation escalates much further.

### Market Da

#### Forcing broad executive compliance on cyber disrupts private innovation ---- crushes fragile SEC guidelines and turns cyber-defensive operations

BODENHEIMER AND GOLDING 2013 (David Z. Bodenheimer , a partner, and Elliot R. Golding , an associate, in Crowell & Moring LLP’s Washington, D.C. of - fice. Mr. Bodenheimer specializes in Government Contracts and heads the Homeland Security practice. He currently serves as chair of the ABA Science & Technology Law Section’s Security, Privacy, and Information Law Division and co-chair of the Public Contract Law Section’s Cybersecurity, Privacy, and Data Protection Committee. Mr. Golding specializes in Privacy & Cybersecurity compliance counseling and secu - rity incident litigation regarding a wide range of laws and regulations, such as: HIPAA and HITECH; GLBA; state laws regarding pre-breach security requirements, breach notification, and unfair/deceptive trade practices; and foreign laws governing data privacy and security, “FEATURE COMMENT: Regulating Cybersecurity On A Piecemeal Basis- Can The Executive Order Harmonize The Cyber Law Patchwork?”, <http://www.crowell.com/files/FEATURE-COMMENT-Regulating-Cybersecurity-On-A-Piecemeal-Basis-Can-The-Executive-Order-Harmonize-The-Cyber-Law-Patchwork.pdf>, Vol. 55, No. 24, June 26, 2013)

Driven by relentless cyber attacks stealing billions of dollars of U.S. technology and breaching the privacy of millions of Americans, the race is on to regulate cybersecurity in the public and private sectors. The hard question is how. The failure of Congress to pass comprehensive cybersecurity legislation in the last two years has a direct bearing upon this race to regulate.

On one hand, President Obama sought to fill this void with EO 13636, “Improving Critical Infra structure Cybersecurity.” 78 Fed. Reg. 11739 (2013). This order seeks to build a “cybersecurity frame work” to “align” cybersecurity approaches in the public and private sectors, and to “harmonize and make consistent” cyber requirements for federal procurements. Id. at 11741–42. To implement the executive order’s quest for “harmonized” cybersecu rity standards, the General Services Administration and Department of Defense Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition issued a request for information (RFI) on May 13. 78 Fed. Reg. 27966–68 (2013). This RFI specifically seeks information on conflicting cyber standards and requirements:

Harmonization : In general, DoD and GSA seek information about any conflicts in statutes, regulations, policies, practices, contractual terms and conditions, or acquisition processes affecting federal acquisition requirements related to cyber security and how the federal government might address those conflicts

On the other hand, the lack of comprehensive cybersecurity legislation has created a legal vacuum that has been filled with an ad hoc, sector-by-sector approach to regulating cybersecurity through narrowly targeted federal statutes, regulations and policies. Over the past two years, a few examples include: •

Defense Contractors . The most recent Na tional Defense Authorization Act established requirements for certain defense contractors to report security breaches and provide secu rity audit access.

• Public Companies . The Securities and Ex change Commission issued guidelines for public companies to report on material incidents involving security breaches and cybersecurity safeguards.

• Information Technology Companies . For certain federal agencies buying IT systems, Congress has prohibited such acquisitions unless the Federal Bureau of Investigation has made a risk assessment regarding the potential for “cyber-espionage or sabotage” by the People’s Republic of China.

• Health Care Sector . The Department of Health and Human Services published new information security rules and breach notifi cation obligations for the health care sector. •

Critical Infrastructure Sectors . The new execu tive order calls for a framework for standards for the critical infrastructure sectors, but many already have their own information security requirements and standards that may slow the drive towards common standards.

These recent trends in regulating information security on a piecemeal basis underscore the chal lenges ahead for the executive order policy to “align” and “harmonize” cybersecurity standards and re quirements. Both public- and private-sector entities need to understand these trends towards regulating cybersecurity with a patchwork of cyber laws and regulations, as well as the impact of attempting to comply with multiple cyber standards coming from many directions.

Recent Trends in Patchwork Regulation of Cybersecurity —Over the past few years, Congress has been busy with a host of cybersecurity bills, including “several dozen cybersecurity-related bills before Congress” in 2010 alone. Sen. Sheldon White house (D-R.I.), “We Need to Act on Cybersecurity,” The National Law Journal (May 10, 2010). But none of the comprehensive bills have passed.

Instead, Congress has targeted certain industries or niches of cybersecurity with narrow legislation. At the same time, federal agencies have regulated cybersecurity for specific sectors with their own regulations, rules and standards. As a result, both the public and private sectors need to keep track of the new requirements and emerging trends in cyber law and regulation.

Cyber Requirements for “Cleared Defense Con tractors” : In 2013, Congress imposed cybersecurity requirements specifically aimed at “cleared defense contractors,” defined as “a private entity granted clearance by the Department of Defense to access, re ceive, or store classified information for the purpose of bidding for a contract or conducting activities in sup port of any program of the Department of Defense.” National Defense Authorization Act for Fiscal Year 2013, P.L. 112-239, § 941 (2013).

Section 941 also defined “covered network,” but did not limit the scope to classified networks: “The term ‘covered network’ means a network or informa tion system of a cleared defense contractor that con tains or processes information created by or for the Department of Defense with respect to which such contractor is required to apply enhanced protection.” Federal contractors without a security clearance need not worry about § 941.

But for “cleared” defense contractors, this sec tion leaves open the possibility that it may extend to both classified and unclassified networks. If unclassified networks also fall within the scope of § 941, then the provision could have expansive reach, potentially driving cyber requirements throughout a contractor’s network and organization.

Section 941 established two basic requirements for securing networks and information systems of “each cleared defense contractor”: (1) security breach notification requirements, and (2) security audit ac cess to the networks of such military contractors. Security breach notification requirements already exist in some areas at both the federal and state levels. Now, § 941 adds yet another. Under this new reporting requirement, § 941 requires that covered defense contractors provide “rapid reporting” of suc cessful penetrations of their networks and informa tion systems:

(1) Rapid Reporting. The procedures established pursuant to subsection (a) shall require each cleared defense contractor to rapidly report to a component of the Department of Defense desig nated pursuant to subsection (a) of each success ful penetration of the network or information systems of such contractor that meet the criteria established pursuant to subsection.

Just how “rapid” is not explained in this reporting requirement. DOD’s implementing procedures will presumably provide more detailed guidance on how rapidly to report “successful penetrations” of such networks.

For this “rapid reporting,” § 941 specifies that “[e] ach such report shall include the following”:

• “A description of the technique or method used in such penetration,”

• “A sample of the malicious software, if discov ered and isolated by the contractor, involved in such penetration,” and

• “A summary of information created by or for the Department in connection with any De partment program that has been potentially compromised due to such penetration.”

Given such reporting requirements, covered defense contractors will need to react quickly by gathering forensic evidence and identifying the hack ing tools used. In addition, § 941 includes a “harm” analysis that must address whether DOD information has been compromised by the successful penetration.

Not only must covered defense contractors satisfy the “rapid reporting” requirement, but they must also provide “access” rights for DOD to review their networks and information systems. The implement ing DOD procedures will “include mechanisms for Department of Defense personnel to, upon request, obtain access to equipment or information of a cleared defense contractor necessary to conduct forensic analysis in addition to any analysis conducted by such contractor.”

However, § 941 does impose some limitations on the scope of DOD’s access: (a) the access must be limited to the purpose of determining whether a DOD program suffered an exfiltration of data, and (b) DOD must provide for reasonable protection of the contractor’s trade secrets and other business data

SEC Guidance for Publicly Traded Companies : On Oct. 13, 2011, SEC entered the race to regulate cybersecurity, identifying this area as a potential material risk for publicly traded companies. SEC, “Cybersecurity: CF Disclosure Guidance: Topic No. 2” (Oct. 13, 2011). In this guidance, SEC addressed cer tain risk factors that may trigger a corporate duty to make a public disclosure.

Impact of Cyber Attacks

. As documented in a host of congressional hearings, Government investigations and private-sector reports, cyber attacks have done great damage to corporations of all sizes. In its guid ance, SEC incorporated a panoramic list of potential injuries and impacts from cyber attacks and breaches that corporations may need to report:

The objectives of cyber attacks vary widely and may include theft of financial assets, intellectual property, or other sensitive information belong ing to registrants, their customers, or other business partners. Cyber attacks may also be directed at disrupting the operations of regis trants or their business partners. Registrants that fall victim to successful cyber attacks may incur substantial costs and suffer other nega tive consequences, which may include, but are not limited to:

• Remediation costs that may include liability for stolen assets or information and repairing system damage that may have been caused. Remediation costs may also include incentives offered to customers or other business partners in an effort to maintain the business relation ships after an attack;

• Increased cybersecurity protection costs that may include organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;

• Lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;

• Litigation; and • Reputational damage adversely affecting cus tomer or investor confidence.

Cyber Risk Assessment . Conducting a risk assess ment of cyber threats represents a common element of an information security program. The SEC guidance underscores the importance for corporations to identify major threats and critical cyber risks that may affect their particular business:

Registrants should disclose the risk of cyber incidents if these issues are among the most sig nificant factors that make an investment in the company speculative or risky. [Footnote omitted.]

In determining whether risk factor disclosure is required, we expect registrants to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents. As part of this evaluation, registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, includ ing the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or op erational disruption. In evaluating whether risk factor disclosure should be provided, registrants should also consider the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.

Security Safeguards . Merely identifying and as sessing the cyber threat is just one part of a corpora tion’s cyber defenses. In addition, the SEC guidance instructs corporations to address security controls and any deficiencies that may increase exposure to cyber threats and security breaches:

Registrants are required to disclose conclusions on the effectiveness of disclosure controls and procedures. To the extent cyber incidents pose a risk to a registrant’s ability to record, process, summarize, and report information that is re quired to be disclosed in Commission filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective.

[Footnote omitted.] For example, if it is reason ably possible that information would not be re corded properly due to a cyber incident affecting a registrant’s information systems, a registrant may conclude that its disclosure controls and procedures are ineffective.

Security Breaches . In the event of a material security breach, the SEC guidance specifies that corporations should address the impact in their public disclosures:

For example, if material intellectual property is stolen in a cyber attack, and the effects of the theft are reasonably likely to be material, the registrant should describe the property that was stolen and the effect of the attack on its results of operations, liquidity, and finan cial condition and whether the attack would cause reported financial information not to be indicative of future operating results or financial condition. If it is reasonably likely that the attack will lead to reduced revenues [or], an increase in cybersecurity protection costs, including related to litigation, the regis trant should discuss these possible outcomes, including the amount and duration of the ex pected costs, if material. Alternatively, if the attack did not result in the loss of intellectual property, but it prompted the registrant to materially increase its cybersecurity protec tion expenditures, the registrant should note those increased expenditures.

In summary, the SEC guidance on cybersecurity remains relatively new, with limited experience for corporations to apply the guidance and make public disclosures so far. Given the risk of major security breaches, the SEC guidance may ratchet up the pressure on companies to accelerate risk assessments and security safeguards to mitigate the risks of a major cybersecurity incident.

Supply Chain Security for Select Federal Agencies : Protecting the supply chain represents a fundamental element of a typical information security program. In the massive bill to continue funding federal agencies for 2013, Congress again took the ad-hoc approach to cybersecurity by regulating one piece of the supply chain. 2013 Consolidated and Further Continuing Appropriations Act, Division B, § 516(a), P.L. 113-6 (March 20, 2013).

This law applies not to the entire Federal Govern ment, but just to select agencies buying products from Chinese entities:

(a) None of the funds appropriated or otherwise made available under this Act may be used by the Departments of Commerce and Justice, the National Aeronautics and Space Administration, or the National Science Foundation to acquire an information technology system unless the head of the entity involved, in consultation with the Federal Bureau of Investigation or other appropriate Federal entity, has made an assess ment of any associated risk of cyber-espionage or sabotage associated with the acquisition of such system, including any risk associated with such system being produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People’s Republic of China.

(b) None of the funds appropriated or otherwise made available under this Act may be used to acquire an information technology system described in an assessment required by sub section (a) and produced, manufactured or as sembled by one or more entities that are owned, directed or subsidized by the People’s Republic of China unless the head of the assessing entity described in subsection (a) determines, and reports that determination to the Committees on Appropriations of the House of Representa tives and the Senate, that the acquisition of such system is in the national interest of the United States.

This patchwork surprise in § 516 raises a host of questions about its scope, meaning and intent. • Why does it apply only to the departments of Commerce and Justice, NASA, and the Na tional Science Foundation?

• May the “head of the entity” delegate the assessment of “any associated risk of cyberespionage or sabotage”?

• What type of consultation is required with the FBI—and who is the “other appropriate Fed eral entity” for consultation?

• Why does this requirement apply only to Chi nese entities?

But § 516 does not include legislative history to guide either the agencies or contractors in how to comply with its terms.

A number of industry trade groups have combined to oppose the restrictions in § 516 as being unworkable. See, e.g., BSA/The Software Alliance et al., Letter to Congressional Leadership (April 4, 2013), available at www.bsa.org . If § 516 remains unchanged, these agencies and contractors will face major challenges in acquiring IT systems due to the difficulties in determining whether such systems include Chinese-derived components and assessing whether any “risk of cyber-espionage or sabotage” may exist.

Security Rules for the Health Care Industry : Al though not new, the Health Insurance Portability and Accountability Act (HIPAA) required implementation of security standards for health information, including “reasonable and appropriate administrative, technical, and physical safeguards” to ensure the integrity and confidentiality of such information, protect against “reasonably anticipated” threats and unauthorized uses and disclosures, and otherwise ensure compli ance. 42 USCA § 1320d-2(d). Years ago, HHS issued regulations incorporating cybersecurity requirements for “protected health information” (PHI).

On January 25, HHS published new HIPAA regu lations making major changes in how the public and private sectors must protect PHI. 78 Fed. Reg. 5566 (2013). Key revisions include subjecting additional entities to cybersecurity requirements (security rule), imposing liability directly upon business associates and downstream subcontractors, and presumptively requiring breach notification in more situations. Some of the key changes include the following.

Breach Notification . Under the prior rule, covered entities had greater flexibility in determining whether breach notification would be required, as HHS only re quired notification if there was a “ significant risk of fi nancial, reputational, or other harm to the individual.” In the final rule, HHS eliminated the more subjective “risk of harm” standard that previously applied when determining whether a security incident constituted a “breach” requiring individual notification.

The final rule establishes a presumption that any impermissible use or disclosure of PHI constitutes a breach that compromises the security or privacy of the information. The covered entity or business as sociate bears the burden of proving a low probability that the PHI has been “compromised,” thus avoiding the need to notify. HHS characterized the previous “risk of harm” standard as too subjective, undermin ing uniformity regarding the duty for notification.

Thus, the new risk assessment standard focuses on whether unauthorized recipients have accessed or had the opportunity to access PHI, rather than the risk of harm to an individual.

Penalty Methodology and Assessment . In the final rule, HHS also raised the stakes for violation and data breaches by widening its enforcement net and invoking tougher penalties. HHS finalized the increased liability structure created by the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of P.L. 1115, Act by: (1) applying civil monetary penalties to violations of the HITECH Act and implementing regulations, (2) subjecting business associates and all downstream subcontractors to direct liability for certain HIPAA violations (discussed below), and (3) increasing the monetary penalties for such violations. The degree of culpability determines the range of the potential penalty for each violation of a given provision, as illustrated by the following table The precise fine will depend on factors set forth in 45 CFR § 160.408, such as the nature and extent of the violation (including the number of persons af fected and time period during which the violation oc curred), the nature and extent of the resulting harm, the history of prior compliance with the provision, the financial condition of the covered entity or business associate, and “such other matters as justice may require.” The final rule also clarified how HHS will impose fines for “multiple identical violations” where the violation of a provision affects multiple people or is ongoing. In such cases, HHS may impose a separate fine for each person affected by a violation or for each day that the violation continued.

Business Associate Direct Liability . Under the prior rule, the HIPAA obligations applied directly to covered entities, but business associates generally faced only contractual liability to the covered entity depending on what had been flowed down by the covered entity. The final rule makes business associates and their subcon tractors directly liable for violating the HIPAA security rule, as well as certain provisions of the privacy and breach notification rules. These provisions include:

• impermissible uses and disclosures;

• failure to provide breach notification to the covered entity;

failure to provide access to a copy of electronic PHI to either the covered entity, the individual or the individual’s designee (whichever is speci fied in the business associate agreement);

• failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or re quest;

• failure to enter into business associate agree ments with subcontractors that create or re ceive PHI on their behalf;

• failure to disclose PHI where required by the secretary to investigate or determine the busi ness associate’s compliance with the HIPAA rules;

• failure to provide an accounting of disclosures (if subject to those requirements pursuant to the business associate agreement); and

• failure to comply with the requirements of the security rule.

The final rule also establishes a parallel set of contractual requirements for subcontractors of busi ness associates who create, receive, maintain or trans mit PHI on behalf of the business associate. In the final rule, covered entities must obtain satisfactory assurances regarding the protection of PHI from their business associates, and business associates must do the same with their subcontractors, and so on, no mat ter how far “down the chain” the information flows.

Business Associate “Conduit” Exception . The HIPAA regulations previously carved out an excep tion to the definition of “business associate” for enti ties that serve merely as “conduits” through which PHI travels (such as the U.S. Postal Service). Many data storage companies had sought to expand this exception in the final rule to cover arrangements in which an entity stores, but does not normally access, PHI that it maintains on behalf of a covered entity. However, the final rule rejected attempts to exempt more entities from HIPAA compliance.

Instead, business associates now include a wide array of entities, such as: (1) health information or ganizations, E-prescribing gateways, or other persons that provide data transmission services involving PHI to a covered entity and that require routine access to such PHI; and (2) a person who offers a personal health record to one or more individuals on behalf of a covered entity (i.e., a personal health record vendor).

Although the final rule does not provide a bright-line test for what constitutes “routine access,” the rule does clarify that the conduit exception is intended to exclude only those entities providing courier services, such as the Postal Service or United Parcel Service, and their electronic data transmission equivalents, such as internet service providers.

Security Standards for Critical Infrastructure Sectors : As discussed above, President Obama issued EO 13636, “Improving Critical Infrastructure Cy bersecurity,” in February. This latest executive order builds on prior statutory authority under the Home land Security Act of 2002, tasking the Department of Homeland Security to “develop a comprehensive national plan for securing key resources and critical infrastructure of the United States,” including IT. 6 USCA § 121(d)(5).

EO 13636 calls for a “baseline framework” for reducing cyber risk to the various critical infrastruc ture sectors:

Sec. 7 . Baseline Framework to Reduce Cyber Risk to Critical Infrastructure . (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technol ogy (the “Director”) to lead the development of a framework to reduce cyber risks to critical infrastructure (the “Cybersecurity Framework”). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cy bersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objec tives of this order, and shall meet the require ments of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and [Office of Management and Budget] Circular A-119, as revised.

78 Fed. Reg. 11740–41. In short, this executive order seeks to bring a degree of uniformity—along with minimum standards—to the various sectors of critical infrastructure.

However, the drafters of the cybersecurity framework will not be writing on a blank slate. To the contrary, many critical infrastructure sectors have already been tasked with addressing cyber -security standards. 2007 Homeland Security Appro priations Act, P.L. 109-295, § 550; 6 CFR §§ 27.215, 27.225, 27.230, 27.235, 27.240, 27.245 (chemical sector); Electricity Modernization Act (title XII), P.L. 109-58, § 1211, 119 Stat. 941–42 (2005); 7 CFR §§ 1730.20, 1730.21, 1730.22, 1730.27, 1730.28 (energy sector); 10 CFR § 73.1 (nuclear sector); 9/11 Act, P.L. 110-53, § 1512(d) (railroad and bus carriers).

For sectors and industries that have already invested in cybersecurity defenses built to existing statutory and regulatory standards, the predictable reaction will be to avoid material changes imposing significant rework and additional cost. Thus, the existing patchwork of critical infrastructure cybersecurity standards may serve as a countervailing factor weighing against new cyber standards emerging from the executive order’s cybersecurity framework, particularly for these sectors that have already implemented sector-specific standards.

EO 13636 also requires DOD and GSA to work with the Federal Acquisition Regulatory Council and prepare a report addressing “what steps can be taken to harmonize and make consistent procurement requirements related to cybersecurity.” 78 Fed. Reg. 11742 (2013). In an RFI, the Joint Working Group on Improving Cybersecurity and Resilience Through Ac quisition has sought information “about any conflicts in statutes, regulations, policies, practices, contractual terms and conditions, or acquisition processes affect ing federal acquisition.” 78 Fed. Reg. 27968 (2013). In performing this overview of the federal acquisition process, the joint working group will find a patch work of agency-specific regulations with both major and minor differences in cybersecurity requirements and standards. See, e.g., Defense Federal Acquisition Regulation Supplement § 239.7102-1; GSA Acquisi tion Manual (GSAM) § 539.700; Department of Home land Security (HSAR) § 3004.470; Health and Human Services Acquisition Regulation subpt. 339.71; NASA FAR Supplement § 1804.470-1.

Of greater concern, many agencies incorporate internal instructions and policies into the acquisi tion process, introducing even greater variation and uncertainty regarding federal cybersecurity standards. See, e.g., DFARS § 239.7102-1 (various DOD directives and policies); GSAM § 539.7001(d) (GSA CIO IT Security Procedural Guide); HSAR § 3004.470-2 (various DHS directives and policies). To the extent that such internal guidance has not been published for public notice and comment, this guid ance not only impedes the executive order’s directive to harmonize cybersecurity standards and practices, but also raises questions about compliance with the Administrative Procedure Act. 5 USCA § 552(a); see also NI Indus., Inc. v. U.S., 841 F.2d 1104, 1107 (Fed. Cir. 1988) (declining to enforce internal agency proce dures that had not been previously published in the Federal Register ); 30 GC ¶ 119.

Conclusion —In summary, cybersecurity law and policy have not been static in the past 18 months. While the latest executive order seeks to move cyber standards towards a common framework, the absence of comprehensive cyber legislation has allowed the march towards sector-specific regulation and cyber safeguards to continue without a break in stride. For companies crossing several industries and critical infrastructure sectors, the path towards more robust cybersecurity programs and procedures will be increasingly uneven, as different types of data in sepa rate sectors will trigger sector-specific requirements, thus further complicating the already difficult efforts to build corporate-wide, cost-effective cyber defenses

#### SEC leadership k2 Dodd-Frank success

Mont ’13 – writer for Compliance Week

(Joe, “Dodd-Frank Act Poses Threat to SEC's Independence, Gallagher Says”, Compliance Week, 2-27-2013, http://www.complianceweek.com/dodd-frank-act-poses-threat-to-secs-independence-gallagher-says/article/282203/)

During a speech last week at the Practising Law Institute's annual “The SEC Speaks” conference, Gallagher began by offering a historical note. It was originally intended that the Federal Trade Commission would administer the Securities Exchange Act of 1934. Congress ultimately, however, decided that an independent, bipartisan agency with a high level of technical expertise in securities matters was warranted and the SEC was created. Its core attribute of autonomy, however, is now threatened by a “constant stream of external influences.” ¶ Congress has traditionally provided the Commission with considerable flexibility to exercise its expertise and authority and avoided imposing “minutely detailed mandates,” Gallagher said. In the post-financial crisis regulatory environment, all that is changing. The Dodd-Frank Act, which contains approximately 400 specific mandates, around 100 of which apply directly to the SEC, are highly prescriptive and the Commission faces a demand to issue highly technical rules under all-too-short deadlines, he said. This limits its flexibility, while occupying time and resources that could be better spent fulfilling other responsibilities.¶ Gallagher's plea to fellow Commissioners is to push back.¶ “Although the Commission continues to stare down an overflowing plate of Dodd-Frank mandates in addition to its other responsibilities… it must not allow itself to assume a secondary role in the regulation of matters squarely within its jurisdiction and core competencies,” he said. “This, I'm afraid, is exactly the role that the Commission has taken thus far with respect to critical initiatives.”¶ Among those initiatives is the Volcker Rule, a prohibition on federally-insured, commercial banks engaging in proprietary trading and sponsoring or investing in hedge or private equity funds. Gallagher says the SEC, required to work cooperatively with banking regulators and the Commodity Futures Trading Commission, has “taken a back seat” throughout the rulemaking process, even though many of the specific activities to be regulated fall firmly within its core competencies. “For this rule to get done, and get done properly, the SEC must take a leadership role,” he said.

#### Successful dodd-frank model k2 safe euro-financial reforms

Financial Reform Regulatory Center ’12

(“Better Late Than Never – FSB Reports Regulatory Reform Is Advancing … But Slowly”, 2012, http://financial-reform.weil.com/credit-rating-agencies/late-fsb-reports-regulatory-reform-advancing-slowly/#axzz2NRVnvBig)

FSB member nations have been implementing resolution-planning regimes and other measures to increase SIFIs’ ability to be resolved in a crisis without government support and with limited disruption to the financial system. These measures are guided at a high level by the FSB’s 2011 publication Key Attributes of Effective Resolution Regimes for Financial Institutions (“Key Attributes”) and, in the U.S., have been implemented by the FRB and FDIC’s joint regulations under the Dodd-Frank Act. The FSB has recommended that its member nations prioritize SIFIs’ development of recovery and resolution plans (colloquially known in the U.S. as “Living Wills”), which the FSB views as a critical and, at present, delayed component of global financial reform.¶ The FSB did, however, identify certain examples of progress in resolution planning. It specifically named the U.S.’s regime under Dodd-Frank as an example of progress in implementing the Key Attributes. (The FSB did not specifically mention the U.K.’s regime, though the Financial Services Authority’s resolution-planning requirements have much in common with those under Dodd-Frank.) It also noted that the E.U.’s eventual adoption of recently proposed resolution-planning legislation would be an important step toward consistent implementation of reforms throughout the E.U.

#### Strong EU key to solve extinction

Bruton, 2 -- former prime minister of Ireland

(John, former ambassador of the EU to the US, European Commission Delegation ambassador, "The Future of the European Union," The Irish Times, 1-31-2002, 195.7.33.33/newspaper/special/2002/europe/index.htm)

As the Laeken Declaration put it, "Europe needs to shoulder its responsibilities in the governance of globalisation" adding that Europe must exercise its power in order "to set globalisation within a moral framework, in other words to anchor it in solidarity and sustainable development". Only a strong European Union is big enough to create a space, and a stable set of rules, within which all Europeans can live securely, move freely, and provide for themselves, for their families and for their old age. Individual states are too small to do that on their own. Only a strong European Union is big enough to deal with the globalised human diseases, such as AIDS and tuberculosis. Only a strong European Union is big enough to deal with globalised criminal conspiracies, like the Mafia, that threaten the security of all Europeans. Only a strong European Union is big enough to deal with globalised environmental threats, such as global warming, which threaten our continent and generations of its future inhabitants. Only a strong European Union is big enough to deal with globalised economic forces, which could spread recession from one country to another and destroy millions of jobs. Only a strong European Union is big enough to regulate, in the interests of society as a whole, the activities of profit seeking private corporations, some of which now have more spending power than many individual states. These tasks are too large for individual states. Only by coming together in the European Union can we ensure that humanity, and the values which make us, as individuals, truly human, prevail over blind global forces that will otherwise **overwhelm us.**

### Ptx

#### The sanctions bill won’t pass now – Democrats are supporting Obama but continued capital is key to keep them aligned with the base

Voice of America 1/23/14 ("Support Slipping for Iran Sanctions in US Senate")

CAPITOL HILL — More Democratic senators are quietly signaling their opposition to a bill that spells out new sanctions against Iran if negotiations to limit the country’s nuclear program do not yield a final accord. ¶ The bill retains bipartisan support in both houses of Congress, but passage is seen as increasingly unlikely in the Democratic-led Senate amid an intense lobbying effort by the Obama administration to hold off on sanctions while international negotiations proceed. ¶ Senators Patty Murray and Elizabeth Warren are the latest Democrats to announce their opposition to the Iran sanctions bill currently before Congress. ¶ In a letter to constituents in Washington state, Murray said “the administration should be given time to negotiate a strong verifiable comprehensive agreement” on Iran’s nuclear program. At the same time, she pledged to work “to swiftly enact sanctions” if the talks ultimately fail.¶ Similarly, a spokeswoman for Warren says the Massachusetts senator “does not support imposing additional sanctions through new legislation while diplomatic efforts to achieve a long-term agreement are ongoing.”¶ The sanctions bill has 16 Democratic co-sponsors, near-unanimous support among Republicans, and the backing of politically potent pro-Israeli U.S. lobbying groups. But 11 Senate committee chairs, including Murray, currently oppose the bill. ¶ Among Democrats who signed on to the measure late last year, some have grown less vocal in their defense and promotion of the measure in recent weeks. Senate Majority Leader Harry Reid has neither explicitly promised a vote on the bill, nor ruled it out. Congressional expert William Galston of the Brookings Institution says pressure from President Barack Obama appears to be swaying a growing number of Democratic lawmakers. “The White House is determined to prevent this from happening," he said. "The administration believes in the marrow of its bones that the executive branch is the lead negotiator in the matter and that it deserves a chance to conduct its own foreign policy."

#### PC is stopping veto-proof bill

Kampeas 1/14/14 (Ron, The Times of Israel, "Iran Sanctions Have Senate Majority But Veto Looms")

WASHINGTON (JTA) — More than half the United States Senate has signed on to a bill that would intensify sanctions against Iran. But in a sign of the so-far successful effort by the White House to keep the bill from reaching a veto-busting 67 supporters, only 16 Democrats are on board. The number of senators cosponsoring the bill, introduced by Sens. Mark Kirk (R-Illinois) and Robert Menendez (D-New Jersey), reached 59 this week, up from just 33 before the Christmas holiday break.

#### Plan wrecks PC

Douglas L. Kriner 10, Assistant Professor of Political Science at Boston University, 2010, After the Rubicon: Congress, Presidents, and the Politics of Waging War, p. 68-69

Raising or Lowering Political Costs by Affecting Presidential Political Capital

Shaping both real and anticipated public opinion are two important ways in which Congress can raise or lower the political costs of a military action for the president. However, focusing exclusively on opinion dynamics threatens to obscure the much broader political consequences of domestic reaction—particularly congressional opposition—to presidential foreign policies. At least since Richard Neustadt's seminal work Presidential Power, presidency scholars have warned that costly political battles in one policy arena frequently have significant ramifications for presidential power in other realms. Indeed, two of Neustadt's three "cases of command"—Truman's seizure of the steel mills and firing of General Douglas MacArthur—explicitly discussed the broader political consequences of stiff domestic resistance to presidential assertions of commander-in-chief powers. In both cases, Truman emerged victorious in the case at hand—yet, Neustadt argues, each victory cost Truman dearly in terms of his future power prospects and leeway in other policy areas, many of which were more important to the president than achieving unconditional victory over North Korea."¶ While congressional support leaves the president's reserve of political capital intact, congressional criticism saps energy from other initiatives on the home front by forcing the president to expend energy and effort defending his international agenda. Political capital spent shoring up support for a president's foreign policies is capital that is unavailable for his future policy initiatives. Moreover, any weakening in the president's political clout may have immediate ramifications for his reelection prospects, as well as indirect consequences for congressional races.59 Indeed, Democratic efforts to tie congressional Republican incumbents to President George W. Bush and his war policies paid immediate political dividends in the 2006 midterms, particularly in states, districts, and counties that had suffered the highest casualty rates in the Iraq War.60¶ In addition to boding ill for the president's perceived political capital and reputation, such partisan losses in Congress only further imperil his programmatic agenda, both international and domestic. Scholars have long noted that President Lyndon Johnson's dream of a Great Society also perished in the rice paddies of Vietnam. Lacking both the requisite funds in a war-depleted treasury and the political capital needed to sustain his legislative vision, Johnson gradually let his domestic goals slip away as he hunkered down in an effort first to win and then to end the Vietnam War. In the same way, many of President Bush's highest second-term domestic priorities, such as Social Security and immigration reform, failed perhaps in large part because the administration had to expend so much energy and effort waging a rear-guard action against congressional critics of the war in Iraq.61¶ When making their cost-benefit calculations, presidents surely consider these wider political costs of congressional opposition to their military policies. If congressional opposition in the military arena stands to derail other elements of his agenda, all else being equal, the president will be more likely to judge the benefits of military action insufficient to its costs than if Congress stood behind him in the international arena.

#### Causes Israel strikes

**Perr, 12/24/13 –** B.A. in Political Science from Rutgers University; technology marketing consultant based in Portland, Oregon. Jon has long been active in Democratic politics and public policy as an organizer and advisor in California and Massachusetts. His past roles include field staffer for Gary Hart for President (1984), organizer of Silicon Valley tech executives backing President Clinton's call for national education standards (1997), recruiter of tech executives for Al Gore's and John Kerry's presidential campaigns, and co-coordinator of MassTech for Robert Reich (2002).(Jon, “Senate sanctions bill could let Israel take U.S. to war against Iran” Daily Kos, [http://www.dailykos.com/story/2013/12/24/1265184/-Senate-sanctions-bill-could-let-Israel-take-U-S-to-war-against-Iran#](http://www.dailykos.com/story/2013/12/24/1265184/-Senate-sanctions-bill-could-let-Israel-take-U-S-to-war-against-Iran)

As 2013 draws to close, the negotiations over the Iranian nuclear program have entered a delicate stage. But in 2014, the tensions will escalate dramatically as a bipartisan group of Senators brings a new Iran sanctions bill to the floor for a vote. As many others have warned, that promise of new measures against Tehran will almost certainly blow up the interim deal reached by the Obama administration and its UN/EU partners in Geneva. But Congress' highly unusual intervention into the President's domain of foreign policy doesn't just make the prospect of an American conflict with Iran more likely. As it turns out, the Nuclear Weapon Free Iran Act essentially empowers Israel to decide whether the United States will go to war against Tehran. On their own, the tough new sanctions imposed automatically if a final deal isn't completed in six months pose a daunting enough challenge for President Obama and Secretary of State Kerry. But it is the legislation's commitment to support an Israeli preventive strike against Iranian nuclear facilities that almost ensures the U.S. and Iran will come to blows. As Section 2b, part 5 of the draft mandates: If the Government of Israel is compelled to take military action in legitimate self-defense against Iran's nuclear weapon program, the United States Government should stand with Israel and provide, in accordance with the law of the United States and the constitutional responsibility of Congress to authorize the use of military force, diplomatic, military, and economic support to the Government of Israel in its defense of its territory, people, and existence. Now, the legislation being pushed by Senators Mark Kirk (R-IL), Chuck Schumer (D-NY) and Robert Menendez (D-NJ) does not automatically give the President an authorization to use force should Israel attack the Iranians. (The draft language above explicitly states that the U.S. government must act "in accordance with the law of the United States and the constitutional responsibility of Congress to authorize the use of military force.") But there should be little doubt that an AUMF would be forthcoming from Congressmen on both sides of the aisle. As Lindsey Graham, who with Menendez co-sponsored a similar, non-binding "stand with Israel" resolution in March told a Christians United for Israel (CUFI) conference in July: "If nothing changes in Iran, come September, October, I will present a resolution that will authorize the use of military force to prevent Iran from developing a nuclear bomb." Graham would have plenty of company from the hardest of hard liners in his party. In August 2012, Romney national security adviser and pardoned Iran-Contra architect Elliott Abrams called for a war authorization in the pages of the Weekly Standard. And just two weeks ago, Norman Podhoretz used his Wall Street Journal op-ed to urge the Obama administration to "strike Iran now" to avoid "the nuclear war sure to come." But at the end of the day, the lack of an explicit AUMF in the Nuclear Weapon Free Iran Act doesn't mean its supporters aren't giving Prime Minister Benjamin Netanyahu de facto carte blanche to hit Iranian nuclear facilities. The ensuing Iranian retaliation against to Israeli and American interests would almost certainly trigger the commitment of U.S. forces anyway. Even if the Israelis alone launched a strike against Iran's atomic sites, Tehran will almost certainly hit back against U.S. targets in the Straits of Hormuz, in the region, possibly in Europe and even potentially in the American homeland. Israel would face certain retaliation from Hezbollah rockets launched from Lebanon and Hamas missiles raining down from Gaza. That's why former Bush Defense Secretary Bob Gates and CIA head Michael Hayden raising the alarms about the "disastrous" impact of the supposedly surgical strikes against the Ayatollah's nuclear infrastructure. As the New York Times reported in March 2012, "A classified war simulation held this month to assess the repercussions of an Israeli attack on Iran forecasts that the strike would lead to a wider regional war, which could draw in the United States and leave hundreds of Americans dead, according to American officials." And that September, a bipartisan group of U.S. foreign policy leaders including Brent Scowcroft, retired Admiral William Fallon, former Republican Senator (now Obama Pentagon chief) Chuck Hagel, retired General Anthony Zinni and former Ambassador Thomas Pickering concluded that American attacks with the objective of "ensuring that Iran never acquires a nuclear bomb" would "need to conduct a significantly expanded air and sea war over a prolonged period of time, likely several years." (Accomplishing regime change, the authors noted, would mean an occupation of Iran requiring a "commitment of resources and personnel greater than what the U.S. has expended over the past 10 years in the Iraq and Afghanistan wars combined.") The anticipated blowback? Serious costs to U.S. interests would also be felt over the longer term, we believe, with problematic consequences for global and regional stability, including economic stability. A dynamic of escalation, action, and counteraction could produce serious unintended consequences that would significantly increase all of these costs and lead, potentially, to all-out regional war.

#### Global war

**Reuveny, 10** – professor in the School of Public and Environmental Affairs at Indiana University (Rafael, “Unilateral strike could trigger World War III, global depression” Gazette Xtra, 8/7, - See more at: <http://gazettextra.com/news/2010/aug/07/con-unilateral-strike-could-trigger-world-war-iii-/#sthash.ec4zqu8o.dpuf>)

A unilateral Israeli strike on Iran’s nuclear facilities would likely have dire consequences, including a regional war, global economic collapse and a major power clash. For an Israeli campaign to succeed, it must be quick and decisive. This requires an attack that would be so overwhelming that Iran would not dare to respond in full force. Such an outcome is extremely unlikely since the locations of some of Iran’s nuclear facilities are not fully known and known facilities are buried deep underground. All of these widely spread facilities are shielded by elaborate air defense systems constructed not only by the Iranians but also the Chinese and, likely, the Russians as well. By now, Iran has also built redundant command and control systems and nuclear facilities, developed early warning systems, acquired ballistic and cruise missiles and upgraded and enlarged its armed forces. Because Iran is well-prepared, a single, conventional Israeli strike—or even numerous strikes—could not destroy all of its capabilities, giving Iran time to respond. Unlike Iraq, whose nuclear program Israel destroyed in 1981, Iran has a second-strike capability comprised of a coalition of Iranian, Syrian, Lebanese, Hezbollah, Hamas, and, perhaps, Turkish forces. Internal pressure might compel Jordan, Egypt and the Palestinian Authority to join the assault, turning a bad situation into a regional war. During the 1973 Arab-Israeli War, at the apex of its power, Israel was saved from defeat by President Nixon’s shipment of weapons and planes. Today, Israel’s numerical inferiority is greater, and it faces more determined and better-equipped opponents. After years of futilely fighting Palestinian irregular armies, Israel has lost some of its perceived superiority—bolstering its enemies’ resolve. Despite Israel’s touted defense systems, Iranian coalition missiles, armed forces, and terrorist attacks would likely wreak havoc on its enemy, leading to a prolonged tit-for-tat. In the absence of massive U.S. assistance, Israel’s military resources may quickly dwindle, forcing it to use its alleged nuclear weapons, as it had reportedly almost done in 1973. An Israeli nuclear attack would likely destroy most of Iran’s capabilities, but a crippled Iran and its coalition could still attack neighboring oil facilities, unleash global terrorism, plant mines in the Persian Gulf and impair maritime trade in the Mediterranean, Red Sea and Indian Ocean. Middle Eastern oil shipments would likely slow to a trickle as production declines due to the war and insurance companies decide to drop their risky Middle Eastern clients. Iran and Venezuela would likely stop selling oil to the United States and Europe. From there, things could deteriorate as they did in the 1930s. The world economy would head into a tailspin; international acrimony would rise; and Iraqi and Afghani citizens might fully turn on the United States, immediately requiring the deployment of more American troops. Russia, China, Venezuela, and maybe Brazil and Turkey—all of which essentially support Iran—could be tempted to form an alliance and openly challenge the U.S. hegemony. Russia and China might rearm their injured Iranian protege overnight, just as Nixon rearmed Israel, and threaten to intervene, just as the U.S.S.R. threatened to join Egypt and Syria in 1973. President Obama’s response would likely put U.S. forces on nuclear alert, replaying Nixon’s nightmarish scenario. Iran may well feel duty-bound to respond to a unilateral attack by its Israeli archenemy, but it knows that it could not take on the United States head-to-head. In contrast, if the United States leads the attack, Iran’s response would likely be muted. If Iran chooses to absorb an American-led strike, its allies would likely protest and send weapons but would probably not risk using force. While no one has a crystal ball, leaders should be risk-averse when choosing war as a foreign policy tool. If attacking Iran is deemed necessary, Israel must wait for an American green light. A unilateral Israeli strike could ultimately spark World War III.

# Case

### Solvency – 1nc

#### Secrecy means Congress would be ineffective—no solvency

Stephen Dycus—1AC Author—10, Professor, Vermont Law School, 8/11/10, “Congress’s Role in Cyber Warfare,” <http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf>

The National Security Act of 1947 23 showed Congress’s determination to exert some control over this nation’s intelligence apparatus. That determination was strengthened after the disclosure of widespread intelligence abuses by the CIA and other agencies.24¶ In 1991, in response to the Iran-Contra Affair, Congress adopted a measure directing the President to keep the congressional intelligence committees “fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity.”25 The term “intelligence activity” expressly includes “covert actions,”26 which additionally require a written finding by the President that they are “necessary to support identifiable foreign policy objectives of the United States and [are] important to the national security of the United States.”27 Intelligence activities are also understood to include “all activities that elements of the Intelligence Community are authorized to conduct pursuant to [Executive Order No. 12,333],” the executive charter for such activities.28 The “intelligence community” includes the Office of the Director of National Intelligence, CIA, NSA, other Defense Department intelligence components, and other federal intelligence elements,29 which are authorized to engage in, inter alia, intelligence collection and analysis and “activities to protect against international terrorism . . . and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents.”30 This broad mandate certainly encompasses many U.S. efforts to defend against cyber attack and to employ cyber weapons offensively. By this definition, most preparations for and conduct of cyber warfare should be reported to the intelligence committees as “intelligence activities.” It is significant that the reporting requirement in the 1991 law is not limited to agencies within the intelligence community. ¶ Yet this legislation provides no guarantee that Congress will receive the information it needs to play a meaningful role in the development or execution of cyber warfare policy. It is not known, for example, precisely what it means for the intelligence committees to be “fully and currently” informed, what kinds of intelligence activities are regarded as “significant” enough to report, or who decides.31 Other sections of the 1991 law call on all agencies involved in intelligence activities, not just the President, to keep the intelligence committees informed about those activities, but only “[t]o the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters.”32 The “due regard for” language might be invoked to keep Congress in the dark. ¶ Under the 1991 law, “covert actions,” those with respect to which “it is intended that the role of the United States Government will not be apparent or acknowledged publicly,”33 need only be reported to a small group of legislators known as the “Gang of Eight,”34 and then only in a “timely fashion,” a term not defined by statute.35 Characterization of U.S. planning and execution of electronic warfare as “covert” could enable reporting to the smaller group, making it more difficult for Congress to play a significant role.36 Moreover, any reporting might be delayed indefinitely.37

### Solvency – nsa 1nc

#### The aff increases OCO operations- Alexander being the head of command means the affirmative is a concession to him

Grubbs ’13 (Larry Grubbs, Senior Lecturer in the Department of History at Georgia State University. In U.S. history, he studies foreign relations, the Cold War, and the cultural history of the five human senses. His work has appeared in the journals Diplomatic History and Peace and Change, among other publications. His book, Secular Missionaries: Americans and African Development in the 1960s, was published by the University of Massachusetts Press in 2010, “I’d Tap That,” or Whither General Keith Alexander?”, <http://tropicsofmeta.wordpress.com/2013/09/09/id-tap-that-or-whither-general-keith-alexander/>, September 9, 2013)

On August 23 the Wall Street Journal reported that National Security Agency (NSA) analysts abused their extraordinary power to conduct surveillance on love interests – “LOVEINT,” as intelligence analysts call it. This had Twitter sizzling with such hashtags as #NSAPickuplines and #NSALovePoems and the popular parody @PRISM\_NSA (a reference to the PRISM surveillance program disclosed by Edward Snowden earlier this summer) where citizens poke a little fun at the shadowy officials who spy on them in the name of national security (with such suggestive adaptations of spy-speak as “I’d tap that,” “I’d like to violate your privacy,” “After all that metadata, I’m looking forward to some content”). Meantime, Snowden, the erstwhile hacker nerd for hire employed as a contractor for the NSA, has now become a global icon, complete with his own Wikileaks line of merchandise and the essential Che Guevara-inspired t-shirts. Though hounded by Washington for his leaking of classified secrets, Snowden is justly admired by most of the world for his disclosure of the extraordinary and deeply disturbing surveillance programs the NSA has pursued without any public debate or meaningful congressional oversight. It’s hard not to enjoy these expressions of a robust humor and commitment to transparency that have remained unscathed in this age of ultra-surveillance. Perhaps, however, we can agree that it is, ultimately, no laughing matter that Americans and citizens of the world now live under a high-tech NSA Leviathan with a fetish for hyper secrecy. If, as recent reports suggest, “the NSA has secretly worked to gain access to virtually all communications entering, leaving, or going through the country,” scrutiny is overdue. When the last drop of ribald fun has been wrung from our tweets and we’ve bought as many Snowden mugs as we can afford, it might be time to put into perspective the man whom Snowden has forced out of the shadows and who is singularly responsible for some of the most disturbing tendencies of our age. Have Snowden adorn the merchandise, but let it be four-star General Keith Alexander who endures the heat of the public glare. Despite his public obscurity (until Snowden’s leaks), Alexander is a stealthy but shrewd bureaucratic operator who has reshaped the national security state to serve his agenda. As head of NSA, Cyber Command and even more shadowy parts of the surveillance state, he has built an empire that threatens the basic privacy and civil liberties of all Americans and much of the population of the world, and threatens the peace of the world with the development and proliferation of dangerous cyberweapons. The NSA under Alexander has, in the words of one expert, “transformed itself into the largest, most covert, and most potentially intrusive intelligence agency ever created.” Alexander’s Cyber-Industrial Complex Snowden blew the whistle heard round the world before embarking on his own global tour, which currently has him marooned in Moscow. Snowden’s revelations came as a bombshell to many citizens in this country and abroad, but perhaps they should not have. For one thing, Snowden only disclosed a portion of the iceberg. There are more – and possibly more dangerous – NSA programs than those he has revealed. Second and more importantly, there is, in a certain sense, nothing completely new about the recent abuse of power emanating from Fort Meade, Maryland. Though government classification of documents, and the inherently arcane nature of espionage – and especially signals intelligence, the NSA’s specialty – limits how much of the terrain we can see, enough is known about the history of the U.S. intelligence community to feel a sense of expectation. In a way, the current mania of the NSA is a fitting conclusion to generations of paranoia, power hunger, incompetence and abuse by the entire U.S. intelligence community (and their foreign partners). Nevertheless, like many others, I found the steady outpouring of new details about the NSA’s surveillance and cyberwar programs – and the absurd secrecy and hypocrisy surrounding them – left me increasingly anxious and angry about the apotheosis of the surveillance state. It’s hard to keep up: from the Bush-era revelations about warrantless wiretapping to the Obama-era disclosures from Wikileaks and Snowden, the sheer range and scope of the intelligence community’s eavesdropping makes the subject daunting and, perhaps, has induced fatalism in many Americans. To make sense of it all, it is helpful to revisit the work of the most reliable guide to all things NSA, James Bamford, and to read his latest contributions. Bamford, author of four finely researched volumes on the history of the NSA and its pre-1952 signals intelligence predecessors dating back to the First World War, is THE expert on the agency. Since 1982, when he published The Puzzle Palace, Bamford has doggedly pursued as much information as possible about what the secretive agency – often referred to as No Such Agency – does, how, and why. Through Freedom of Information Act requests and interviews with current and former NSA officials, he follows the trail of an agency dedicated to concealment. The cover of The Puzzle Palace depicts an ear, the symbol of eavesdropping, and he often writes there and in subsequent books about the NSA turning its “ear” this way and that as it seeks to listen in on international – and, increasingly, domestic – communications. A thoughtful profile of Bamford earlier this summer by Alexander Nazaryan for The New Yorker notes that even his earliest writings warned of the NSA’s indifference to legal restraints and its voracious appetite for as much information as it could possibly get, even if it meant violating its charter by spying on Americans. By 2008, Bamford had published a scathing takedown of the agency’s exploitation of 9/11, The Shadow Factory. Written shortly after Alexander had succeeded General Michael Hayden, the book makes only a few brief references to the new director of the agency. However, in three articles published in 2012-13 – two for Wired and one for The New York Review of Books – Bamford has zeroed in on Alexander and the behemoth that his agency has become. Bamford, though described by Nazaryan as “a slightly mischievous character,” is ideally suited to offer this introduction to Alexander in his June 2013 contribution to Wired: …. Never before has anyone in America’s intelligence sphere come close to his degree of power, the number of people under his command, the expanse of his rule, the length of his reign, or the depth of his secrecy. A four-star Army general, his authority extends across three domains: He is director of the world’s largest intelligence service, the National Security Agency; chief of the Central Security Service; and commander of US Cyber Command. As such, he has his own secret military, presiding over the Navy’s 10th Fleet, the 24th Air Force, and the Second Army. The massive expansion of Alexander’s cyber warfare resources has been illustrated by one of Snowden’s latest revelations. At the end of August, we learned that in 2011 alone, the United States “carried out 231 offensive cyber-operations,” mostly aimed at such adversaries as Russia, China, Iran, and North Korea. Despite American claims that China is threatening the stability of the world with its hacking, the United States remains the most prolific in cyber warfare. Alexander has used the specter of a devastating cyberattack – what former CIA Director and Secretary of Defense Leon Panetta calls “a cyber Pearl Harbor” – on the United States as principal justification for amassing control over so much data and erecting such a formidable institutional edifice. One can only sigh, perhaps, at the inevitability that someone like Alexander would respond to the drop off of actual global terrorism against American interests by invoking a new, frightening-sounding if vague bogeyman. As a bureaucratic strategy, the use of cyber threats to justify ever-growing “cyberspace operations” budgets for both the NSA and the Department of Defense has been a signature success. At a time when sequestration has hit other intelligence agencies, Alexander has been able to spend more and more. The NSA’s massive expansion of the headquarters at Fort Meade and several facilities across the country and its enlistment of “cyberattack teams” has, in turn, been very good for certain businesses. “What’s good for Alexander,” writes Bamford, “is good for the fortunes of the cyber-industrial complex, a burgeoning sector made up of many of the same defense contractors who grew rich supplying the wars in Iraq and Afghanistan.” With $30 billion being spent annually on cybersecurity the bonanza shows no signs of slowing down, as companies build or expand vast facilities and hire armies of “attack and penetration consultants.” Snowdens abound. What Alexander has done is to persuade Washington that the best defense against this threat is a great offense. Established in 2009 by the Pentagon, US Cyber Command has become a key part of Alexander’s realm. As he explained recently during congressional testimony, “I would like to be clear that this team, this defend-the-nation team, is not a defensive team.” Cyber Command has over 14,000 personnel. The goal has been to “dominate cyberspace” the same way the United States armed forces “dominate air and space.” That dominance, of course, comes at the expense not only of other countries, but of American citizens who value even a modicum of privacy. For all his personal blandness (he “more closely resembles a head librarian than George Patton. His face is anemic, his lips a neutral horizontal line… Some combat types had a derisive nickname for him: Alexander the Geek”), Alexander embodies and is responsible for a number of disturbing tendencies that make apathy no longer an option. Bamford quotes a “senior intelligence official” familiar with the NSA’s recent success at code-breaking: “Everybody’s a target; everybody with communication is a target.” The NSA is getting better and better at reading even the encrypted information of both governments and individual citizens in the United States and abroad. To store all of the data the NSA is swiping, it has erected the Utah Data Center at a staggering cost of $2 billion. This heavily protected facility “will become, in effect, the NSA’s cloud.” It will take in data from American spy satellites, overseas listening posts and a series of perhaps ten to twenty NSA domestic listening posts, “secret monitoring rooms in telecom facilities throughout the US.” (Bamford notes that these secret rooms, called “switches,” have not been a secret for some time, as the practice dates back to the immediate aftermath of 9/11, but the NSA refuses to acknowledge their existence.) The data then becomes fodder for “NSA code breakers, data-miners, China analysts, counterterrorism specialists, and others” at Fort Meade and beyond. As ever, Bamford captures the drama: Flowing through its servers and routers and stored in near-bottomless databases will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails – parking receipts, travel itineraries, bookstore purchases, and other digital “pocket litter.” It is, in some measure, the realization of the “total information awareness” program created during the first term of the Bush administration – an effort that was killed by Congress in 2003 after it caused an outcry over its potential for invading Americans’ privacy. From James Bamford, “The NSA Is Building the Country’s Biggest Spy Center (Watch What You Say)” Menacing, all-encompassing systems of information gathering are unsettling, to be sure, but so, too, is the human failure. Bamford strongly doubts Alexander’s ambitious programs are protecting Americans. If the NSA is so much better as a result of its recent buildup, why did it fail to catch “the near-disastrous attempted attacks by the underwear bomber on a flight to Detroit in 2009 and by the car bomber in Times Square in 2010?” Congressional critics have argued the agency gives misleading statements that exaggerate the impact the programs have had in counterterrorism. Those who are familiar with the basics of how, historically, espionage works find it difficult to take NSA claims at face value. As Kenneth Roth, director of Human Rights Watch and a former prosecutor has argued, when U.S. intelligence has disrupted specific plots, the success has been “not because of the mass collection of our metadata but through more traditional surveillance of particular phone numbers or e-mail addresses – the kinds of targeted inquiries that easily would have justified a judicial order allowing review of records kept by communications companies.” Endgame? Fittingly, I’m writing this in downtown Atlanta, Georgia. Bamford has pointed to this city as the corporate home of “one of the most secretive” of the defense contractors to rise alongside Alexander’s empire. His Wired essay on Alexander singles out, as an extreme example of the “cyber-industrial complex,” Endgame Systems, which is located in Midtown at 817 West Peachtree Street. Such defense contractors, according to Bamford, sell the services Alexander’s conception of cyberwar requires, recruiting “cyberwarriors [who] play offense and defense,” “computer network attack specialists,” “attack and penetration consultants.” Endgame, a startup created in 2008, “is transparently antitransparent.” Wikileaks disclosed an internal email quoting the company’s desire to stay that way: “We don’t ever want to see our name in a press release.” Endgame is, however, too flush with capital and too important a player to go wholly unnoticed. Why? Endgame is developing ways to break into internet-connected devices through chinks in their antivirus armor. Like safecrackers listening to the click of tumblers through a stethoscope, the “vulnerability researchers” use an extensive array of digital tools to search for hidden weaknesses in commonly used programs and systems, such as Windows and Internet Explorer. And since no one else has ever discovered these unseen cracks, the manufacturers have never developed patches for them. Endgame also serves to NSA, Cyber Command, the CIA and British intelligence “a unique map showing them exactly where their targets are located. Dubbed Bonesaw, the map displays the geolocation and digital address of basically every device connected to the Internet around the world, providing what’s called network situational awareness.” For millions of dollars, Endgame can give its clients the capability of pinpointing seemingly complete information on foreign targets – such as government agencies in China – and to find in their defenses “the equivalent of a back door left open.” The high stakes this represents worries even intelligence officials, who debate the extent to which “the buying and selling of such a subscription by nation-states could be seen as an act of war.” Bamford quotes Mike Jacobs, a former top NSA official who thinks it is, indeed: “In my opinion, these activities constitute acts of war, or at least a prelude to future acts of war.” Jacobs, noting the complete lack of regulation or oversight of this development and sale of cyberweapons, says “It should be illegal. I knew about Endgame when I was in intelligence. The intelligence community didn’t like it, but they’re the largest consumer of that business.” Bamford concludes that by buying the services of a firm like Endgame, “the spy agencies are helping drive a lucrative, dangerous, and unregulated cyber arms race, one that has developed its own gray and black markets.” Endgame and its competitors could choose to sell their cyberweapons to anyone, including adversarial nations like Iran or to terrorists, a prospect Alexander himself has called his “greatest worry.” I would add that even if Endgame and others remain committed to selling only to the Americans and to American allies, the danger remains that the manic drive for offensive cyberweapons might well provoke a real war. That it would have begun shrouded in such secrecy and as a result of a corporate profit strategy would make the disaster all the greater. Endgame’s website (http://www.endgamesystems.com/) implores potential clients to “Visualize Risk, Create Opportunity.” It doesn’t offer much detail on what, exactly, Endgame does, or how to interact with its personnel. It does give us cyberwarfare with a human face on the “Meet the Team” page, which cutely mingles personal details (“Telvis is a lover of hard problems and loud music”) with a fairly conventional rundown of the executive management, albeit one stuffed with national security connections, capped by the membership on the Board of Directors, which includes former NSA Director Lt. General Kenneth A. Minihan. The retired Lt. General seems to have been swayed by the gusher of capital pouring into Endgame in the last several months. Chris Rouland, “co-founder and founding CEO,” is a Georgia Tech grad whose previous experience includes, reassuringly, a stint as Vice President at Lehman Brothers.[15] America’s economic recovery remains sluggish, the nation might yet default on its debt, but the times they are a-booming for firms such as Endgame that make themselves indispensable within the cyberwar complex. With a report this week listing sixteen firms (including Endgame) among those reaping “eight-figure venture capital deals directed at tech security firms in the past 20 months,” we seem to have a self-reinforcing mechanism at work. It is said that Snowden’s revelations have, ironically, increased the value of the services of these shadowy firms that offer “solutions” to corporate and national security planners worried about their cyber vulnerabilities. While it’s nice to see a bull market for at least one sector of the American economy, one might fail, however, to accept the Panglossian assurance from the chief marketing officer at one of these cash-rich security start-ups: “The cybersecurity market is in a renaissance period that should enable the good guys to leapfrog the bad guys in prevention and detection capabilities.” Such a claim belies not only the improbability that cash or technology alone will best “the bad guys” overseas, but also the enormous risks to American civil liberties posed by the wild west, anything goes lack of regulation and oversight that has created countless Snowdens, snooping on citizens without scrutiny at the behest of the NSA.

## Cyber adv

### A2 cyber arms race

#### Squo solves

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

In May 2011, the US International Strategy for Cyberspace answered the President's call and was the first US policy document to provide, in Secretary Clinton's introductory words, ‘an approach that unifies our engagement with international partners on the full range of cyber issues’.82 Norms are promoted in the context of ‘applying the broad expectations of peaceful and just interstate conduct to cyberspace’ in order to effect ‘stability’, as obtains in ‘other spheres of international relations’.83 The document stresses the collaborative and cooperative aspects of global normative change whilst reiterating states' rights to self-defence consistent with the UN Charter. Norms extended not only to technical issues of network functionality but also to ‘upholding fundamental freedoms’ consistent with several high-profile speeches by Secretary Clinton on this topic,84 and a range of other responsibilities of states to the privacy of their citizens and so on. Importantly, the document stated, ‘[a]dherence to such norms brings predictability to state conduct, helping prevent the misunderstandings that could lead to conflict’.85 Norms are therefore principally, although not exclusively, to be understood as regulative norms concerned with preventing inter-state conflict, and can be framed as a form of norms-based deterrence.

#### Can’t solve with norms

BAKER 2012 - partner at Steptoe & Johnson in Washington, D.C., and former assistant secretary for policy and technology at the Department of Homeland Security (Baker, Stewart, May 1, 2012, “What Is the Role of Lawyers in Cyberwarfare?”, http://www.abajournal.com/magazine/article/what\_is\_the\_role\_of\_lawyers\_in\_cyberwarfare)

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

#### 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.

### A2 grid

#### The warrant to their 1ac extinction claim is grid collapse ---- Grid is resilient and sustainable

**Clark ’12** (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).

### A2 china

#### US cyber norms don't translate to China

Healey 13 Jason Healey is the director of the Cyber Statecraft Initiative at the Atlantic Council of the United States, Foreign Policy, April 16, 2013, "China Is a Cyber Victim, Too", http://www.foreignpolicy.com/articles/2013/04/16/china\_is\_a\_cyberwar\_victim\_too?page=full

Yet U.S. cyber-operations are extremely different from their Chinese equivalents and cannot be compared in the way the Chinese suggest. When the U.S. military or intelligence community conducts cyber-operations, they are quiet, coordinated, exceptionally well targeted, and under the strict control of senior officers and government executives. Lawyers review every stage. Even Stuxnet, though it was a breathtakingly sophisticated and brazen attack, was so tightly controlled that, when it escaped its target network, it caused no disruption. The White House keeps a close hold on cyber-operations through senior executives, generals, and political appointees throughout the bureaucracy.

Chinese espionage, by comparison, is under no such control. As in other areas of Chinese society, the People's Liberation Army and state-owned enterprises are subject to little oversight and feel little need to coordinate their actions. Recently, one colleague that works for a specialized incident-response firm reported finding as many as seven different Chinese espionage groups operating in the same network, all sending information back to different masters. Few, if any, senior party officials care to rein in activities helping domestic companies (and probably lining their own pockets) by stealing foreign intellectual property.

#### The warrant to their china war scenario is because we can’t defend ourselves against A2AD --- military doctrine means no A2AD threat

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

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

#### No US-China war

**Rosecrance et al ‘10** (Richard, Political Science Professor @ Cal and Senior Fellow @ Harvard’s Belfer Center and Former Director @ Burkle Center of IR @ UCLA, and Jia Qingguo, PhD Cornell, Professor and Associate Dean of School of International Studies @ Peking University, “Delicately Poised: Are China and the US Heading for Conflict?” Global Asia 4.4, <http://www.globalasia.org/l.php?c=e251>)

**Will China and the US Go to War?** If one accepts the previous analysis, the answer is “**no**,” or at least not likely. Why? First, despite its revolutionary past, **China has** gradually **accepted the US-led world** order **and become a status quo power.** It has joined most of the important inter-governmental international organizations. It has subscribed to most of the important international laws and regimes. It has not only accepted the current world order, it has become a strong supporter and defender of it. China has repeatedly argued that the authority of the United Nations and international law should be respected in the handling of international security crises. China has become an ardent advocate of multilateralism in managing international problems. And China has repeatedly defended the principle of free trade in the global effort to fight the current economic crisis, despite efforts by some countries, including the US, to resort to protectionism. To be sure, there are some aspects of the US world order that China does not like and wants to reform. However, **it wishes to improve that world order rather than to destroy it.**  Second, **China has** **clearly rejected** the option of **territorial expansion.** It argues that territorial expansion is both immoral and counterproductive: immoral because it is imperialistic and counterproductive because it does not advance one’s interests. China’s behavior shows that instead of trying to expand its territories, **it has been trying to settle its border disputes through negotiation**. Through persistent efforts, China has concluded quite a number of border agreements in recent years. As a result, most of its land borders are now clearly drawn and marked under agreements with its neighbors. In addition, China is engaging in negotiations to resolve its remaining border disputes and making arrangements for peaceful settlement of disputed islands and territorial waters. Finally, **even on the question of Taiwan**, which China believes is an indisputable part of its territory, **it has adopted a policy of peaceful reunification**. A country that handles territorial issues in such a manner is by no means expansionist. Third, **China has relied on trade** and investment **for** national welfare and **prestige, instead of military conquest.** And like the US, Japan and Germany, China has been very successful in this regard. In fact, so successful that **it** really **sees no other option than to continue on this path to prosperity**. Finally, after years of reforms, China increasingly finds itself sharing certain basic values with the US, such as a commitment to the free market, rule of law, human rights and democracy. Of course, there are still significant differences in terms of how China understands and practices these values. However, at a conceptual level, Beijing agrees that these are good values that it should strive to realize in practice. A Different World It is also important to note that certain changes in international relations since the end of World War II have made the peaceful rise of a great power more likely. To begin with, the emergence of nuclear weapons has drastically reduced the usefulness of war as a way to settle great power rivalry. By now, all great powers either have nuclear weapons or are under a nuclear umbrella. If the objective of great power rivalry is to enhance one’s interests or prestige, the sheer destructiveness of nuclear weapons means that these goals can no longer be achieved through military confrontation. Under these circumstances, countries have to find other ways to accommodate each other — something that China and the US have been doing and are likely to continue to do. Also, globalization has made it easier for great powers to increase their national welfare and prestige through international trade and investment rather than territorial expansion. In conducting its foreign relations, the US relied more on trade and investment than territorial expansion during its rise, while Japan and Germany relied almost exclusively on international trade and investment. China, too, has found that its interests are best served by adopting the same approach. Finally, the development of relative pacifism in the industrialized world, and indeed throughout the world since World War II, has discouraged any country from engaging in territorial expansion. **There is less and less popular support for using force to address even legitimate concerns** on the part of nation states. Against this background, efforts to engage in territorial expansion are likely to rally international resistance and condemnation. Given all this, is the rise of China likely to lead to territorial expansion and war with the US? The answer is no.

## Convergence adv

### A2 terror risk

#### No risk of terrorism

Mearsheimer 1/2 (John J. Mearsheimer, Does he need quals?, “America Unhinged”, <http://nationalinterest.org/article/america-unhinged-9639>, January-February 2014)

Am I overlooking the obvious threat that strikes fear into the hearts of so many Americans, which is terrorism? Not at all. Sure, the United States has a terrorism problem. But it is a minor threat. There is no question we fell victim to a spectacular attack on September 11, but it did not cripple the United States in any meaningful way and another attack of that magnitude is highly unlikely in the foreseeable future. Indeed, there has not been a single instance over the past twelve years of a terrorist organization exploding a primitive bomb on American soil, much less striking a major blow. Terrorism—most of it arising from domestic groups—was a much bigger problem in the United States during the 1970s than it has been since the Twin Towers were toppled. What about the possibility that a terrorist group might obtain a nuclear weapon? Such an occurrence would be a game changer, but the chances of that happening are virtually nil. No nuclear-armed state is going to supply terrorists with a nuclear weapon because it would have no control over how the recipients might use that weapon. Political turmoil in a nuclear-armed state could in theory allow terrorists to grab a loose nuclear weapon, but the United States already has detailed plans to deal with that highly unlikely contingency. Terrorists might also try to acquire fissile material and build their own bomb. But that scenario is extremely unlikely as well: there are significant obstacles to getting enough material and even bigger obstacles to building a bomb and then delivering it. More generally, virtually every country has a profound interest in making sure no terrorist group acquires a nuclear weapon, because they cannot be sure they will not be the target of a nuclear attack, either by the terrorists or another country the terrorists strike. Nuclear terrorism, in short, is not a serious threat. And to the extent that we should worry about it, the main remedy is to encourage and help other states to place nuclear materials in highly secure custody.

### A2 bioterror

#### The worst case bio-scenario happened – no extinction

**Dove 12** [Alan Dove, PhD in Microbiology, science journalist and former Adjunct Professor at New York University, “Who’s Afraid of the Big, Bad Bioterrorist?” Jan 24 2012, http://alandove.com/content/2012/01/whos-afraid-of-the-big-bad-bioterrorist/]

The second problem is much more serious. Eliminating the toxins, we’re left with a list of infectious bacteria and viruses. With a single exception, these organisms are probably near-useless as weapons, and history proves it.¶ There have been at least three well-documented military-style deployments of infectious agents from the list, plus one deployment of an agent that’s not on the list. I’m focusing entirely on the modern era, by the way. There are historical reports of armies catapulting plague-ridden corpses over city walls and conquistadors trying to inoculate blankets with Variola (smallpox), but it’s not clear those “attacks” were effective. Those diseases tended to spread like, well, plagues, so there’s no telling whether the targets really caught the diseases from the bodies and blankets, or simply picked them up through casual contact with their enemies.¶ Of the four modern biowarfare incidents, two have been fatal. The first was the 1979 Sverdlovsk anthrax incident, which killed an estimated 100 people. In that case, a Soviet-built biological weapons lab accidentally released a large plume of weaponized Bacillus anthracis (anthrax) over a major city. Soviet authorities tried to blame the resulting fatalities on “bad meat,” but in the 1990s Western investigators were finally able to piece together the real story. The second fatal incident also involved anthrax from a government-run lab: the 2001 “Amerithrax” attacks. That time, a rogue employee (or perhaps employees) of the government’s main bioweapons lab sent weaponized, powdered anthrax through the US postal service. Five people died.¶ That gives us a grand total of around 105 deaths, entirely from agents that were grown and weaponized in officially-sanctioned and funded bioweapons research labs. Remember that.¶ Terrorist groups have also deployed biological weapons twice, and these cases are very instructive. The first was the 1984 Rajneeshee bioterror attack, in which members of a cult in Oregon inoculated restaurant salad bars with Salmonella bacteria (an agent that’s not on the “select” list). 751 people got sick, but nobody died. Public health authorities handled it as a conventional foodborne Salmonella outbreak, identified the sources and contained them. Nobody even would have known it was a deliberate attack if a member of the cult hadn’t come forward afterward with a confession. Lesson: our existing public health infrastructure was entirely adequate to respond to a major bioterrorist attack.¶ The second genuine bioterrorist attack took place in 1993. Members of the Aum Shinrikyo cult successfully isolated and grew a large stock of anthrax bacteria, then sprayed it as an aerosol from the roof of a building in downtown Tokyo. The cult was well-financed, and had many highly educated members, so **this** release over the world’s largest city really **represented a worst-case scenario**.¶ **Nobody got sick** or died. From the cult’s perspective, it was a complete and utter failure. Again, the only reason we even found out about it was a post-hoc confession. Aum members later demonstrated their lab skills by producing Sarin nerve gas, with far deadlier results. Lesson: one of the top “select agents” is extremely hard to grow and deploy even for relatively skilled non-state groups. It’s a really crappy bioterrorist weapon.¶ Taken together, these events point to an uncomfortable but inevitable conclusion: our biodefense industry is a far greater threat to us than any actual bioterrorists.

### AT: Russia

#### No Russian War

Weitz ‘11 (Richard, senior fellow at the Hudson Institute and a World Politics Review senior editor, “Global Insights: Putin not a Game-Changer for U.S.-Russia Ties,” <http://www.scribd.com/doc/66579517/Global-Insights-Putin-not-a-Game-Changer-for-U-S-Russia-Ties>, September 27, 2011)

Fifth, there will inevitably be areas of conflict between Russia and the United States regardless of who is in the Kremlin. Putin and his entourage can never be happy with having NATO be Europe's most powerful security institution, since Moscow is not a member and cannot become one. Similarly, the Russians will always object to NATO's missile defense efforts since they can neither match them nor join them in any meaningful way. In the case of Iran, Russian officials genuinely perceive less of a threat from Tehran than do most Americans, and Russia has more to lose from a cessation of economic ties with Iran -- as well as from an Iranian-Western reconciliation. On the other hand, these conflicts can be managed, since they will likely remain limited and compartmentalized. Russia and the West do not have fundamentally conflicting vital interests of the kind countries would go to war over. And as the Cold War demonstrated, nuclear weapons are a great pacifier under such conditions. Another novel development is that Russia is much more integrated into the international economy and global society than the Soviet Union was, and Putin's popularity depends heavily on his economic track record. Beyond that, there are objective criteria, such as the smaller size of the Russian population and economy as well as the difficulty of controlling modern means of social communication, that will constrain whoever is in charge of Russia.

# Block

## PTX

#### China doesn't care about plan

Segal 11

Adam Segal is the Ira A. Lipman senior fellow for counterterrorism and national security studies at the Council on Foreign Relations, China US Focus, May 26, 2011, "Chinese Responses to the International Strategy for Cyberspace", http://www.chinausfocus.com/peace-security/chinese-responses-to-the-international-strategy-for-cyberspace/

A week after the United States released its International Strategy for Cyberspace, it is possible to gauge some Chinese responses. Not surprisingly, there was a relatively high degree of skepticism about U.S. intentions. Chinese concerns revolved around three issues:

The strategy is really about military capabilities and deterrence. Perhaps following the lead of some U.S. news reports, Chinese press reports focused on the statement that Washington reserved the right “to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law,” to defend itself and its allies. This must be frustrating to the State Department since it was trying to de-emphasize cyberspace as a warfighting “domain” and stress its importance as a public forum, market, and source of innovation. They wanted less talk about Cyber Command and more about international engagement. Certainly it couldn’t have been an accident that Deputy Secretary of Defense William Lynn spoke after Homeland Security Advisor John Brennan, Secretary of State Hillary Clinton, Attorney General Eric Holder, Secretary of Commerce Gary Locke, and Secretary of Homeland Security Janet Napolitano.

Despite the calls for cooperation, the U.S. is trying to maintain its technological lead. In the view of some Chinese analysts, the call for interoperability and global standards mask an effort to lock others into technologies owned by U.S. companies. Global Times quoted one analyst as saying: “The U.S. masters a number of core technologies for cyberspace usage, and it aims to continuously consolidate its advantages.” Similarly, in the area of Internet governance, no matter how often U.S. government officials refer to international cooperation, they still want the United States “to maintain its lead role. At a press conference on the same day, Hillary Clinton made this point very clear.”

#### No cooperation and no conflict—structural issues overwhelm

**Harding ’11** (Harry Harding 11, founding dean of the School of Leadership and Public Policy at the University of Virginia, “Are China and the U.S. on a collision course?”, June 14, http://thinkingaboutasia.blogspot.com/2011/06/are-china-and-us-on-collision-course.html

In my judgment, **it is highly unlikely for the relationship between the US and China to be primarily cooperative**, at least in the short to medium term. **The differences in values, political systems, interests, levels of development, and perceptions of the existing international order are simply too great for the two countries to find common ground on all issues, or even to find a mutually agreeable allocation of costs and benefits when they try to pursue common interests**. Only a common interest that was massively compelling – say a widespread pandemic, another financial crisis, a global outbreak of terrorist activity targeted at both countries, or increasingly severe consequences of climate change – might produce a predominantly cooperative relationship. **Fortunately, an essentially confrontational relationship is also unlikely**, especially **if one is primarily concerned with** the risks of **military conflict**. **The high degree of economic interdependence between the two countries has already created a relatively resilient relationship**. **The cost of military conflict**, especially given the fact that both China and the US are nuclear powers, **will be a significant deterrent** against military conflict. Equally important, **the probability of the most worrying of the trigger events** identified above– a unilateral declaration of independence by Taiwan – **is presently quite low**, as is the risk that China would try to compel unification through the use of force.

## T

### A2 We Meet

#### Contextual definitions bad – intent to define outweighs

Eric Kupferbreg 87, University of Kentucky, Senior Assistant Dean, Academic & Faculty Affairs at Northeastern University, College of Professional Studies Associate Director, Trust Initiative at Harvard School of Public Health 1987 “Limits - The Essence of Topicality” http://groups.wfu.edu/debate/MiscSites/DRGArticles/Kupferberg1987LatAmer.htm

Often, field contextual definitions are too broad or too narrow for debate purposes. Definitions derived from the agricultural sector necessarily incorporated financial and bureaucratic factors which are less relevant in considering a 'should' proposition. Often subject experts' definitions reflected administrative or political motives to expand or limit the relevant jurisdiction of certain actors. Moreover, field context is an insufficient criteria for choosing between competing definitions. A particularly broad field might have several subsets that invite restrictive and even exclusive definitions. (e.g., What is considered 'long-term' for the swine farmer might be significantly different than for the grain farmer.) Why would debaters accept definitions that are inappropriate for debate? If we admit that debate is a unique context, then additional considerations enter into our definitional analysis.

#### Authority is the exercise of power over others

OED 13 (http://www.oed.com/viewdictionaryentry/Entry/13349)

authority, n.

I. Power to enforce obedience.

a. Power or right to enforce obedience; moral or legal supremacy; the right to command, or give an ultimate decision.

b. in authority: in a position of power; in possession of power over others.

### A2 CI

#### There's a clear brightline---restrictions require a floor and a ceiling---oversight is a floor but doesn't set a cap on the President's potential actions

USCA 77, UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT, 564 F.2d 292, 1977 U.S. App. LEXIS 10899,. 1978 Fire & Casualty Cases (CCH) P317

Continental argues that even if the Aetna and Continental policies provide coverage for the Cattuzzo accident, that coverage should [\*\*8] be limited to a total of $300,000 because Atlas agreed to procure "not less than" $300,000 coverage. The District Court properly found that the subcontract language does not support a restriction on the terms of Continental's policy because the subcontract only sets a floor, not a ceiling, for coverage.

## K

### Terror K – FW 2NC

#### This is key to all coherent debate

CRAWFORD 2002 - Neta Crawford ,PhD MA MIT, BA Brown, Prof. of poli sci at boston univ. Argument and Change in World Politics, 2002 p. 19-21

Coherent arguments are unlikely to take place unless and until actors, at least on some level, agree on what they are arguing about. The at least temporary resolution of meta-arguments- regarding the nature of the good (the content of prescriptive norms); what is out there, the way we know the world, how we decide between competing beliefs (ontology and epistemology); and the nature of the situation at hand( the proper frame or representation)- must occur before specific arguments that could lead to decision and action may take place. Meta-arguments over epistemology and ontology, relatively rare, occur in instances where there is a fundamental clash between belief systems and not simply a debate within a belief system. Such arguments over the nature of the world and how we come to know it are particularly rare in politics though they are more frequent in religion and science. Meta-arguments over the “good” are contests over what it is good and right to do, and even how we know the good and the right. They are about the nature of the good, specifically, defining the qualities of “good” so that we know good when we see it and do it. Ethical arguments are about how to do good in a particular situation. More common are meta-arguments over representations or frames- about how we out to understand a particular situation. Sometimes actors agree on how they see a situation. More often there are different possible interpretations. Thomas Homer-Dixon and Roger karapin suggest, “Argument and debate occur when people try to gain acceptance for their interpretation of the world”. For example, “is the war defensive or aggressive?”. Defining and controlling representations and images, or the frame, affects whether one thinks there is an issue at stake and whether a particular argument applies to the case. An actor fighting a defensive war is within international law; an aggressor may legitimately be subject to sanctions. Framing and reframing involve mimesis or putting forward representations of what is going on. In mimetic meta-arguments, actors who are struggling to characterize or frame the situation accomplish their ends by drawing vivid pictures of the “reality” through exaggeration, analogy, or differentiation. Representations of a situation do not re-produce accurately so much as they creatively re-present situations in a way that makes sense. “mimesis is a metaphoric or ‘iconic argumentation of the real.’ Imitating not the effectivity of events but their logical structure and meaning.” Certain features are emphasized and others de-emphasized or completely ignored as their situation is recharacterized or reframed. Representation thus becomes a “constraint on reasoning in that it limits understanding to a specific organization of conceptual knowledge.” The dominant representation delimits which arguments will be considered legitimate, framing how actors see possibities. As Roxanne Doty argues, “the possibility of practices presupposes the ability of an agent to imagine certain courses of action. Certain background meanings, kinds of social actors and relationships, must already be in place.” If, as Donald Sylvan and Stuart Thorson argue, “politics involves the selective privileging of representations, “it may not matter whether one representation or another is true or not. Emphasizing whether frames articulate accurate or inaccurate perceptions misses the rhetorical import of representation- how frames affect what is seen or not seen, and subsequent choices. Meta-arguments over representation are thus crucial elements of political argument because an actor’s arguments about what to do will be more persuasive if their characterization or framing of the situation holds sway. But, as Rodger Payne suggests, “No frame is an omnipotent persuasive tool that can be decisively wielded by norm entrepreneurs without serious political wrangling.” Hence framing is a meta-argument.

#### on the representations are better to foreign policy

JOURDE 2006 - Cedric Jourde \* Ph.D., Political Science, University of Wisconsin-Madison, Madison, 2002 \* M.A., Political Science, University of Wisconsin-Madison, Madison, 1996 \* B.Sc., Political Science, Université de Montréal, Montréal, 1995 Hegemony or Empire?: The redefinition of US Power under George W Bush Ed. David and Grondin p. 182-3 2006

Relations between states are, at least in part, constructed upon representations. Representations are interpretative prisms through which decision-makers make sense of a political reality, through which they define and assign a subjective value to the other states and non-state actors of the international system, and through which they determine what are significant international political issues.2 For instance, officials of a given state will represent other states as 'allies', 'rivals', or simply 'insignificant', thus assigning a subjective value to these states. Such subjective categorizations often derive from representations of these states' domestic politics, which can for instance be perceived as 'unstable\*, 'prosperous', or 'ethnically divided'. It must be clear that representations are not objective or truthful depictions of reality; rather they are subjective and political ways of seeing the world, making certain things 'seen' by and significant for an actor while making other things 'unseen' and 'insignificant'.3 In other words, they are founded on each actor's and group of actors' cognitive, cultural-social, and emotional standpoints. Being fundamentally political, representations are the object of tense struggles and tensions, as some actors or groups of actors can impose on others their own representations of the world, of what they consider to be appropriate political orders, or appropriate economic relations, while others may in turn accept, subvert or contest these representations. Representations of a foreign political reality influence how decision-making actors will act upon that reality. In other words, as subjective and politically infused interpretations of reality, representations constrain and enable the policies that decision-makers will adopt vis-a-vis other states; they limit the courses of action that are politically thinkable and imaginable, making certain policies conceivable while relegating other policies to the realm of the unthinkable.4 Accordingly, identifying how a state represents another state or non-state actor helps to understand how and why certain foreign policies have been adopted while other policies have been excluded. To take a now famous example, if a transnational organization is represented as a group of 'freedom fighters', such as the multi-national mujahideen in Afghanistan in the 1980s, then military cooperation is conceivable with that organization; if on the other hand the same organization is represented as a 'terrorist network', such as Al-Qaida, then military cooperation as a policy is simply not an option. In sum. the way in which one sees, interprets and imagines the 'other\* delineates the course of action one will adopt in order to deal with this 'other'.

#### Affirmative form of governmental action precludes personal change killing political activism and link turning the plan

Kappeler 95 (Susanne, Associate Professor at Al-Akhawayn University, *The Will to Violence: The politics*

of personal behavior, Pg. 10- 1 1 )

Yet our insight that indeed we are not responsible for the decisions of a Serbian general or a Croatian president tends to mislead us into thinking that therefore we have no responsibiiitv at all, not evenfor forming our own judgment, and thus into underrating the responsibility we do have within our own sphere of action. In particular, it seems to absolve us from having to try to see any relation between our own actions and those events, or to recognize the connections between those political decisions and our own personal decisions. It not only shows that we participate in what Beck calls 'organized irresponsibility', upholding the apparent lack of connection between bureaucratically, institutionally, nationally, and also individually organized separate competences. It also proves the phenomenal and unquestioned alliance of our personal thinking with the thinking of the major power mongers, Forxtend to think that we cannot 'do' anvthing. say, about a war, because we deem ourselves to be in the wrong situation because we are not where the maior decisions are made. Which is why many of those not vet entirelv disillusioned with politics tend to engage in a form of mental deputy politics, in the style of 'what would **I** do if I were the general, the prime minister, the president, the foreign minister or the minister of defense?' Since *we* seem to regard their meca spheres of action as the only worthwhile and truly effective ones, and since our political analyses tend to dwell there first of all, any question of what I would do if **1** were indeed myself tends to peter out in the comparative insignificance of having what is perceived as 'virtually no possibilities': what I could do seems petty and futile. For my own action I obviously desire the range of action of a general, a prime minister,

or a General Secretary of the UN - finding expression in ever more prevalent formulations like 'I want to stop this war', 'I want military intervention', 'I want to stop this backlash', or 'I want a moral revolution. 'We are this war', however, even if we do not command the troops or participate in co-called peace talks, namely as Drakulic says, in our non-comprehension': our willed refusal to feel responsible for our own thinking and for working out our own understanding, preferring innocently to drift along the ideolo~icacl urrent of prefabricated arguments or less than innocently taking advantage of the advantages these offer. And we 'are' the war in our 'unconscious cruelty towards vou', our tolerance of the 'fact that vou have a yellow form for refugees and I don't'- our readiness, in other words, to build identities, one for ourselves and one for refugees, one of our own and one for the 'others.' We share in the responsibilitv for this war and its violence in the way we let them grow inside us, that is,& the wav we shaue 'our feelings, our relationships, our values' according: to the structures and the values of war and violence.

### Krepon 1

#### They just have no defense of the rhetoric used in this advantage ----- it short-circuits the core of their solvency mechanism

KREPON 2009 - co-founder of Stimson and director of the South Asia and Space Security programs. Krepon received an M.A. from the School of Advanced International Studies at Johns Hopkins University and a B.A. from Franklin & Marshall College (Krepon, Michael, “The Mushroom Cloud That Wasn't”, http://www.foreignaffairs.com/articles/64995/michael-krepon/the-mushroom-cloud-that-wasnt)

At the height of the Cold War, almost no one was bold enough or foolish enough to predict the Soviet Union's collapse, let alone without the eruption of a nuclear exchange between the two superpowers. One of the few who prophesied its demise, George Kennan, was deeply worried about a nuclear cataclysm. Kennan, a former U.S. ambassador to the Soviet Union and the father of containment policy, warned repeatedly that unwise U.S. nuclear policies could lead to Armageddon. The Cold War is now history, but warnings of an impending nuclear catastrophe are still very much alive. Anxieties today stem not from the threat of a surprise Soviet missile attack but from the fear of Iran, North Korea, Pakistan, and terrorist groups seeking to carry out catastrophic attacks against soft targets in the United States.¶ And yet, not a single death has occurred as a result of nuclear terrorism. Since 9/11, there have been more than 36,000 terrorist attacks, resulting in approximately 57,000 fatalities and 99,000 casualties. A terrible, mass-casualty attack using nuclear or biological weapons could occur at any time, and much more can be done to keep the United States safe. As the attacks that have occurred have repeatedly demonstrated, terrorists do not need weapons of mass destruction (WMD) to cause grievous harm; they can do so using hijacked airplanes, fertilizer, automatic weapons, and grenades.¶ But the situation is far from bleak. It is not easy for terrorist groups to acquire the skills and materials necessary to construct a nuclear weapon. Meanwhile, Washington and Moscow have reduced their nuclear arsenals by 34,000 weapons over the past two decades, nuclear testing is now rare, the list of countries with worrisome nuclear programs is very short by historical standards, and the permanent members of the UN Security Council now have less to fight about -- and more reasons to cooperate in preventing worst-case scenarios from occurring -- than ever before.¶ Yet warnings of the possibility of nuclear, chemical, or biological weapons attacks are as loud as ever. These warnings must be put in perspective. The United States has managed to remain safe from nuclear catastrophes in far more dangerous times. And if the threat is so great, and the protections so weak, why have there not been grievous WMD attacks on U.S. cities already? Wise U.S. initiatives to reduce these dangers have helped tremendously, such as programs initiated by then Senator Sam Nunn (D-Ga.) and Senator Richard Lugar (R-Ind.) to lock down dangerous weapons and materials and to dismantle Cold War-era missiles and bombers. There is another explanation as well: the threat itself has been greatly exaggerated.¶ CRYING WOLF¶ Predicting nuclear disasters was common during the Cold War. Paul Nitze, Kennan's successor as director of the State Department's policy planning staff, issued the Cold War's most famous warning to President Harry Truman in April 1950, forecasting four or five years of great danger ahead facing an emboldened Joseph Stalin. The anxieties expressed in Nitze's report -- known as NSC-68 -- were reasonable given that the Soviet Union had conducted its first nuclear test in August 1949, Mao Zedong had just taken over mainland China, and the Korean War, which was to begin in June 1950, was already brewing.¶ The next warning of nuclear danger came in November 1957, four days after the launch of the second Sputnik. The Gaither Committee, headed by a Ford Foundation and RAND Corporation executive and assisted by Nitze, warned President Dwight Eisenhower, "The evidence clearly indicates an increasing threat, which may become critical in 1959 or early 1960." Such anxieties stemmed from presumed gaps between the bomber and missile capacities of the United States and those of the Soviet Union. But these gaps proved to be imaginary -- Washington actually led Moscow in these areas. The most harrowing episode of the Cold War -- the Cuban missile crisis, of October 1962 -- was in fact prompted by Moscow's weakness, rather than its strength, as the Soviets sought a quick fix for their perceived strategic disadvantage. ¶ The doomsayers got it wrong again during the Ford administration, when a group of experts was assembled to determine whether the U.S. intelligence community was underestimating the Soviet threat. These hawkish experts, known as Team B, included the historian Richard Pipes; a young Paul Wolfowitz, who would later become deputy secretary of defense; and Nitze. Team B issued a report in 1976 predicting that unless urgent measures were taken, the Soviet threat would reach its peak between 1980 and 1983. Although the 1979 Soviet invasion of Afghanistan lent credence to Team B's assessment at first, the ill-conceived occupation that followed turned out to be a harbinger of the Soviet Union's dissolution rather than a steppingstone to more ambitious conquests.¶ Today, as was the case during the Cold War, there is no shortage of nonproliferation specialists predicting impending nuclear disasters. Eighty-five experts polled by Senator Lugar in 2005 estimated that the risk of a WMD attack occurring before 2010 was 50 percent and before 2015, 70 percent. The Bulletin of the Atomic Scientists has set its iconic Doomsday Clock at five minutes to midnight -- two minutes closer to Armageddon than it was during the Cuban missile crisis. A bipartisan congressional commission concluded in 2008 that "America's margin of safety is shrinking, not growing" and that "unless the world community acts decisively and with great urgency, it is more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013." Graham Allison, one of the commission's members, had warned in 2004 that "the detonation of a nuclear device in an American city is inevitable if the U.S. continues on its present course." And soon after leaving office, former Vice President Dick Cheney warned that there is a "high probability" that terrorists will attempt a catastrophic nuclear or biological attack on the United States in the coming years.¶ These sorts of scary predictions have a basis in reality. After all, Iran has mastered the ability to enrich uranium, is laying the foundation for a nuclear weapons program, and has close ties to terrorist groups; Pakistan is ramping up its capacity to produce plutonium as the central government's influence is waning; and North Korea has a bomb-making capacity, weapons-grade material, and a need for hard currency. Al Qaeda's leaders have sought to acquire and use these weapons, and other extremist groups have an interest in doing so, too.¶ Experts cite such worrisome developments and then use threat inflation to seize the public's attention and to secure sufficient appropriations for their preferred remedies. They, along with government officials, members of Congress, and the intelligence community are all safer warning of great danger than downplaying threats -- except when their inflated anxieties facilitate a preventive war based on false premises. The Iraq war notwithstanding, when worst cases do not materialize, those who issued dire warnings can take credit. And if attacks do occur, the alarmists can always say, "I told you so."¶ As real as these threats are, hyping them carries its own risks. Crying wolf too often can lead to complacency when action is needed most. Repeated warnings can also prompt taxpayers and lawmakers to question what was gained from prior investments in reducing threats and so limit appropriations for new ones. This is a major problem, since remedial efforts over short periods of time are insufficient; reducing the nuclear threat requires success over the long haul.

## Cyber

### Arms race

#### Squo solves

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

#### Zero impact to cyber arms race --- overwhelming consensus of qualified authors goes neg ---- im fininishing this card

- 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>

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.

### Grid

#### The warrant to their 1ac extinction claim is grid collapse ---- Grid is resilient and sustainable

**Clark ’12** (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).

### China – regime

#### US cyber norms don't translate to China

Healey 13 Jason Healey is the director of the Cyber Statecraft Initiative at the Atlantic Council of the United States, Foreign Policy, April 16, 2013, "China Is a Cyber Victim, Too", http://www.foreignpolicy.com/articles/2013/04/16/china\_is\_a\_cyberwar\_victim\_too?page=full

#### Can’t solve with norms ---- finishing this card

BAKER 2012 - partner at Steptoe & Johnson in Washington, D.C., and former assistant secretary for policy and technology at the Department of Homeland Security (Baker, Stewart, May 1, 2012, “What Is the Role of Lawyers in Cyberwarfare?”, http://www.abajournal.com/magazine/article/what\_is\_the\_role\_of\_lawyers\_in\_cyberwarfare)

cheating is easy and strategically profitable. American compliance will be enforced by all those lawyers. Our adversaries can ignore the rules and say—hell, they are saying—“We’re not carrying out cyberattacks. We’re victims too. Maybe you’re the attacker. Or maybe it’s Anonymous. Where’s your proof?”¶ Even if all sides were genuinely committed to limiting cyberwar, as all sides were in 1939, we’ve seen that the logic of airpower eventually drove all sides to the horror they had originally recoiled from. Each side felt that it had observed the limits longer than the other. Each had lawyerly justifications for what it did, and neither understood or gave credence to the other’s justifications. In that climate, all it took was a single error to break the legal limits irreparably.¶ And error was inevitable. Bombs dropped by desperate pilots under fire go astray. But so do cyberweapons. Stuxnet infected thousands of networks as it searched blindly for Natanz. The infections lasted far longer than intended. Should we expect fewer errors from code drafted in the heat of battle and flung at hazard toward the enemy?¶ Of course not. But the lesson for the lawyers and the diplomats is stark: Their effort to impose limits on cyberwar is almost certainly doomed.¶ No one can welcome this conclusion, at least not in the United States. We have advantages in traditional war that we lack in cyberwar. We are not used to the idea that launching even small wars on distant continents may cause death and suffering here at home. That is what drives the lawyers. They hope to maintain the old world. But they’re driving down a dead end.¶ If we want to defend against the horrors of cyberwar, we need first to face them with the candor of a Stanley Baldwin. Then we need to charge our military strategists, not our lawyers, with constructing a cyberwar strategy for the world we live in, not the world we’d like to live in.

## China

#### The warrant to their china war scenario is because we can’t defend ourselves against A2AD --- military doctrine means no A2AD threat

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

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

#### They have no offense ---- China is restrained in key hotspots- newest expert consensus

**Friedman 12-24**-13 [Uri, senior associate editor at The Atlantic, where he oversees the Global Channel, “The Global Conflicts to Watch in 2014,” <http://www.theatlantic.com/international/archive/2013/12/the-global-conflicts-to-watch-in-2014/282624/>]

The survey, which asked more than 1,200 U.S. government officials, academics, and experts to assess the impact and likelihood of 30 scenarios, divides the results into three tiers of risk. And some of the findings are alarming. Beyond the familiar flashpoints—military intervention in Syria's civil war, strikes against Iran's nuclear facilities—the report raises concerns about overlooked threats ranging from turmoil in Jordan to civil war in Iraq to a border clash between China and India. The study is also notable for the risks it downplays, including armed confrontation between China and its neighbors over territorial disputes in the East and South China Seas.¶ The most threatening and most likely conflicts (in red) include some you might expect: limited military intervention in Syria's deteriorating civil war; a cyberattack on critical infrastructure in the U.S.; military strikes against Iran if nuclear talks fail or Tehran advances its nuclear program; a North Korean crisis sparked by military provocation or internal political instability; a major terrorist attack on the U.S. or an ally; and greater turmoil in Afghanistan and Pakistan as U.S. troops withdraw from the region and Afghanistan holds elections.¶ But other potential crises in this category have received less attention and were deemed less threatening in last year's survey, including the "strengthening of al-Qaeda in the Arabian Peninsula resulting from continued political instability in Yemen and/or backlash from U.S. counterterrorism operations" (in the latest example of those operations, a drone strike hit a Yemeni wedding); "civil war in Iraq due to rising Sunni-Shia sectarian violence" (the civilian death toll in the country more than doubled this year); and "growing political instability and civil violence in Jordan triggered by spillover from the Syrian civil war" (according to the experts polled, there is less of a risk of a similar phenomenon occurring in Lebanon, where a bombing near the Iranian embassy in Beirut recently killed 23 people). Second-tier risks (orange), according to the report, include a "severe Indo-Pakistani military confrontation triggered by a major terrorist attack or heightened violence in Kashmir" and "escalating violence and risk of mass atrocities in the Central African Republic," where a wave of sectarian killings has raised fears of a coming genocide.¶ In what may be the most striking finding, military conflict between China and neighbors like Japan and the Philippines in the East and South China Seas is judged to be less of a threat than it was in 2013, even after a tense year capped most recently by Beijing's creation of an Air Defense Identification Zone in the East China Sea. The thinking, perhaps, is that China's has tested the limits of its assertiveness in the region and will show more restraint in the coming year, or that the countries involved have now established mechanisms to resolve disputes before they devolve into armed confrontation. Some of the least likely and threatening conflicts (yellow) have never before been included in the study, including China and India butting heads over disputed territory, Venezuela succumbing to political crisis in the wake of Hugo Chavez's death, and Buddhists and Muslim Rohingyas clashing in Myanmar. South Sudan is mentioned, but only in the context of possible military conflict with Sudan—not in terms of South Sudan itself imploding (the survey was conducted in November, before internal fighting erupted in the country).

## Convergence

### Terror

#### No risk of terrorism ----- they have shifted their strategies

Mearsheimer 1/2 (John J. Mearsheimer, Does he need quals?, “America Unhinged”, <http://nationalinterest.org/article/america-unhinged-9639>, January-February 2014)

#### Terrorists strategy has shifted- new attacks will be small scale and local

**Schofield ’12** (McClatchy Washington Bureau Print This Article Posted on Thu, Apr. 26, 2012 After Osama bin Laden, al Qaida still a many-headed threat By Matthew Schofield | McClatchy Newspapers last updated: April 29, 2012 08:55:55 AM WASHINGTON -- ]

“What we’re facing today is a much, much larger global threat,” said Seth Jones, an expert at the RAND Corp. who’s advised the Pentagon on Afghanistan and Pakistan. “It’s a more dispersed threat. **The threat is decentralizing** to a broad network of groups. Al Qaida inspires, but doesn’t control, and they work with locals.” The meaning of that threat: **Massive attacks such as those on 9/11 are unlikely to be repeated.** But **expect smaller-scale attacks — the “strategy of a thousand cuts,”** it was called in AQAP’s slick online propaganda magazine Inspire. A deadly example came in 2009 with the rampage at Fort Hood, Texas, where Army psychiatrist Maj. Nidal Malik Hasan, allegedly radicalized online by AQAP, is accused of shooting dead 13 soldiers. His trial is scheduled to begin in August. **Experts note that these groups have largely localized agendas.** Generally, they’re looking to impose Islamic Sharia law and, if not overthrow a local government, carve out a space in which to operate in their home country.

## Solvency

### 2NC

#### Turn

Nakashima ’13 (Ellen Nakashima, national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties. She previously served as a Southeast Asia correspondent for the paper. She wrote about the presidential candidacy of Al Gore and co-authored a biography of Gore, and has also covered federal agencies, Virginia state politics and local affairs. She joined the Post in 1995. “Dual-leadership role at NSA and Cyber Command stirs debate”, <http://www.washingtonpost.com/world/national-security/dual-leadership-role-at-nsa-and-cyber-command-stirs-debate/2013/10/06/ffb2ac40-2c59-11e3-97a3-ff2758228523_story.html>, October 6, 2013)

During suspected Iranian cyber­attacks on the Web sites of commercial banks last year, Gen. Keith B. Alexander, who simultaneously heads the country’s largest electronic spy agency and the military’s Cyber Command, proposed a simple solution: Shut off the attacks at their source. “We had the expertise and could have done something about it,” said one U.S. official, who like others interviewed for this store spoke on the condition of anonymity to describe sensitive discussions. “We’re sitting on their networks overseas. Why don’t we just turn it off?” But the proposal to send a simple computer “reset” command to the attacking servers was ultimately rejected by National Security Council officials this year because the attacks were not causing enough harm to warrant an offensive response. The episode shows the willingness — some say eagerness — of Alexander to use his authority to conduct offensive actions to fend off attacks against the private sector. If a similar proposal were on the table today, it would be the new cyber-teams that Alexander is creating to defend the nation that probably would do the job. As he builds out U.S. Cyber Command at Fort Meade, Md., and other installations to a fighting force of 6,000 over the next three years, there are fresh questions about the wisdom of so much power residing in one “dual-hatted” official. The debate has taken on greater significance in the wake of disclosures by former National Security Agency contractor Edward Snowden about the sweeping scope of the agency’s domestic surveillance to thwart terrorist attacks and gain foreign intelligence. “The mashing together of the NSA and Cyber Command has blurred the lines between a military command and a national spy agency,” said Peter Singer, a Brookings Institution expert on evolving modes of warfare. Alexander disagrees. “It’s one network,” he said in a recent interview. “We all operate on the same network. You create more problems by trying to separate them and have two people fighting over who’s in charge [of both missions] than putting it all together. I think our nation benefits from that.” He said that other countries “do similar things.” Britain’s GCHQ, the equivalent of the NSA, is able to conduct espionage and computer-network attacks. With Alexander expected to retire next year after eight years as the longest-serving NSA director, his successor will face the questions. Administration officials acknowledge that there are concerns with what they call the dual-hat assignment, which includes regularly briefing the president on counterterrorism. “It is an unusual arrangement,” said one senior administration official, speaking on the condition of anonymity. “I’m sure that debate will resurface when General Alexander leaves that position — whether that’s the right mixture to have.” When it comes to cyber­attacks, much of it is done by the NSA’s Tailored Access Operations unit, officials say. Many of the operators are uniformed military personnel who spy on overseas networks for national intelligence priorities, including targets such as Iran, Russia and North Korea, among other countries. According to interviews with U.S. officials, these same personnel, who operate under intelligence legal authorities, may switch to a military authority when they are ordered to conduct a computer attack under an execute order by the president and the defense secretary. The process is documented. “You can be doing intelligence-gathering one second and then pull the trigger on an offensive op the next,” a former intelligence official said. “We’re allowing the same military commander to tell us how bad the problem is and propose and implement suggestions to fix it,” said Jason Healey, director of the Atlantic Council’s Cyber Statecraft Initiative. “The concentration of power at Fort Meade risks further militarizing cyberspace.”

### UQ

#### We control UQ- sweeping NSA restrictions coming in the squo- the aff undermines those and NSA oversight fails

DailyProgress 1/13 (The Daily Progress, News Journal, “Reining in NSA's data overreach”, <http://www.dailyprogress.com/opinion/editorials/reining-in-nsa-s-data-overreach/article_16d01a7e-7c56-11e3-b763-001a4bcf6878.html>, January 13, 2014)

The agency operates by secrets within secrets, making any kind of accountability difficult, if not impossible. Among the potential changes could be improved oversight of the agency, more transparency, and a better system of checks and balances. Restraint ordered from the highest office in the land would be a fitting counterweight to the NSA’s swollen power. Congress is also pondering several bills to correct the situation. Legislative action is both important and necessary. Without accountability, the NSA has been permitted to run amok. It has thrust its tentacles deep into the lives of innocent, everyday Americans and even spied on trusted allies. Let Congress and the president speak, and let them speak for Americans’ right to be free from this form of invasion.

#### Large scale reform coming- the aff consultation requirements get ignored by the NSA

Sensenbrenner ’13 (Jim Sensenbrenner, chairman of the House Judiciary Subcommittee on Crime, Terrorism, Homeland Security and Investigations, “NSA abused trust, must be reined in”, <http://www.jsonline.com/news/opinion/nsa-abused-trust-must-be-reined-in-b99131601z1-230292131.html>, November 2, 2013)

It is impossible to forget the attacks of Sept. 11, 2001. And it is not easy to forget what followed: fear, anger and an upwelling of patriotism. Throughout our nation's history, we've fought in wars both at home and abroad, but until that day, most Americans felt invincible from an attack from the outside world. Following 9-11, the United States felt an unfamiliar vulnerability, but we also felt more unified than ever. Congress knew it had to act to enhance the tools the intelligence community needed to identify and track terrorists, but we never forgot what makes our country great: freedoms and liberties unlike anywhere else in the world. I led a bicameral group of legislators that came together and passed the USA Patriot Act with strong bipartisan support. President Ronald Reagan said, "trust but verify." After 9-11, with the country at risk and poised to enter its most intensive conflict since the Vietnam War, Congress extended the administration broader powers to help protect the American people. But the National Security Agency abused that trust. It ignored restrictions painstakingly crafted by lawmakers and assumed a plenary authority never imagined by Congress. Worse, the NSA has cloaked its operations behind such a thick cloud of secrecy that, even if our trust was restored, Congress and the American people would lack the ability to verify it. Our constitutional democracy was built to be accountable to the people. That principle can never be compromised. Earlier this year, Americans were rightly outraged to learn that the NSA is collecting in bulk the phone records of nearly every American. More recently, the media has revealed additional classified information that has added to our concerns. Since the revelation that the NSA is collecting the details of Americans' phone calls on an unprecedented scale, we have learned that the government searches the content of huge troves of emails, collects in bulk the address books from email accounts and social networking sites, at least temporarily collected geolocation data from our cellphones, committed thousands of privacy violations and lied to courts and Congress. This is not the America our founders envisioned. Not only do many of these programs raise serious legal questions, they have come at a high cost to Americans' privacy rights, business interests and standing in the international community. On Oct. 31, the Senate Intelligence Committee voted to give the NSA the authority to collect private data on innocent Americans. In an 11-4 vote, Sen. Dianne Feinstein (D-Calif.) presided over the first congressional vote in our country's history to allow unrestrained spying on the American people. I am committed to a different approach. On Oct. 29, Senate Judiciary Committee Chairman Patrick Leahy and I came together to introduce the USA Freedom Act. The bill has co-sponsors in the Senate covering the political spectrum, and nearly 90 co-sponsors in the House — almost an even split between Republicans and Democrats. It also has been endorsed by groups ranging from the National Rifle Association to the American Civil Liberties Union and has the support of many of the tech giants, including AOL, Apple, Facebook, Google, Microsoft and Yahoo. The USA Freedom Act restores Americans' privacy rights by ending the government's dragnet collection of phone records under Section 215 of the USA Patriot Act and requires greater oversight, transparency and accountability with respect to surveillance authorities. The bill also provides more safeguards against warrantless surveillance under the FISA Amendments Act and includes significant privacy and oversight provisions, creates a special advocate to focus on the protection of privacy rights before the FISA Court and requires more detailed public reporting. In short, the USA Freedom Act ensures the law is properly interpreted, past abuses are not repeated and American liberties are protected. And over the coming weeks and months, as more revelations are brought to light and public outrage grows, I will be working to push this important legislation through the House Judiciary Committee and onto the House floor. There, members can cast their vote to restore trust and accountability to our intelligence community.